Rechtsfragen im Web

Urheberrecht im Web 2.0, Cloud Computing und Datenschutz im Web waren die Schwerpunkte des 4. Österreichischen IT-Rechtstags am 17. und 18. Juni 2010 im Haus des Sports in Wien. Veranstalter war der Forschungsverein Infolaw.

Das Web 2.0, das „Mitmach-Web", wirft urheberrechtliche Fragen auf. Nicht mehr ein einzelner Kreativer steht einer Menge von Konsumenten gegenüber, sondern diese Menge produziert selbst. Aus der individuellen wird eine kollektive Kreativität. Aus „Produzent" und „Konsument" entsteht der „Prosumer". Die Einzelleistung kann vielfach nicht mehr isoliert betrachtet werden. Beispiele dafür sind Open-Source-Software und Open-Content Communities sowie die Weiterentwicklung von bloß dem Rahmen nach als Construction Kit vorgegebener Online-Games durch die Mitspieler selbst.

Viele „Digital Natives", jene Generation ab 1980, die mit der Informationstechnologie und dem Internet aufgewachsen ist, verstehen nicht, dass einzelne Bild- oder Tonpassagen in eigenen Schöpfungen nicht verwendet werden dürfen. Ass. iur. Gregor Völtz vom Institut für Wirtschaftsrecht der Universität Kassel schlug vor, bloß gebrauchende Benutzungen aus dem Anwendungsbereich des dem Urheber zustehenden Rechts der öffentlichen Wiedergabe herauszunehmen. Er bezog sich dabei auf das „Holden Dance Video": Eine Mutter hatte eine Videosequenz ins Netz gestellt, die ihr zweijähriges Kind zeigt, wie es ein paar Sekunden lang zu Klängen eines bekannten Schlagers tanzt – was ihr prompt eine urheberrechtliche Klage des Musikproduzenten eingebracht hat.

„Der Interessengegensatz, von dem das Urheberrecht in seiner heutigen Form ausgeht, stimmt im Web 2.0 nicht mehr und behindert die Kreativität", meinte auch Rechtsanwalt Dr. Till Kreutzer. Bestimmte Nutzungsszenarien wie „kreative Nutzung", Archivierung oder Nutzung verwaister Werke sollten von Verbotsrechten ausgenommen werden.

Bettina Stomper-Rosam: „Logfiles dürfen nicht gespeichert werden und sind zu löschen."

Alexander Schatten: „Probleme liegen in der Vertraulichkeit und Sicherheit der übermittelten Daten."

Cloud Computing. „So viel Neues ist Cloud Computing auch wieder nicht", sagte Dr. Alexander Schatten (TU Wien). „Es ist eine Art des Outsourcings, also der Datenverarbeitung durch einen externen Dienstleister. Neu ist, dass sich dieser Dienstleister in der Wolke, also im Internet, befindet". Derartige Dienste werden etwa von *Amazon, Microsoft, Google* und *IBM* angeboten. Ein Vorläufer ist das Grid-Computing, bei dem Rechenleistung aus der Steckdose angeboten wird.

Ausgelagert werden können beispielsweise Rechenleistung und Speicherplatz, um Spitzenbedarf auf Abruf zeitnah und kostengünstig abzudecken. Es können auch (standardisierte) Software zur Nutzung angeboten werden, Plattformen wie etwa Programmierumgebungen oder die Übernahme von Geschäftsprozessen, beispielsweise das Management von Kundenbeziehungen.

Es liegt im Wesen der Cloud, dass ein Anbieter auf andere, auch in der Wolke liegende, zurückgreift, wenn seine Kapazitäten nicht ausreichen. Bezahlt wird neben einer Grundgebühr nur die jeweils in Anspruch genommene Leistung, ohne dass teure Hardware gebraucht wird. So vernünftig die Geschäftsmodelle erscheinen, ergeben sich im Detail nicht unbedeutende Probleme technischer, kaufmännischer und juristischer Art, vor allem hinsichtlich der Vertraulichkeit und Sicherheit der übermittelten Daten. Schwierigkeiten ergeben sich auch bei der Archivierung, wie sie nach finanzgesetzlichen Bestimmungen vorgeschrieben ist. Backups sind nur schwer durchzusetzen. Auf andere Systeme umzusteigen, ist teuer. Der Kunde weiß nicht, wo seine Daten liegen. Zwar wäre eine räumliche Einschränkung durch Vertrag möglich, doch sind die AGBs der großen Anbieter in der Regel so gestaltet, dass der Gerichtsstand im Ausland liegt, österreichisches Recht nicht zur Anwendung kommt und zudem weitgehende Haftungsausschlüsse als vereinbart gelten. Abweichende vertragliche Regelungen werden nicht akzeptiert („Take it or leave it").

Daten nur verschlüsselt oder unter einem Pseudonym zu übermitteln oder zu speichern, ist nur vermeintlich ein Ausweg. Dr. Thilo Weichert, Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, wies darauf hin, dass in manchen Staaten ein legales Zugriffsrecht innerstaatlicher Behörden auf Daten besteht, etwa zur Strafverfolgung, für die Finanzbehörden oder für Geheimdienste zur Wirtschaftsspionage.

In vielen Staaten sind Dienstleister zur Herausgabe der Schlüssel verpflichtet. Und selbst bei hohem Standard des Datenschutzes kann illegaler Zugriff nicht ausgeschlossen werden – mit allen daraus resultierenden Folgen, die ein Unternehmen existenziell bedrohen können. Bei Auftragsdatenverarbeitung auf hoher See (offshore) fällt jegliche Kontrolle weg. Die Lösung sieht Weichert im Wesentlichen darin, dass Transparenz über die „in der Wolke" ablaufenden Datenverarbeitungen geschaffen wird und dass von einer vertrauenswürdigen, unabhängigen Stelle die Sicherheit der Vorgänge zertifiziert wird und es zu einer Art Gütesiegel für Cloud-

Fotos: Kurt Hickisch

Anbieter kommt („trusted and trustworthy clouds“). Zu erarbeiten seien noch Datenschutzstandards, verbindliche Unternehmensregeln, Auditierungsverfahren und allenfalls internationale Abkommen. Aus datenschutzrechtlichen Aspekten seien Clouds außerhalb des EWR-Raumes generell unzulässig.

Behavioral Advertising. Wie kann Werbung maßgeschneidert zum Kunden gebracht werden? „Cookies machen es möglich“, erläuterte Rechtsanwalt Dr. Rainer Knyrim. In Datenbanken, die die Webbrowser zur Verfügung stellen, können beim Nutzer von besuchten Websites Informationen in Form einer kleinen Datei hinterlegt werden, die es ermöglichen, diese Websites wieder zu besuchen, ohne die zu ihnen führenden Einstellungen erneut vornehmen zu müssen.

Die Speicherung von Informationen oder den Zugriff auf Informationen, die im Endgerät eines Teilnehmers oder Nutzers gespeichert sind (Cookies), ist nach Art 5 Abs. 3 letzter Satz der Datenschutz-Richtlinie für elektronische Kommunikation (DS-RL-eK, 2002/58/EG) bzw., wortgleich, nach § 96 Abs. 3 dritter Satz TKG 2003 zulässig, wenn der alleinige Zweck die Durchführung oder Erleichterung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder, soweit dies unbedingt erforderlich ist, um einen vom Teilnehmer oder Nutzer ausdrücklich gewünschten Dienst der Informationsgesellschaft zur Verfügung zu stellen. Darüber hinaus ist der Anbieter verpflichtet, den Teilnehmer oder Benutzer darüber zu informieren, welche personenbezogenen Daten er ermitteln, verarbeiten und übermitteln wird, auf welcher Rechtsgrundlage und für welche Zwecke dies erfolgt

Rainer Knyrim: „Gespeicherte Cookies machen maßgeschneiderte Werbung möglich.“

Thilo Weichert: „Selbst bei hohem Datenschutzstandard kann illegaler Zugriff nicht ausgeschlossen werden.“

und für wie lange die Daten gespeichert werden. Diese Information hat auch auf das Recht hinzuweisen, die Verarbeitung zu verweigern (§ 96 Abs. 3 TKG).

Die Cookies werden allein vom Nutzer (Client) verwaltet. Er hat es in der Hand, die Speicherung zur Gänze oder beschränkt zuzulassen oder die Cookies zu löschen. Werden sie am Rechner belassen, ergibt sich in Form einer Such-Historie eine Auflistung der besuchten Websites. Bei Bestehen der Möglichkeit, sie umfassend von außen auszulesen – etwa, weil Suchmaschinen benützt wurden – ergibt sich bei der Auswertung ein Profil über die Vorlieben des Users und damit die Grundlage für eine verhaltensorientierte Werbung. Benützt er wiederum die Suchmaschine, erhält er die für ihn passende Werbung mitgeliefert.

Das hat, wie Knyrim zu bedenken gab, Auswirkungen auf die herkömmliche Werbelandschaft durch Zeitungen, Radio und TV, die nicht so zielgenau den potenziellen Kunden erreichen, und die in weiterer Folge mit dem Verlust von Einnahmen aus der Werbung werden rechnen müssen. Ferner ergeben sich datenschutzrechtliche Probleme: Wird durch die Fülle an vorliegenden Informationen eine Person bereits bestimmbar, sodass die über Cookies gewonnenen Daten letztlich dem Datenschutz unterliegen. Das Arbeitspapier (WP) 136 der Art. 29 Datenschutzgruppe vom 20. Juli 2007 setzt für die Identifizierbarkeit einer Person nicht mehr die Kenntnis ihres Namens voraus. Sie ist bestimmbar dann, wenn sie einem oder mehreren spezifischen Elementen zugeordnet werden kann, die Ausdruck ihrer psychischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind. Nach einem auf diesem Arbeitspapier aufbauenden Gutachten der französischen Datenschutzbehörde CNIL vom 5. Februar 2009 liegen in einem solchen Fall personenbezogene Daten vor. CNIL fordert daher eine klare Information der Internetnutzer insbesondere über den Zweck der Cookies, und ein Zustimmungs- und Widerrufsrecht, wenn sie für verhaltensorientierte Werbung ausgewertet werden.

Website-Analyse. Für die Betreiber von Websites ist es von Interesse, Näheres über ihre Besucher zu erfahren, etwa, um den Webauftritt zu verbessern; zu überprüfen, wie wirksam Werbemittel und Marketingaktionen sind; welche Suchmaschinen und welche Suchbegriffe sie verwendet haben, welche Subsites sie wie oft und wie lange aufgesucht haben oder woher die Besucher kommen. Tools hiefür sind unter anderem *Piwik (www.piwik.org)* oder *Google Analytics (www.google.com/analytics)*. Eingesetzt werden unter anderem die Analyse von Cookies und die Auswertung von Logfiles.

Logfiles sind Verkehrsdaten im Sinne des § 99 Abs. 1 TKG, dürfen somit außer in den gesetzlich geregelten Fällen nicht gespeichert werden und sind vom Betreiber nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren. Allerdings darf der Betreiber mit Zustimmung des Teilnehmers die Daten zur Vermarktung für Zwecke der eigenen Telekommunikationsdienste oder für die Bereitstellung von Diensten mit Zusatznutzen verwenden (§ 99 Abs. 4 letzter Satz TKG).

Wie bei Cookies hängt die Auswertung von Logfiles von der (jederzeit widerrufbaren) Zustimmung des Teilnehmers ab. Die Gültigkeit dieser Zustimmung ist nach der Judikatur des OGH aber an strenge Voraussetzungen gebunden. So müssen die Datenarten taxativ bezeichnet und der Übermittlungsempfänger exakt benannt sowie der Zweck genau beschrieben werden, mit dem ausdrücklichen Hinweis auf den jederzeit möglichen schriftlichen Widerruf der Zustimmung. In formeller Hinsicht dürfen die Zustimmungserklärungen nicht in AGBs versteckt, sondern müssen von diesen deutlich getrennt werden, müssen deutlich lesbar und hervorgehoben sein und müssen gesondert unterschrieben bzw. auf Websites, angeklickt werden. Diesen datenschutzrechtlichen Anforderungen scheinen derzeit verwendete Analyse-Tools nicht gerecht zu werden. *Kurt Hickisch*

FOTO: KURT HICKISCH