

## 10. Kapitel: Zusammenfassung der Ergebnisse bezüglich der Auswirkungen des Einsatzes von Content-Identification-Technologien auf die Haftung von Web 2.0-Diensten

Durch das Web 2.0 entsteht nunmehr ein weiteres Dilemma für die Rechtsinhaber: einerseits bieten Web 2.0-Dienste den Nutzern vielfältige Möglichkeiten, Urheberrechte zu verletzen. Andererseits stellen diese Dienste ein extrem effektives Marketing- und Verbreitungsinstrument dar, das es den Rechtsinhabern ermöglicht, die Aufmerksamkeit der breiten Öffentlichkeit auf ein urheberrechtlich geschütztes Multimediawerk zu lenken und hierdurch Kommerzialisierungsmöglichkeiten zu eröffnen. Insoweit bieten vor allem werbefinanzierte Geschäftsmodelle, auf denen vor allem soziale Netzwerke und Videoplattformen zumeist basieren, großes Wachstumspotential. Der technische Fortschritt im Bereich der Content-Identification-Technologien eröffnet zudem die Möglichkeit, urheberrechtlich geschützte Multimediawerke auf Web 2.0-Diensten zu identifizieren, zu löschen oder durch die automatische Zuschaltung von Werbung kommerziell fruchtbar zu machen. Durch diese ständig fortentwickelten und verbesserten Technologien wird es somit möglich, die Verbreitung und Verfügbarmachung von digitalen Multimediawerken im Internet besser zu kontrollieren und zu steuern.

Damit werden jedoch gleichzeitig die Haftungsbeschränkungen für Host-Provider und damit der zweite wichtige Bereich von Gesetzgebungsakten, die speziell angesichts der Herausforderungen des digitalen Zeitalters, insbesondere des Internets, in den USA und im deutsch-europäischen Rechtskreis geschaffen wurden, auf den Prüfstein gestellt. Die im Rahmen der vorliegenden Arbeit durchgeführte Analyse hat gezeigt, dass gesetzgeberische Maßnahmen, die als Antwort auf eine spezifische technische Neuentwicklung erfolgen, ein hohes Risiko laufen, daran zu scheitern, dass sie zukünftige Entwicklungen, durch die solche technischen Errungenschaften regelmäßig modifiziert und verändert werden, mangels juristischer Evolutionselastizitäten nicht adäquat berücksichtigen können. Die Haftungsbeschränkungen wurden vor dem Hintergrund eingeführt, dass man die Haftungsrisiken der ISPs für Rechtsverletzungen, die Nutzer innerhalb ihrer Dienste begehen, begrenzen wollte, weil sie diese Rechtsverletzungen einerseits nicht kontrollieren konnten und andererseits ihre Dienstleistungen als wichtig für die Fortentwicklung des Internets und des E-Commerce erachtet wurden. Allerdings sehen weder der US-amerikanische noch der deutsch-europäische Ansatz zur Beschränkung der Haftung von ISPs eine adäquate, effektive Reaktionsmöglichkeit für den Fall vor, dass den ISPs die Kontrolle des innerhalb ihrer Dienste abgewickelten Datenverkehrs und damit der Rechtsverletzungen der Nutzer nachträglich möglich wird.

In den USA läuft daher gegenwärtig ein ISP, der Content-Identification-Technologien einsetzt, Gefahr, deswegen den Schutz der Haftungsbeschränkung zu verlieren, da er damit die Kontrolle über rechtswidriges Nutzerverhalten erhält. Damit befindet er sich jedoch in einer schlechteren Position als sein Konkurrent, der keine solche Technologie einsetzt, und der wegen des Ausschlusses allgemeiner proaktiver Überwachungspflichten auch nicht dazu verpflichtet werden kann, eine solche Technologie einzusetzen. Eine solche Verpflichtung wäre einzig möglich, sofern die Technologie eine STM darstellt. Aufgrund der misslungenen Definition von STMs ist jedoch weitgehend sicher, dass diese niemals zur Entstehung gelangen werden. Dieses unbefriedigende Ergebnis wird lediglich durch das Notice&Takedown-Verfahren weitgehend entschärft, wodurch die eigentliche rechtliche Auseinandersetzung auf die Ebene des Rechtsinhabers und des Nutzer eingegrenzt wird, aber dafür dem Rechtsinhaber ein klar geregeltes und effektives Verfahren zur Verfügung gestellt wird, um Rechtsverletzungen zügig durch einen ISP beseitigen zu lassen.

Auch nach deutsch-europäischem Recht besteht keine Handhabe, um auf die veränderten Kontrollmöglichkeiten der ISPs adäquat zu reagieren. Zwar ist nach den Erwägungsgründen der E-Commerce-Richtlinie die Kontrolle der ISPs über rechtswidrige Inhalte der Hauptanknüpfungspunkt für dessen Haftung, jedoch findet diese grundlegende Annahme keinen Widerhall in den eigentlichen Regelungen der Haftungsbeschränkungen. Zudem sind auch nach deutsch-europäischem Recht proaktive Überwachungspflichten ausdrücklich ausgeschlossen, so dass auch aus diesem Grund die Verpflichtung des ISPs, Content-Identification-Technologien zum Schutz von Urheberrechten einzusetzen, ausscheidet. In Deutschland wird diese unbefriedigende Situation allein dadurch ausgeglichen, dass sich der BGH standhaft weigert, die Haftungsbeschränkungen auch auf die Störerhaftung anzuwenden und den gesetzlich ausdrücklich festgehaltenen Ausschluss allgemeiner Überwachungspflichten bei der Bestimmung des Umfangs der dem ISP obliegenden Prüfpflichten zu berücksichtigen. Auf diese Weise bleibt es – allerdings um den Preis des Verlusts der Rechtssicherheit betreffend die Voraussetzungen der Haftung von ISPs – möglich, Einzelfallabwägungen vorzunehmen, in deren Rahmen insbesondere auch die einem ISP tatsächlich zur Verfügung stehenden technischen Kontrollmöglichkeiten berücksichtigt werden können.

## 11. Kapitel: Fazit

„The answer to the machine is not in the machine.“ So lassen sich die Ergebnisse des ersten Schwerpunkts dieser Arbeit auf den Punkt bringen. Dies bedeutet, dass auch im Zeitalter der Digitalisierung den Marktteilnehmern auf dem Markt für Multimediawerke nicht erspart bleibt, sich auf die neuen Gegebenheiten des Marktes einzustellen und diese anzuerkennen. Denn die Entwicklung in der Musikindustrie ist ein eindrucksvoller Beleg dafür, dass es nicht möglich ist, die neuen Vervielfältigungs- und Verbreitungsmöglichkeiten durch technische Schutzmaßnahmen effektiv zu bekämpfen und zu eliminieren, sondern diese ein unabänderliches Faktum darstellen, an dem es nichts mehr zu Rütteln gibt. Auch der spezielle Schutz, den das internationale und nationale Recht solchen technischen Schutzmaßnahmen gewährt, vermag hieran nichts zu ändern. Es gilt somit, die „normative Kraft des Faktischen“ anzuerkennen und die neuen Gegebenheiten als Chance für neue Geschäftsfelder und Wachstumspotentiale zu begreifen. Der Erfolg solcher zukünftiger Geschäftsmodelle wird davon abhängen, die neuen technischen Umstände und die dadurch veränderten Erwartungen der Nutzer mit den berechtigten Interessen der Rechtsinhaber an der wirtschaftlichen Nutzbarmachung ihrer Rechtspositionen in Einklang zu bringen. Dass dies kein Ding der Unmöglichkeit ist, zeigt sich wiederum an der Musikindustrie, deren Hinwendung zu neuen Geschäftsfeldern, wie z.B. den DRM-freien Vertrieb von Musikdownloads über viele verschiedene Anbieter, berechtigten Anlass zu der Hoffnung gibt, dass in diesem Industriezweig die Trendwende hin zu neuem Wachstum bald Realität werden wird.

Weiterhin zeigen die Ergebnisse des zweiten Schwerpunkts dieser Arbeit, dass eine Haftungsfreizeichnung von bestimmten Marktteilnehmern allein auf der Grundlage sich ständig fortentwickelnder und sich überholender technologischer Gegebenheiten wenig interessengerecht ist. Viel zu groß ist die Gefahr, dass kurze Zeit später die Gründe, die eine besondere Schutzwürdigkeit der privilegierten Marktteilnehmer ursprünglich zu rechtfertigen schienen, obsolet werden. Tritt dieser Fall ein, führt dies jedoch zu einem Ungleichgewicht der Interessen aller von der Haftungsbeschränkung Betroffenen, in diesem Fall derjenigen, deren Rechte verletzt werden, und die dann keine Möglichkeit haben, gegen diese Rechtsverletzungen durch Inanspruchnahme der ISPs effektiv vorzugehen. Das Ergebnis ist somit eine gleichsam „institutionalisierte“ partielle Rechtslosigkeit der Betroffenen. Wenn dennoch solche Haftungsbeschränkungen geschaffen werden sollen, gilt es darauf zu achten, in den entsprechenden gesetzlichen Regelungen den Schutzzweck und die speziellen Umstände, die die Haftungsbeschränkung im Zeitpunkt ihrer Schaffung zu rechtfertigen scheinen, festzuhalten. Auch muss sichergestellt werden, dass die Regelungen ausreichend darauf reagieren können, wenn