Rechtsguide der Forschungsstelle Recht im DFN

A. Inhaltsverzeichnis

B. Rechtsguide

Die folgenden Erläuterungen dienen zur ersten Orientierung über wichtige Rechtsfragen, die im Betrieb der Rechenzentren beim Datentransfer in Netzen und der Übermittlung von E-Mails eine Rolle spielen.

I. Das Benutzungsverhältnis

1. Einführung

Die Bereitstellung von Diensten der Informations- und Kommunikationstechnik(IuK-Dienste) an Hochschulen und Forschungseinrichtungen kann im Nutzungsverhältnis eine Vielzahl von Fragen aufwerfen, für die ein Regelungsbedürfnis besteht. So besteht ein Bedürfnis zur Aufstellung grundlegender Regeln, die eine möglichst störungsfreie, ungehinderte und sichere Nutzung der Kommunikations- und Datenverarbeitungsstruktur gewährleisten. In diesem Zusammenhang stellen sich beispielsweise die Fragen, welche grundlegenden Rechte und Pflichten dem Rechenzentrum und den zugelassenen Nutzern zukommen, unter welchen Voraussetzungen Nutzer zugelassen oder von der Nutzung ausgeschlossen werden können und welche Zuständigkeiten innerhalb der Einrichtung bestehen. Absehbare Probleme, die in der täglichen Praxis der Erbringung von IuK-Diensten auftauchen können, werden bei kommerziellen Anbietern im Rahmen des Vertragsverhältnisses mit dem Kunden üblicherweise durch Allgemeine Geschäftsbedingungen (AGB) geregelt. Im Arbeitsverhältnis können Regelungen durch Dienstvereinbarungen getroffen werden. Insbesondere bei Hochschulen gestaltet sich dies meist schwierig er, da die Erbringung von IuK-Diensten für die Nutzer oft im Zusammenhang mit der Wahrnehmung der Aufgaben der Einrichtung als Körperschaft des Öffentlichen Rechts erfolgt. In diesen Fällen besteht das Bedürfnis der Ausgestaltung der meist öffentlich-rechtlich zu beurteilenden Benutzungsverhältnisse, was in der Regel durch eine Benutzungsordnung erfolgt (Vergleiche zum öffentlich-rechtlichen Nutzungsverhältnis: Gurlit in: Ehlers/Pünder, Allgemeines Verwaltungsrecht, 15. Aufl., Berlin 2016, § 35 33 ff.).

2. Benutzungsordnung zur Ausgestaltung des Benutzerverhältnisses

Benutzungsordnungen dienen der inhaltlichen Ausgestaltung des öffentlich-rechtlichen Nutzungsverhältnisses zwischen der Einrichtung (beziehungsweise dem Rechenzentrum als unselbständige Verwaltungseinheit) und dem Nutzer, der die Dienste des Rechenzentrums in Anspruch nimmt. Sie erlangt somit insbesondere für Benutzungsverhältnisse in Hochschulen Bedeutung. Als verbindliches Regelungswerk für das Nutzungsverhältnis sollten die Benutzungsordnungen alle Rechte und Pflichten der Beteiligten, Zuständigkeiten und insbesondere die Ermächtigungsgrundlagen für hoheitliche Sanktionen, wie etwa den Ausschluss eines Nutzers wegen missbräuchlicher Nutzung, beinhalten. Benutzungsordnungen, Netzordnungen, Nutzungsrichtlinien etc. können grds. entweder als Satzungen oder Ordnungen im Sinne der Hochschulgesetze durch den Senat/Rektor der Hochschule oder als Verwaltungsnormen in Form sogenannte Allgemeinverfügungen durch den Leiter des Rechenzentrums erlassen werden. Für die rechtliche Einordnung als Rechtsnorm oder Verwaltungsnorm ist die Benennung des Regelungswerks als „Benutzungsordnung“, „Nutzungsrichtlinien“ etc. unerheblich. Die rechtliche Bewertung richtet sich ausschließlich nach der Rechtsqualität der aufgestellten Nutzungsregeln.

a) Als Rechtsnorm

Als Satzung beziehungsweise förmliche Ordnungen erlassene Benutzungsordnungen sind verbindliche Rechtsvorschriften, die die Einrichtung als verwaltungsrechtliche Personalkörperschaft des öffentlichen Rechts kraft ihrer Rechtssetzungskompetenz für Selbstverwaltungsaufgaben auf der

Grundlage des jeweiligen Landeshochschulgesetzes erlassen kann. Sie binden alle Angehörigen der Hochschule und sonstigen Anstaltsnutzer, die aufgrund einer (öffentlich-rechtlichen) Zulassung die Dienste des Rechenzentrums in Anspruch nehmen. In einer als Satzung (= Rechtsnorm) erlassenen Benutzungsordnung können grundsätzlich alle Fragen des Nutzungsverhältnisses, insbesondere auch der Ausschluss einzelner Nutzer wegen missbräuchlicher oder rechtswidriger Nutzung, geregelt werden. Allerdings setzt der Erlass der Benutzungsordnung als Satzung die Beachtung der einschlägigen Zuständigkeits-, Verfahrens- und Formvorschriften des hierzu ermächtigenden Gesetzes (Landeshochschulgesetze) voraus. So ist in der Regel nur der Senat oder Verwaltungsrat der Hochschule für den Erlass einer Universitätssatzung zuständig. Überdies muss eine Satzung als amtliche Bekanntmachung der Hochschule veröffentlicht werden.

b) Als Verwaltungsnorm

Die Benutzungsordnung kann auch als Verwaltungsakt in Form einer Allgemeinverfügung durch den Leiter des Rechenzentrums erlassen werden. Hierzu muss jedoch eine entsprechende Ermächtigungsgrundlage in einer höherrangigen, allgemeinen Nutzungsordnung enthalten sein, die ihrerseits als Satzung (= Rechtsnorm) ergehen muss. Nach dieser Ermächtigungsgrundlage richtet sich auch der Inhalt und Umfang einer Ordnung, die vom Leiter des Rechenzentrums als Verwaltungsakt erlassen werden kann. Im Übrigen ergibt sich die Befugnis zur Regelung interner Ablauf- und Organisationsfragen auch aus der Organisations- und Anstaltsgewalt des Leiters des Universitätsrechenzentrums. Allerdings dürfen entsprechende Nutzungsordnungen lediglich interne Ordnungsfragen des „Anstaltsalltags“ enthalten, also z. B. technisch-organisatorische Vorgaben für einen störungsfreien Betrieb des Rechnernetzes. Diese Einschränkung ergibt sich aus der sogenannten Wesentlichkeitstheorie (Dazu grundlegend BVerfGE 33, 303 (303 ff). zur Zulassungsbeschränkung an Hochschulen). Hiernach müssen hoheitliche Regelungen, die sich auf die Verwirklichung von Grundrechten auswirken oder den Status des Benutzers im sogenannten Grundverhältnis berühren, als Rechtsnormen, d. h. zumindest als Satzungen, ergehen. „Wesentliche“ Eingriffe, wie z. B. die Nichtzulassung eines Studierenden oder der Ausschluss von der Nutzung, können folglich nicht durch eine Benutzungsordnung geregelt werden, die lediglich als Verwaltungsakt in Form einer Allgemeinverfügung durch den Leiter des Rechenzentrums erlassen wird. Solche wesentlichen Eingriffe betreffen nicht nur interne Ordnungsfragen zur Gewährleistung eines ordnungsgemäßen Netzbetriebs, sondern sie berühren grundsätzliche Bestandsfragen des Nutzungsverhältnisses. Ist z. B. ein Studierender im Rahmen seines Studiums auf den Informationsaustausch über das Internet angewiesen, kann unter anderem die Berufsfreiheit aus Art. 12 Grundgesetz (GG) betroffen sein. Ähnliches gilt für wissenschaftliche Mitarbeiter im Hinblick auf die Wissenschafts- und Forschungsfreiheit. Die Benutzungsordnung in Gestalt einer Satzung (= Rechtsnorm) ist somit klar vorzugswürdig.

3. Wichtige Einzelaspekte zum Benutzungsverhältnis

Im Folgenden werden einige wichtige Einzelaspekte zum Benutzungsverhältnis übergreifend dargestellt.

a) Zulassung zur Nutzung

Die Zulassung einer natürlichen Person zur Nutzung der Dienste führt zur individuellen Berechtigung zur Nutzung der IuK-Einrichtungen der jeweiligen Einrichtung und damit in der Regel zugleich zum Zugang zum Wissenschaftsnetz. In öffentlich-rechtlichen Benutzungsverhältnissen erfolgt die ebenfalls als öffentlich-rechtlich zu qualifizierende Zulassungsentscheidung in der Regel aufgrund der in der jeweiligen Benutzungsordnung enthaltenen Ermächtigung durch einen Verwaltungsakt, wenn

die Zulassungsvoraussetzungen vorliegen. Hierbei ist gegebenenfalls in der Interessenabwägung zu beachten, dass die Nichtzulassung im Einzelfall zu Grundrechtsbeeinträchtigungen führen kann. So kann die Berufsfreiheit eines Studierenden aus Art. 12 GG betroffen sein, wenn er im Rahmen seines Studiums auf den Informationsaustausch über das Internet angewiesen ist. Ebenfalls kann ein wissenschaftlicher Mitarbeiter in seiner Wissenschafts- und Forschungsfreiheit betroffen sein, wenn er für wissenschaftliche Zwecke auf das Rechnernetz zugreifen muss.

b) Privatnutzung der IuK-Dienste

Die Zulassung zur Nutzung in Hochschulen und Wissenschaftseinrichtungen erfolgt in erster Linie zu wissenschaftlichen Zwecken in Forschung, Lehre und Studium, für Zwecke der Bibliothek und der einrichtungsinternen Verwaltung, Aus- und Weiterbildung sowie zur Erfüllung sonstiger Aufgaben der jeweiligen Einrichtung. An vielen Einrichtungen stellt sich die Frage, ob und inwieweit auch eine private Nutzung in geringfügigem Ausmaß durch die Berechtigten zugelassen werden soll. Namentlich geht es darum, ob die Berechtigten über die einrichtungsbezogene Nutzung des Zugangs hinaus private E-Mails versenden oder aus privaten Interessen Seiten im Internet aufrufen dürfen. Unter Umständen kann die Erlaubnis einer geringfügigen Privatnutzung auch dann angenommen werden, wenn eine ausdrückliche Regelung hierzu nicht existiert und sich die private Nutzungsmöglichkeit für die Verantwortlichen erkennbar in der Einrichtung dauerhaft eingebürgert hat. Soll die private Nutzung prinzipiell ausgeschlossen werden, empfiehlt sich von daher eine ausdrückliche und klare Regelung gegenüber den Nutzern der Einrichtungen, dass die private Nutzung nicht erlaubt ist. Auch im Hinblick auf eine mögliche Beschränkung der erlaubten Privatnutzung empfehlen sich ausdrückliche Vorgaben. Ein Hauptargument für den gänzlichen Ausschluss der Privatnutzung liegt in den dann nicht zu beachtenden Vorgaben des Fernmeldegeheimnisses und des IuK-spezifischen Datenschutzes. Zwar überwiegt in der Regel auch bei einer zugelassenen Privatnutzung die einrichtungsbezogene Nutzung der Dienste deutlich. Diese lässt sich allerdings kaum von der privaten Kommunikation trennen, so dass die Einrichtung umfassend die Vorgaben des Fernmeldegeheimnisses und des Datenschutzes zu beachten hat. Praktisch hat die Einrichtung damit ähnliche Vorgaben bei Erhebung und Verwendung von Daten zu beachten wie ein kommerzieller Provider. Relevant wird dies beispielsweise im Hinblick auf die Einführung von Filterkriterien beim einrichtungsinternen Maildienst. Andererseits sprechen auch Gründe für die Zulassung einer geringfügigen privaten Nutzung. Dies gilt insbesondere im Hinblick auf die Studierenden an Hochschulen, die über das Diensteangebot der Rechenzentren im Rahmen ihrer Ausbildung oft erstmalig ernsthaft mit dem Medium Internet in Berührung kommen.

c) Nutzungsausschluss bei Pflichtverletzung

In auf die Erbringung von Kommunikationsdienstleistungen gerichteten Vertragsverhältnissen erfolgt der Ausschluss des Nutzers in der Regel durch eine außerordentliche Beendigung des Vertrages aufgrund erheblicher Verstöße gegen wesentliche Vertragspflichten. In öffentlich-rechtlichen Benutzungsverhältnissen, in denen die Nutzer in der Regel durch eine öffentlich-rechtliche Verwaltungsentscheidung (siehe oben) zur Nutzung zugelassen werden, stellt sich dies etwas anders dar. Ebenso wie die Zulassung zur Nutzung stellt auch der Ausschluss in der Regel eine öffentlich-rechtliche Verwaltungsentscheidung dar. Diese erfolgt aufgrund einer ermächtigenden Norm in der meist als Satzung erlassenen Benutzungsordnung (siehe oben), in der die Zuständigkeit und die zum Ausschluss berechtigenden Gründe genannt werden. Gründe können beispielsweise die Nutzung außerhalb der Zweckbestimmung (z. B. kommerzielle Nutzung) oder schwerwiegende Verletzungen gegen die in der Ordnung bestimmten Nutzerpflichten sein. In Bezug auf das Verfahren ist zu

beachten, dass einem eingreifenden Verwaltungsakt regelmäßig eine Anhörung des Beteiligten vorausgehen muss. Dies ergibt sich aus § 28 Verwaltungsverfahrensgesetz (VwVfG) und den entsprechenden landesrechtlichen Vorgaben zum Verwaltungsverfahren. Materiell sind auch hier wie bei der Zulassungsentscheidung mögliche Folgen für die Grundrechtsausübung insbesondere Studierender (Art. 12 GG) und wissenschaftlicher Mitarbeiter (Art. 5 Abs. 3 GG) zu beachten. So ist es beispielsweise kaum vorstellbar, dass ein Studierender, der für sein Studium auf den Netzzugang angewiesen ist, wegen eines nur unerheblichen Verstoßes gegen die Benutzungsordnung gänzlich von der Nutzung ausgeschlossen wird. Abgesehen davon ist außer in Fällen sehr schwerwiegender Verstöße aus Gründen der Verhältnismäßigkeit geboten, eine vorherige Abmahnung des betreffenden Nutzers vorzusehen. Aus den gleichen Gründen sollte zudem immer die Möglichkeit eines nur teilweisen Ausschlusses bezogen auf einzelne Netzdienste geprüft werden.

II. Datentransfer in Netzen und Übermittlung von E-Mails

1. Einführung

Das folgende Kapitel des Rechtsguides widmet sich wichtigen Rechtsfragen im Zusammenhang mit der Tätigkeit der Datenübermittlung durch die Rechenzentren. Der Schwerpunkt liegt hierbei auf den Problemen im Zusammenhang mit der Bereitstellung des Internetzugangs (Access-Provider) und dem Angebot der Übermittlung von E-Mails (Mail-Provider) für die Nutzer in Hochschulen und Forschungseinrichtungen. Entsprechend der nach den jeweiligen Tätigkeiten differenzierenden Darstellung werden die Rechtsfragen im Zusammenhang mit Inhalten auf eigenen Webseiten und der Zurverfügungstellung von Speicherplatz für fremde Angebote in den folgenden Kapiteln des Rechtsguides dargestellt.

2. Haftung

Von im Internet oder per E-Mail übermittelten Inhalten können zahlreiche Rechtsverletzungen ausgehen. In Betracht kommen z. B. Verletzungen von Urheber- und Markenrechten und Verstöße gegen Strafgesetze. Das besondere Gefahrenpotential liegt darin, dass über das Internet jedermann inhaltlich kaum kontrollierbar Daten von Servern abrufen oder selbst übermitteln kann. Der Zugang zum Internet ermöglicht somit auch die Verbreitung und den Empfang von Informationen in rechtsverletzender Weise. Praktische Beispiele sind die Verbreitung urheberrechtlich geschützter Werke durch E-Mail, FTP-Server, Filesharing oder etwa die Einstellung beleidigender Kommentare in ein Meinungsforum. Der Netzzugang ist somit Ausgangspunkt für legale und illegale Kommunikation über das Internet durch die angeschlossenen Nutzer. Für die Rechenzentren stellt sich dabei die sehr wichtige Frage, ob und inwieweit aufgrund des zur Verfügung gestellten Netzzugangs eine Verantwortlichkeit für durch Nutzer begangene und somit fremde Rechtsverletzungen bestehen kann. Anknüpfungspunkt für eine mögliche Mitverantwortlichkeit ist die Zurverfügungstellung des Netzzugangs. Gegen eine Mitverantwortlichkeit spricht die unmittelbare Begehung durch den Nutzer und die aus rechtlichen und tatsächlichen Gründen fehlende lückenlose Kontrollmöglichkeit durch den Zugangsanbieter.

a) Haftungserleichterung durch §§ 8, 9 Telemediengesetz (TMG)

Diese Sachlage hat der Gesetzgeber erkannt und deshalb Haftungsprivilegierungen in den §§ 8, 9 Telemediengesetz (TMG) erlassen, die auf der europäischen E-Commerce-Richtlinie (RL 2000/31/EG) beruhen. Wenn Hochschulen und Forschungseinrichtungen ihren Angehörigen einen Netzzugang zur Verfügung stellen, gelten die Haftungserleichterungen auch für sie. Zugangsanbieter sind nach den genannten Vorschriften von einer Verantwortlichkeit für fremde rechtswidrige Informationen, die sie

in einem Kommunikationsnetz lediglich übermitteln, weitgehend befreit. Dies gilt nach § 9 TMG auch für den Fall einer zeitlich begrenzten Zwischenspeicherung, die lediglich einer effizienteren Übermittlung der Informationen dient, wobei weitere in § 9 TMG explizit aufgezählte spezifische Voraussetzungen erfüllt sein müssen.

Nach § 7 Abs. 1 TMG sind Diensteanbieter hingegen für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich. Die Haftungsprivilegierungen gelten damit nur für fremde Informationen. Fremd sind hierbei solche Informationen, die nicht der jeweiligen Einrichtung zuzurechnen sind, die also keine eigenen Informationen sind. Fremde Informationen sind beispielsweise die privaten E-Mails eines Mitarbeiters oder Daten, die aufgrund einer privaten Nutzung des einrichtungsinternen Internetzugangs übermittelt werden. Für solche Informationen ist der Zugangsvermittler nicht verantwortlich und somit grundsätzlich nicht haftbar zu machen. Dies gilt gemäß § 8 Abs. 1 S. 1 TMG jedoch nicht, wenn er die Übermittlung der fremden Informationen selbst veranlasst, wenn er den Adressaten der übermittelten Informationen selbst auswählt oder die übermittelten Informationen selbst auswählt oder verändert. Im Normalfall geschieht dies jedoch durch den Nutzer als Veranlasser der Datenübermittlung, während sich der Internetzugangsanbieter auf die Tätigkeit des inhaltsneutralen Datentransports beschränkt. Der Zugangsanbieter kann sich außerdem dann nicht auf seine Nichtverantwortlichkeit berufen, wenn er absichtlich mit einem der Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen (§ 8 Abs. 1 S. 2 TMG).

Stark umstritten ist jedoch die Frage, unter welchen Umständen ein Access-Provider doch für fremde Rechtsverletzungen in die Pflicht genommen werden kann, obwohl die genannten Voraussetzungen für die Haftungserleichterungen erfüllt sind und der Zugangsanbieter somit eigentlich nicht verantwortlich ist.

b) Pflicht zur Entfernung oder Sperrung von Informationen, § 7 Abs. 2 S. 2 TMG

Ausgangspunkt für die partielle Durchbrechung des Grundsatzes der Nichtverantwortlichkeit für fremde Inhalte ist § 7 Abs. 2 S. 2 TMG. Demnach bleiben Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach §§ 8, 9 TMG unberührt. Daraus wird gefolgert, dass der nicht verantwortliche Zugangsanbieter dennoch zur Entfernung oder Sperrung fremder rechtsverletzender Informationen verpflichtet sein kann, weshalb die Geltendmachung entsprechender Unterlassungsansprüche möglich sein soll. Praktische Bedeutung erlangt diese Vorschrift dadurch, dass der eigentliche Verursacher oftmals nicht ermittelt werden kann und somit der Provider die einzig greifbare Möglichkeit ist, andauernde oder wiederholte Rechtsverletzungen zu unterbinden.

Aus zivilrechtlicher Sicht kommt eine Inanspruchnahme des Access-Providers insbesondere zur Unterbindung andauernder oder weiterer Verletzungen von sogenannten absoluten, also gegenüber jedermann geltenden Rechten in Betracht, zu denen beispielsweise Urheberrechte und Markenrechte zählen. Grundlage eines möglichen Anspruchs des Verletzten ist die sogenannte Störerhaftung, die im Wege einer analogen Anwendung des § 1004 Abs. 1 Satz 2 Bürgerliches Gesetzbuch (BGB) einen Unterlassungsanspruch begründen kann. Dieser kann dann auf die Verhinderung beziehungsweise Erschwerung des Zugangs zu bestimmten Inhalten mithilfe von Netzsperren (z.B. DNS-, IP- oder URL-Sperren) gerichtet sein, wenn der Rechteinhaber zuvor angemessene Versuche unternommen hat, den unmittelbaren Rechtsverletzer zu ermitteln, dies aber nicht gelungen ist. Zu diesen angemessenen Ermittlungsversuchen gehört nach der

Rechtsprechung des Bundesgerichtshofs auch die Einschaltung der staatlichen Ermittlungsbehörden oder die Beauftragung eines Privatdetektivs. Die erforderliche Störereigenschaft kann demjenigen zukommen, der nur mittelbar an einer Rechtsverletzung beteiligt ist. Die mittelbare Beteiligung des Access-Providers besteht in der für die Verletzung mitursächlichen Bereitstellung des Internetzugangs. Um eine ausufernde Haftung der Provider zu vermeiden, fordert der BGH jedoch, dass der Dritte zumutbare Prüfpflichten verletzt haben muss. Dabei sind unter anderem die Größe des jeweiligen Zugangsanbieters und der erforderliche technische, administrative und personelle Aufwand zur Umsetzung von Netzsperren zu berücksichtigen.

Betreiber von WLANs sind gemäß § 8 Abs. 3 TMG ebenfalls von dieser Privilegierung erfasst. Sie können aber durch eine gerichtliche Anordnung dazu verpflichtet werden, den Zugang zu ihrem WLAN durch ein Passwort zu beschränken und dieses nur Nutzern zur Verfügung zu stellen, die sich ihnen gegenüber identifizieren, sodass eine anonyme Nutzung ausgeschlossen ist.

In diesem Zusammenhang ist jedoch hervorzuheben, dass Diensteanbieter nach § 7 Abs. 2 S. 1 TMG nicht allgemein verpflichtet sind, die von ihnen übermittelten oder gespeicherten fremden Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Für anlassbezogene Prüfpflichten dagegen ist die entscheidende Frage stets, ob die begehrte Unterbindung weiterer Rechtsverletzungen zumutbar ist. Dies kann mit guten Gründen bezweifelt werden, bedarf aber in jedem Fall einer Abwägung aller Interessen im Einzelfall. Sollte sich im Nachhinein der Verdacht einer Rechtsverletzung als unbegründet herausstellen, kann der Provider von seinem Kunden gegebenenfalls wegen Vertragsverletzung in Anspruch genommen werden. In Bezug auf eine Sperrung des Internetzugangs sind im Hochschulbereich und in Forschungseinrichtungen bei Maßnahmen gegen Wissenschaftler oder Studierende zudem die Wissenschaftsfreiheit aus Art. 5 Abs. 3 GG und die Berufsfreiheit aus Art. 12 GG in die Entscheidung über eine Sperrung einzubeziehen, was auch nicht ohne Auswirkung auf die Frage der Zumutbarkeit bleiben kann. Erleichtert werden können solche Entscheidungen durch eine ausdrückliche Regelung in der Benutzungsordnung, dass eine vorübergehende Sperrung bis zur Klärung der Rechtslage vorgenommen werden kann. Zu betonen ist, dass lediglich Unterlassungs- und Beseitigungsansprüche gegen mittelbar Verantwortliche geltend gemacht werden können, nicht jedoch Schadensersatzansprüche, da diesen die Haftungsprivilegierungen des Telemediengesetzes entgegenstehen. Daneben besteht für Access-Provider seit der Einführung des zivilrechtlichen Auskunftsanspruchs in § 101 UrhG eine Auskunftspflicht über die Identität eines Nutzers gegenüber Privaten, wie zum Beispiel Inhabern von Urheberrechten. Wird das Rechenzentrum auf Rechtsverletzungen (z. B. Urheberrecht) durch einen Nutzer hingewiesen und aufgefordert, dies durch Sperrung des Zugangs zu unterbinden, sollte der Vorgang so schnell wie möglich an das Justitiariat abgegeben werden.

c) Wer haftet?

(1) Zivilrechtliche Haftung

Soweit das Rechenzentrum für Rechtsverletzungen (mit-) verantwortlich ist, haftet grundsätzlich die Einrichtung/Hochschule beziehungsweise deren Rechtsträger als juristische Person. Dies gilt auch in Bezug auf Fachbereiche und Institute, die in der Regel keine eigene Rechtspersönlichkeit haben und somit als Diensteanbieter im Sinne von § 2 Satz 1 Nr. 1 TMG nicht in Betracht kommen. Mitarbeiter haften in der Regel nicht persönlich, soweit eine Rechtsverletzung in Ausübung ihrer Diensttätigkeit geschieht. Bei Beamten folgt dies aus den Grundsätzen der Amtshaftung gemäß Art. 34 GG;

Angestellte haben grundsätzlich einen Haftungsfreistellungsanspruch gegen den Arbeitgeber. Davon unberührt bleiben allerdings eventuelle Haftungsrückgriffe der Hochschule gegen den verantwortlichen Mitarbeiter aus dem Dienstverhältnis. Rückgriffe kommen in Betracht, wenn Dienstpflichten vorsätzlich oder in grobem Maß verletzt wurden und der Hochschule dadurch ein Schaden entstanden ist.

Soweit Aufgaben von Einrichtungen wahrgenommen werden, die keine organisatorischen Untergliederungen der Hochschulen sind, sondern selbständige juristische Personen des öffentlichen Rechts (wie z.B. Studierendenwerke), sind diese selbst und nicht etwa die Hochschule als Diensteanbieter im Sinne des § 2 Satz 1 Nr. 1 TMG anzusehen und können als solche haftbar gemacht werden.

(2) Strafrechtliche Verantwortlichkeit

Strafrechtlich können nur einzelne Personen persönlich verantwortlich sein, nicht die Hochschule oder das Studentenwerk als juristische Personen. Deshalb ist für jeden beteiligten Hochschulangehörigen individuell zu prüfen, ob er sämtliche Voraussetzungen eines Straftatbestandes selbst verwirklicht hat. Die Haftungsprivilegierungen des Telemediengesetzes finden aber auch hier Anwendung.

3. Verdacht auf Straftaten

Die Einrichtungen eines Rechenzentrums können zur Begehung verschiedener Straftaten missbraucht werden. In Betracht kommen z. B. Delikte wie das Ausspähen von Daten nach § 202a StGB, Computersabotage nach § 303b StGB oder Computerbetrug nach § 263a StGB, die Verbreitung rechtswidriger Inhalte oder die Verbreitung beziehungsweise Verschaffung von Kinderpornographie nach § 184b StGB. Besteht der Verdacht, dass ein Benutzer über die Einrichtungen des Rechenzentrums Straftaten begangen hat, so sollten keine Ermittlungen auf eigene Faust angestellt werden. Es sollten nur Beweise gesichert werden (Ausdruck und Speicherung der Dateien, Informierung anderer Mitarbeiter als Zeugen etc.), aber keine neuen Beweise eigenmächtig ermittelt werden. Stattdessen ist frühzeitig die Polizei oder Staatsanwaltschaft zu informieren, um gegebenenfalls Anzeige zu erstatten. Der weitere Verlauf des Ermittlungsverfahrens wird dann von der Staatsanwaltschaft bestimmt, die über die entsprechenden gesetzlichen Befugnisse für Ermittlungen verfügt.

a) Auskünfte an Strafverfolgungsbehörden

Es ist keine Seltenheit, dass Strafverfolgungsbehörden (hierzu zählen die Behörden der repressiven Strafverfolgung, wie z. B. die Staatsanwaltschaft und deren polizeilichen Hilfsbeamten; nicht umfasst sind die Polizeibehörden, sofern sie zur Gefahrenabwehr handeln) an Mitgliedsinstitutionen des DFN-Vereins herantreten, um von diesen Daten ihrer User aus der Online-Kommunikation zu erlangen. Die folgende Übersicht zeigt nur überblicksartig die Befugnisse der Strafverfolgungsbehörden und als Kehrseite die Auskunftsverpflichtung der Rechenzentren auf. Nach der Eingriffsintensität und den daran anknüpfenden formalen Voraussetzungen für ein Auskunftsersuchen der Strafverfolgungsbehörden ist zwischen Bestandsdaten, Verkehrsdaten und Inhalten der Kommunikation zu trennen.

(1) Inhalte der Kommunikation

Inhalte der Kommunikation sind diejenigen Daten, die jedenfalls dem Fernmeldegeheimnis unterliegen. Dies sind im Bereich der Online-Kommunikation vor allem Inhalte von E-Mails oder von

VoIP-Verbindungen. Wichtigste gesetzliche Grundlage für die Überwachung sind §§ 100a, 100b Strafprozessordnung (StPO). Neben hohen materiellen Anforderungen muss für die inhaltliche Telekommunikationsüberwachung in formeller Hinsicht eine gerichtliche Anordnung auf Antrag der Staatsanwaltschaft vorliegen. Nur bei Gefahr im Verzug kann die Anordnung auch direkt durch die Staatsanwaltschaft getroffen werden, wobei sie in diesem Fall innerhalb von drei Werktagen gerichtlich zu bestätigen ist. Die Anordnung bedarf in jedem Fall der Schriftform. Wird eine entsprechende schriftliche Anordnung vorgelegt, muss das Rechenzentrum die Überwachung ermöglichen und der Strafverfolgungsbehörde die erforderlichen Auskünfte unverzüglich erteilen.

(2) Verkehrsdaten

Verkehrsdaten sind Daten, die bei der Bereitstellung und Erbringung von Diensten erhoben werden und damit in einem unmittelbaren Zusammenhang mit einem konkreten Kommunikationsvorgang stehen. Hier sind in erster Linie Beginn und Ende von Internetverbindungen, besuchte Webseiten oder dynamisch vergebene IP-Adressen zu nennen. Wollen Strafverfolgungsbehörden solche Verkehrsdaten einholen, stellt der mittlerweile relativ komplexe § 100g StPO die richtige Ermächtigungsgrundlage dar. Die Auskunft kann sich dabei auf in der Vergangenheit oder auch in der Zukunft liegende Kommunikationsvorgänge beziehen. Zu den materiellen Voraussetzungen einer Verkehrsdatenauskunft gehört unter anderem der Verdacht einer Straftat von auch im Einzelfall erheblicher Bedeutung oder der Verdacht, dass eine Straftat mittels Telekommunikation begangen worden ist. Die formellen Voraussetzungen sind weitgehend mit denen der Telekommunikationsüberwachung vergleichbar, sodass auch hier grundsätzlich ein Richtervorbehalt gilt. Unter bestimmten Voraussetzungen sind darüber hinaus auch Standortdaten von der Ermächtigungsnorm des § 100g StPO erfasst. Die genauen Einzelheiten sind insofern im Leitfaden „Auskunftsverlangen von Ermittlungsbehörden“ aufgeführt. Im Falle eines rechtmäßigen Ersuchens nach § 100g StPO ist das Rechenzentrum zur Auskunft verpflichtet. Eine Auskunft über Daten der Vergangenheit ist selbstverständlich nur dann möglich, wenn die entsprechenden Daten noch vorhanden sind und damit noch nicht aufgrund datenschutzrechtlicher Pflichten gelöscht wurden (vergleiche Abschnitt zu datenschutzrechtlichen Anforderungen). Bei einem auf zukünftige Kommunikationsvorgänge gerichteten Auskunftsersuchen müssen die betreffenden Daten entsprechend des richterlichen Beschlusses aufgezeichnet und an die Behörden weitergegeben werden.

(3) Bestandsdaten

Bestandsdaten sind Daten, die für die Begründung und inhaltliche Ausgestaltung eines Vertragsverhältnisses über die Nutzung eines Dienstes erforderlich sind. Dies sind regelmäßig Name, Anschrift des Users oder eine statische IP-Adresse. Für die Bestandsdatenauskunft gilt das sogenannte Doppeltürmodell, demzufolge einerseits die Ermittlungsbehörde eine gesetzliche Grundlage benötigt, die es ihr erlaubt, die jeweiligen Bestandsdaten abzufragen, und andererseits für den Telekommunikationsdiensteanbieter eine gesetzliche Erlaubnisnorm vorliegen muss, die ihm aus datenschutzrechtlicher Sicht die Übermittlung der Daten erlaubt. Letzteres ist § 113 Telekommunikationsgesetz (TKG). Nach § 113 Abs. 1 TKG darf jeder geschäftsmäßige Telekommunikationsdiensteanbieter unter den Voraussetzungen des Absatzes 2 Bestandsdaten an bestimmte Behörden zu Auskunftszwecken übermitteln. Zu den berechtigten Empfängern gehören eine Reihe von Ermittlungs-/Sicherheitsbehörden, die in § 113 Abs. 3 TKG benannt sind. Eine richterliche Anordnung ist nicht erforderlich, sondern es reicht ein Auskunftsverlangen in Textform, welches eine gesetzliche Bestimmung angibt, die der anfragenden Behörde eine Erhebung der Daten

erlaubt. Bei Gefahr im Verzug darf das Verlangen auch in anderer Form gestellt werden, ist dann aber unverzüglich in Textform zu bestätigen. Die Auskunftserteilung darf insbesondere auch unter Verwendung dynamischer IP-Adressen erfolgen, was häufig erforderlich ist, wenn beauskunftet werden soll, wer zu einem bestimmten Zeitpunkt eine konkret benannte IP-Adresse genutzt hat. Sind die formellen Voraussetzungen erfüllt, ist der Telekommunikationsdiensteanbieter verpflichtet, dem Ersuchen unverzüglich nachzukommen. Die Verantwortung für die Zulässigkeit des Auskunftsverlangens trägt dabei die anfragende Stelle.

In allen Fällen der staatlichen Auskunftsverlangen muss der in Anspruch genommene Diensteanbieter in der Regel Stillschweigen gegenüber dem Betroffenen und Dritten wahren. Für eine etwaige Benachrichtigung des Betroffenen ist die Behörde zuständig, die die Daten anfragt.

Bei Anfragen von Strafverfolgungsbehörden sollte nicht in Hektik verfallen werden. Vor der Übermittlung sollte immer das Justitiariat über das Ersuchen informiert und die weitere Vorgehensweise abgesprochen werden. Wie gezeigt wurde, sind die Strafverfolgungsbehörden im Rahmen ihrer Ermittlungen an bestimmte gesetzliche Vorgaben gebunden. Dies bedeutet vor allem, dass im Falle von Telekommunikationsüberwachungsmaßnahmen, die Inhalte oder Verkehrsdaten betreffen, nach der StPO eine schriftliche richterliche Anordnung oder ausnahmsweise eine Anordnung der Staatsanwaltschaft vorgelegt werden muss. Für die Bestandsdatenauskunft gelten dagegen niedrigere Hürden. Es empfiehlt sich – bei aller Kooperationsbereitschaft mit den Sicherheitsbehörden – auch in den anderen Fällen nach Möglichkeit zu versuchen, eine schriftliche Bestätigung für die Auskunftserteilung einzuholen. Dies dient in erster Linie dazu, im Nachhinein Vorwürfe über datenschutzrechtliche Verstöße von Seiten der Nutzer auszuräumen.

b) Auskünfte an Polizeibehörden

Seltener ist es, dass die für die Gefahrenabwehr zuständigen Behörden die Herausgabe von User-Daten aus der Online-Kommunikation ersuchen. Hierfür sind jedoch die Landespolizei- beziehungsweise Gefahrenabwehrgesetze der jeweiligen Bundesländer einschlägig. Als Faustformel kann gelten, dass für ein rechtmäßiges Ersuchen der Behörde auf Herausgabe von Inhalts- und Verbindungsdaten eine spezielle Ermächtigungsgrundlage erforderlich ist. Der Verweis auf eine allgemeine ordnungsbehördliche Generalklausel oder die Amtshilfe ist in diesen Fällen regelmäßig nicht ausreichend. Im Hinblick auf Bestandsdaten gilt wiederum § 113 TKG, der voraussetzt, dass sich die für die Gefahrenabwehr zuständige Behörde auf eine spezielle Ermächtigungsnorm stützen kann, die zur Abfrage von Bestandsdaten ermächtigt (z. B. § 20a Abs. 1 S. 1 Nr. 1 Polizeigesetz NRW). Sofern es möglich ist, sollte immer ein Schriftstück mit Angabe der jeweils einschlägigen Befugnisnorm von der anfordernden Behörde verlangt werden.

c) Einbindung in Ermittlungsverfahren und Prävention

Ferner können die Mitarbeiter in Rechenzentren in behördliche Maßnahmen dergestalt eingebunden werden, dass sie z. B. visuelle Wahrnehmungen beziehungsweise Beobachtungen des Nutzerverhaltens an die Staatsanwaltschaft oder Polizei zukünftig weitergeben. Diese Kooperation in Form eines "Augen und Ohren offen halten" ist unbedenklich. Bei einer weitergehenden Zusammenarbeit sollte eine Anordnung von der Staatsanwaltschaft beziehungsweise dem Behördenleiter eingeholt werden. Auf jeden Fall sollte bei Verdacht begangener oder

bevorstehender Straftaten zunächst die zuständige Stelle informiert und die weitere Vorgehensweise abgestimmt werden.

4. Nutzungsausschluss bei missbräuchlicher Internetnutzung

Bei missbräuchlicher oder rechtswidriger Nutzung des Internetzugangs stellt sich die Frage, unter welchen Voraussetzungen ein Nutzer von der weiteren Nutzung der Dienste des Rechenzentrums ausgeschlossen werden kann. Dies wird vor allem bei besonders schwerwiegenden oder wiederholten Verstößen gegen die Benutzungsordnung oder bei strafbarer Nutzung der Online-Ressourcen relevant. Dementsprechend enthalten die meisten Benutzungsordnungen der DFN-Mitgliedsinstitutionen entsprechende Ausschlusstatbestände, nach denen Nutzer vorübergehend oder dauerhaft in der Nutzung eingeschränkt oder vollständig von der weiteren Internetnutzung ausgeschlossen werden können. Allerdings kann der Ausschluss oder die Beschränkung des Internetzugangs eines Nutzers, z.B. eines Studierenden an einer Hochschule, unter Umständen erhebliche Auswirkungen für den Betroffenen haben, wenn nämlich der Student auf die Informationsrecherche im Internet angewiesen ist. Hier können unter anderem die Wissenschaftsfreiheit (Art. 5 Abs. 3 S. 1 GG), die Berufsfreiheit (Art. 12 GG) oder die Informationsfreiheit (Art. 3 Abs. 1 GG) betroffen sein.
Aus diesem Grund kommt ein dauerhafter und vollständiger Ausschluss eines Studierenden grundsätzlich nur bei besonders schwerwiegenden oder wiederholten Missbräuchen in Betracht. Als Ausprägung des Verhältnismäßigkeitsgrundsatzes ist für jeden Einzelfall zu prüfen, ob nicht weniger einschneidende Maßnahmen, wie die vorübergehende Beschränkung einzelner Internet-Dienste (z.B. nur WWW oder nur E-Mail), möglich sind. Insbesondere bei weniger schwerwiegenden Missbräuchen dürfte zudem eine vorherige Abmahnung und Anhörung des Betroffenen geboten sein. In der Benutzungsordnung sollte ein entsprechendes formelles Ausschlussverfahren mit hinreichend konkreten Ausschlussgründen vorgesehen sein. Allerdings bleibt es grundsätzlich eine Frage des Einzelfalls und der konkreten Umstände, ob und in welchem Umfang ein missbräuchliches Verhalten beziehungsweise die rechtswidrige Nutzung des Internetzugangs durch einen Nutzungsausschluss "sanktioniert" werden kann.

5. Welche datenschutzrechtlichen Anforderungen sind zu beachten?

Soweit Rechenzentren durch den Netzzugang und den E-Mail-Dienst geschäftsmäßig Telekommunikationsdienste (TK-Dienste) erbringen, sind die Vorgaben des Fernmeldegeheimnisses und die für den Bereich der Telekommunikation einschlägigen Datenschutzvorschriften des Telekommunikationsgesetzes (TKG) zu beachten. Das geschäftsmäßige Erbringen von Telekommunikationsdiensten setzt keine Gewinnerzielungsabsicht voraus, sondern lediglich ein dauerhaftes Erbringen normalerweise entgeltlicher Dienste gegenüber Dritten, so dass Rechenzentren bei erlaubter Privatnutzung hiervon erfasst werden.

a) Situation bei ausgeschlossener Privatnutzung

Ist die Nutzung der TK-Dienste nur zu dienstlichen Zwecken erlaubt (vollständiges Verbot der Privatnutzung für Beschäftige), kommt die Anwendung der datenschutzrechtlichen Vorschriften des TKG (§§ 88, 91 ff. TKG) nicht in Betracht, da die Hochschule insofern nicht als TK-Diensteanbieter zu qualifizieren ist, weil dazu die Erbringung von TK-Dienstleistungen für Dritte erforderlich wäre. Im Falle der rein dienstlichen Nutzung handelt es sich gewissermaßen nur um eine Erbringung des Dienstes der Hochschule für sich selbst, da die Kommunikation der Mitarbeiter der Hochschule zugerechnet wird. Die Mitarbeiter gelten in dem Fall nicht als außenstehende „Dritte“. Deshalb führt ein Ausschluss der Privatnutzung dazu, dass die telekommunikationsspezifischen

Datenschutzanforderungen nicht beachtet werden müssen. Das Verbot der Privatnutzung muss in der Benutzungsordnung oder Dienstvereinbarung ausdrücklich und unmissverständlich erfolgen. Allerdings folgt hieraus keine unbegrenzte Zugriffsmöglichkeit auf die Kommunikationsinhalte, da die Einrichtung auch gegenüber ihren Arbeitnehmern zur Achtung der Persönlichkeitsrechte verpflichtet ist. Die Überwachung von Nutzern über Stichproben hinaus kann somit auch bei einer verbotenen Privatnutzung nur dann in Betracht kommen, wenn tatsächliche Anhaltspunkte für Verstöße oder eine missbräuchliche Nutzung vorliegen.

b) Situation bei erlaubter Privatnutzung

Bei erlaubter oder geduldeter Privatnutzung sind die telekommunikationsspezifischen Datenschutzvorschriften auch durch Hochschulen und Forschungseinrichtungen zu beachten. Relevant sind insbesondere Vorgaben zur Wahrung des Fernmeldegeheimnisses (§ 88 TKG), zum Datenschutz (§§ 91 ff.) und zu technischen Schutzmaßnahmen (§ 109 TKG).

(1) Fernmeldegeheimnis

Grundsätzlich müssen alle, die geschäftsmäßig (mit oder ohne Gewinnerzielungsabsicht) TK-Dienste erbringen, das grundgesetzlich in Art. 10 GG garantierte Fernmeldegeheimnis wahren. Hierzu werden durch § 88 Abs. 1, 2 TKG alle Diensteanbieter verpflichtet, sodass auch Hochschulrechenzentren betroffen sind, sofern eine Privatnutzung der Dienste nicht verboten ist. Danach ist es untersagt, sich über das "für die Erbringung der TK-Dienste einschließlich des Schutzes der technischen Systeme erforderliche Maß" hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen (§ 88 Abs. 3 S. 1 TKG). Die Einsichtnahme in Mail-Postfächer einzelner Nutzer oder die Überwachung des Mail-Verkehrs durch den Systemadministrator sind also ohne Einwilligung der Betroffenen grundsätzlich unzulässig. Dieser allgemeine Schutz des Fernmelde-/Telekommunikationsgeheimnisses wird durch die Vorgaben zur Datensicherheit und zum Datenschutz ergänzt und konkretisiert.

(2) Datenschutzrechtliche Vorgaben

Hochschulen und Forschungseinrichtungen haben bei erlaubter Privatnutzung die telekommunikationsspezifischen Datenschutzvorschriften in §§ 91 ff. TKG zu beachten. Durchgängiger Grundsatz des Datenschutzrechts ist es, dass die Erhebung und der Umgang mit personenbezogenen Daten nur dann erlaubt sind, wenn eine gesetzliche Erlaubnisnorm dies vorsieht oder eine Einwilligung der betroffenen Person vorliegt. Für den Schutz personenbezogener Daten wird im TKG im Wesentlichen zwischen zwei Datenkategorien differenziert.

Aus § 95 TKG ergeben sich die Vorgaben zum Schutz sogenannten Bestandsdaten. Hierbei handelt es sich um Daten, die für die Begründung und inhaltliche Ausgestaltung eines Vertragsverhältnisses über die Nutzung eines Dienstes erforderlich sind. Dies sind beispielsweise Name, Anschrift des Users oder eine fest vergebene IP-Adresse. § 95 TKG erlaubt die Erhebung und Verarbeitung von Bestandsdaten, soweit dies für die Durchführung des Nutzungsverhältnisses erforderlich ist. Die Erlaubnis ist hierbei eng auf die tatsächlich hierfür erforderlichen Daten zu beschränken. So ist beispielsweise kaum vorstellbar, dass der Familienstand eines Nutzers ein erforderliches Datum für die Durchführung des Nutzungsverhältnisses sein kann. Sollen darüber hinaus Bestandsdaten erhoben und verwendet werden, ist die Einwilligung des entsprechenden Nutzers erforderlich, die den Anforderungen des § 4a Bundesdatenschutzgesetz (BDSG) beziehungsweise den vergleichbaren Vorschriften in den Landesdatenschutzgesetzen genügen muss. Unter den Voraussetzungen des § 94 TKG kann die Einwilligung auch elektronisch erklärt werden.

Aus §§ 96 ff. TKG ergeben sich die Vorgaben in Bezug auf die sogenannten Verkehrsdaten. Als solche werden die Daten bezeichnet, die bei der Bereitstellung und Erbringung von Diensten erhoben werden. Hierunter sind in erster Linie Beginn und Ende von Internetverbindungen, übermittelte Datenmengen, besuchte Webseiten oder dynamisch vergebene IP-Adressen zu verstehen. Verkehrsdaten sind somit diejenigen Daten mit zumindest herstellbarem Personenbezug, die bei der tatsächlichen Nutzung des Netzzugangs durch den Nutzer anfallen. Da sie Aufschlüsse über die näheren Umstände der Kommunikation liefern können, werden sie insoweit vom Fernmeldegeheimnis erfasst und genießen damit einen höheren Schutz als die Bestandsdaten. Die Rechtslage ist entsprechend komplexer, wobei auch hier der allgemeine Grundsatz gilt, dass entweder eine gesetzliche Erlaubnis oder eine Einwilligung für die Erhebung und Verwendung der Daten bestehen muss.

§ 96 TKG führt verschiedene Erlaubnistatbestände für die Erhebung von Verkehrsdaten auf:

Es dürfen die zum Aufbau und zur Aufrechterhaltung der Kommunikation und die zur Entgeltabrechnung erforderlichen Daten verwendet werden. Die Befugnisse umfassen damit alle betrieblich notwendigen Daten für die Erbringung der Kommunikationsleistung.

Nach dem Ende der jeweiligen Verbindung sind die Möglichkeiten zur Verwendung auf Grundlage einer gesetzlichen Erlaubnis deutlich eingeschränkt. Dies ist auch für die weitere Speicherung der Daten von Bedeutung. Besteht keine Befugnis zur Verwendung der Daten (mehr), müssen diese nach Beendigung der Verbindung gelöscht werden.

Folgende für den Bereich der Hochschulen und Forschungseinrichtungen in Betracht kommende Befugnisse bestehen nach Beendigung der Verbindung:

Werden Verkehrsdaten zu anderen als den in § 96 Abs. 1 genannten Zwecken verwendet, ist dies gemäß § 96 Abs. 2 unzulässig. Es gibt jedoch einige Rechtsnormen, die ebenfalls den Umgang mit Verkehrsdaten erlauben.

Eine eher theoretische Bedeutung hat mittlerweile die Erlaubnis nach § 96 Abs. 1 i. V. m. § 97 TKG, derzufolge Verkehrsdaten gespeichert und verwendet werden dürfen, soweit sie zur Ermittlung oder Abrechnung von Entgelten benötigt werden. Denn die Internetnutzung ist für Studierende und Mitarbeiter an Hochschulen in aller Regel kostenlos und es gibt keinerlei Abrechnung der in Anspruch genommenen Dienste, zumal eine Abrechnung nach der Menge der übermittelten Daten in Zeiten der Internet-Flatrates meistens nur noch im Mobilfunkbereich vorkommt. Sollte dies ausnahmsweise anders sein, ist zu beachten, dass die Daten zu diesem Zweck erforderlich sein müssen. Wird beispielsweise gegenüber einer Kostenstelle mit mehreren Arbeitsplätzen abgerechnet, ist die gesonderte Dokumentation für jeden Arbeitsplatz nicht erforderlich, da es in der Regel nur auf den Gesamtverbrauch der Kostenstelle ankommt. Wird individuell gegenüber den einzelnen Nutzern abgerechnet, ist in der Regel die Speicherung von zu einem bestimmten Zeitpunkt verwendeten IP-Adressen zur Abrechnung nicht erforderlich, wenn der Verbrauch anhand der Benutzerkennung zugeordnet werden kann. Findet eine interne Abrechnung überhaupt nicht statt, ist die Befugnis für die Einrichtung bedeutungslos. Zu Abrechnungszwecken gespeicherte Daten dürfen ohne gesonderte Erlaubnis oder Einwilligung nicht zu anderen Zwecken verwendet werden. Die Daten dürfen im Regelfall höchstens für 6 Monate seit dem Zeitpunkt der Versendung der Rechnung gespeichert werden.

Von großer praktischer Relevanz ist jedoch die Erlaubnisnorm des § 100 TKG. Dieser erlaubt eine Verwendung von Verkehrsdaten, um Störungen von Telekommunikationsanlagen und dem Missbrauch von TK-Diensten zu begegnen. So darf der Diensteanbieter nach § 100 Abs. 1 TKG zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen Verkehrsdaten erheben und verwenden. Dies gilt auch für Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können. Zwar setzt die Befugnis zur Speicherung nicht voraus, dass im Einzelfall bereits Anhaltspunkte für eine tatsächliche Störung oder einen Fehler vorliegen, sondern es genügt, dass die in Rede stehende Datenerhebung und -verwendung geeignet, erforderlich und im engeren Sinn verhältnismäßig ist, um abstrakten Gefahren für die Funktionstüchtigkeit des Telekommunikationsbetriebs entgegenzuwirken. Denn das „Erkennen“ von Störungen und Fehlern findet in der Regel in einem Stadium statt, in dem Anhaltspunkte hierfür erst gewonnen werden, also ein konkreter Verdacht noch nicht bestehen muss (BGH, Urteil vom 13.1.2011 – Az.: III ZR 146/10). Allerdings darf die Befugnis nicht dahingehend missverstanden werden, dass Verkehrsdaten zu Zwecken der Fehlererkennung unbegrenzt vorgehalten werden dürfen. Auch in Bezug auf diese Befugnis kommt es maßgeblich auf die Erforderlichkeit der Daten zu diesem Zweck an. Sobald erkennbar ist, dass die Daten für die Erkennung, Eingrenzung oder Beseitigung einer Störung nicht oder nicht mehr benötigt werden, sind diese zu löschen, es sei denn, dass eine anderweitige Befugnis (z. B. Abrechnungszwecke) besteht. Das Gleiche gilt für solche Daten, die bei Vorliegen einer Störung nicht zu deren Eingrenzung oder Beseitigung benötigt werden. Die Rechtsprechung akzeptiert derzeit eine Speicherung für einen Zeitraum von bis zu sieben Tagen, wenn diese Daten zum Erkennen und Beseitigen technischer Störungen benötigt werden (BGH, Urteil vom 3.7.2014 – Az. III ZR 391/13; BGH, Urteil vom 13.1.2011 – Az. III ZR 146/10). Nach sieben Tagen sind sie jedoch zu löschen, soweit keine anderen gesetzlichen Ermächtigungen vorliegen.

Nach § 100 Abs. 3 TKG kann der Diensteanbieter bei Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte auch Verkehrsdaten erheben und verwenden, die zum Aufdecken sowie Unterbinden einer rechtswidrigen Inanspruchnahmen der Telekommunikationsnetze und -dienste, wie z.B. einer Leistungserschleichung, erforderlich sind. Die Voraussetzungen sind deutlich schärfer: es bedarf konkret vorliegender Anhaltspunkte für einen Missbrauch, die zudem dokumentiert werden müssen, und die Datenverwendung muss der Sicherung des Entgeltanspruchs dienen. Für die weiteren Einzelheiten wird auf § 100 Abs. 3 TKG verwiesen. Eine allgemeine, möglicherweise latent vorhandene Missbrauchsgefahr der Netzdienste kann eine präventive Protokollierung aller Verkehrsdaten daher grundsätzlich nicht rechtfertigen. Insgesamt dürfte die praktische Relevanz von § 100 Abs. 3 TKG für Hochschulen und Forschungseinrichtungen eher gering sein.

Eine Erhebung und Verwendung von Verkehrsdaten außerhalb der gesetzlich eingeräumten Befugnisse bedarf der Einwilligung durch den Betroffenen, die den Voraussetzungen des § 4a BDSG oder den vergleichbaren Vorschriften der für die Hochschulen zumeist einschlägigen Landesdatenschutzgesetze genügen muss. Unter den Voraussetzungen des § 94 TKG kann eine Einwilligung auch im elektronischen Verfahren eingeholt werden.

(3) Technische Schutzmaßnahmen zur Datensicherheit

Nach § 109 Abs. 1 TKG haben Diensteanbieter erforderliche technische Vorkehrungen und sonstige Maßnahmen zum Schutz des Fernmeldegeheimnisses und gegen die Verletzung des Schutzes personenbezogener Daten zu treffen, wobei der Stand der Technik zu berücksichtigen ist.

Diese Verpflichtung zur Ergreifung bestimmter technischer Schutzmaßnahmen trifft auch die Rechenzentren der Hochschulen und Forschungseinrichtungen als Diensteanbieter und Betreiber von Netz-Servern und Routern. Im Hinblick auf das Fernmeldegeheimnis muss jeder Diensteanbieter verhindern, dass Eingriffe vorgenommen werden, die nicht von gesetzlichen Erlaubnistatbeständen gedeckt sind, und dass keine unberechtigten Zugriffe erfolgen können. Dies beinhaltet die Verpflichtung, Daten nicht nur vor äußeren Einflussnahmen wie z. B. durch „Hacker" zu schützen, sondern auch vor eigenmächtigen Einflussnahmen der eigenen Mitarbeiter. Hierbei ist neben technischen Schutzvorkehrungen vor allem an Zugangskontrollen für sensible Bereiche, Zugriffsbeschränkungen auf Datenbestände und an die Schulung der Mitarbeiter in Bezug auf den Umgang mit personenbezogenen Daten zu denken.

Unter der Verletzung des Schutzes personenbezogener Daten, gegen die ebenfalls technische Vorkehrungen zu treffen sind, wird nach der Legaldefinition des § 3 Nr. 30a TKG eine Verletzung der Datensicherheit verstanden, die zum Verlust, zur unrechtmäßigen Löschung, Veränderung, Speicherung, Weitergabe oder sonstigen unrechtmäßigen Verwendung personenbezogener Daten führt, die übertragen, gespeichert oder auf andere Weise im Zusammenhang mit der Bereitstellung öffentlich zugänglicher TK-Dienste verarbeitet werden, sowie der unrechtmäßige Zugang zu diesen.

Verlangt werden die „erforderlichen" Schutzmaßnahmen, wobei im Sinne eines hohen Schutzniveaus ein strenger Maßstab anzulegen ist. Dennoch muss als Ausfluss des Verhältnismäßigkeitsgrundsatzes der wirtschaftliche Aufwand noch im Verhältnis zu der Bedeutung des zu schützenden Rechtsguts stehen, sodass hier eine Angemessenheitsbewertung vorgenommen werden muss.

Da außerdem der Stand der Technik zu berücksichtigen ist, handelt es sich bei der Verpflichtung nach § 109 Abs. 1 TKG um eine dynamische Verpflichtung, die eine fortwährende Anpassung an die neuen technischen Entwicklungen und Risiken erfordert.

Unabhängig von der Eigenschaft als Diensteanbieter besteht überdies nach der allgemeinen Regelung in § 9 Bundesdatenschutzgesetz (BDSG) und in vergleichbaren Regelungen der zumeist für Hochschulen einschlägigen Landesdatenschutzgesetze die Verpflichtung zu angemessenen Maßnahmen zur Datensicherung in datenverarbeitenden Stellen. Hochschulen und Forschungseinrichtungen haben daher unabhängig von ihrer Eigenschaft als Kommunikationsdiensteanbieter Datenbestände gegen unerlaubte Zugriffe von innen wie außen durch angemessene Maßnahmen zu schützen. Wichtige Beispiele hierfür sind ein wirksamer Passwortschutz und Maßnahmen zum Schutz der Informationsinfrastruktur vor Viren.

6. Datenschutzrechtliche Konsequenzen für die Praxis

Aufgrund der Komplexität werden im Folgenden die praktischen Konsequenzen für die Rechenzentren durch die zu beachtenden datenschutzrechtlichen Vorgaben beispielhaft dargestellt:

a) Protokollierung von Einwahlvorgängen

Eine vollständige, nutzerbezogene Speicherung und Auswertung aller Verbindungs-/ Nutzungsdaten, die beim Netzzugang über Einwahlpunkte oder sonstige Dialog-Server anfallen, ist unzulässig. Es dürfen lediglich die Daten erhoben und gespeichert werden, die für die jeweilige Verbindung zwingend erforderlich sind. Beispielhaft sind derzeit folgende Daten zu nennen:

Zur Identifikation und Zugangskontrolle müssen zu Beginn der Sitzung der Nutzername, das Passwort oder die Rufnummer (bei aktivierter Rufnummernübermittlung) erhoben werden.

Die dynamische IP-Adresse muss aus technischen Gründen (korrektes Routing) während der konkreten Verbindung gespeichert werden. Jedoch besteht nach Beendigung der jeweiligen Sitzung kein betriebstechnisches Bedürfnis mehr für eine weitere Speicherung.

Insbesondere die Dauer, der Umfang der jeweiligen Nutzung (z.B. übertragene Datenmenge) und die näheren Umstände der Telekommunikation (z.B. Mail-Protokolle, aufgerufene Seiten, kontaktierte Server) dürfen ohne Einwilligung des Nutzers über das Ende der Verbindung nur gespeichert werden, soweit dies zu Abrechnungszwecken, zur Störungsbeseitigung oder zur Missbrauchsaufklärung erforderlich ist. Die Erforderlichkeit zu Abrechnungszwecken hat mittlerweile allerdings stark an Relevanz verloren. Zur Störungserkennung und -beseitigung dürfen die erforderlichen Daten bis zu sieben Tage lang gespeichert werden, aber nur soweit dies auch tatsächlich zu diesen Zwecken erforderlich ist (siehe oben II. 4. Lit. b) Die Aufklärung einer - äußerlich unverdächtigen - Nutzung der eigenen Systeme zum unbefugten Eindringen in externe Systeme setzt allerdings tatsächliche Anhaltspunkte für einen Missbrauch voraus. Eine "verdachtsunabhängige", präventive Protokollierung zum Schutz fremder Systeme ist grundsätzlich unzulässig. Aus Datenbeständen, die aus anderen Gründen erhoben werden dürfen (z.B. für Abrechnungszwecke), können allerdings unter Umständen nachträglich die Daten ermittelt werden, die konkrete Indizien für einen Missbrauch enthalten.

Zur Aufklärung von Hacker-Attacken oder sonstigen unberechtigten Zugriffen oder Zugriffsversuchen auf personenbezogene Daten innerhalb des eigenen Systems können daten- beziehungsweise ereignisbezogene Protokolldateien ausgewertet werden (z.B. Zugriffsversuche auf Passwort-Listen etc.).

b) Konsequenzen für Spam- und Virenfilterung in Einrichtungen

Die rechtlichen Vorgaben durch das Fernmeldegeheimnis und den Datenschutz sind auch bei der einrichtungsinternen Ausfilterung von Spam- und Virenmails zu beachten. Für die rechtliche Beurteilung ist zunächst entscheidend, ob in der jeweiligen Einrichtung die private Nutzung des E-Mail-Dienstes durch Mitarbeiter und/oder Studierende zugelassen ist. In diesem Zusammenhang ist darauf hinzuweisen, dass unter Umständen auch bei einer fehlenden ausdrücklichen Regelung eine Erlaubnis zur Privatnutzung anzunehmen ist, wenn sich dies aus einer dauerhaften Übung in der Einrichtung ergibt.

Ist eine Erlaubnis zur privaten Nutzung des einrichtungsinternen E-Mail-Dienstes anzunehmen, stellen sich in Bezug auf zentrale Filtermaßnahmen zur Spam- oder Virenbekämpfung teils schwierige Rechtsfragen, da die Einrichtung dann als Telekommunikationsdiensteanbieter zu qualifizieren ist. In diesem Fall sind die telekommunikationsspezifischen Datenschutzvorschriften in §§ 91 ff. TKG und das Fernmeldegeheimnis aus § 88 TKG zu beachten. Durch die kaum trennbare Vermischung privater und dienstlicher Inhalte ist in der Regel eine differenzierte Behandlung nicht möglich. Anknüpfend an das Fernmeldegeheimnis stellt die Strafnorm des § 206 Abs. 2 Nr. 2 Strafgesetzbuch (StGB) die unbefugte Unterdrückung einer einem Post- oder Telekommunikationsunternehmen anvertrauten Sendung unter Strafe. Dass auch Hochschulen bei einem Eingriff in die Zustellung von E-Mails unter den Begriff des Unternehmens im Sinne dieser Strafnorm fallen können, ergibt sich aus einer Entscheidung des Oberlandesgerichts Karlsruhe (Beschluss vom 10.1.2005 – 1 Ws 152/04 = MMR 2005, S. 181 ff.). Allerdings stand diese Entscheidung nicht im Zusammenhang mit einer Spam- oder Virenfilterung durch die beteiligte Hochschule, so dass die Rechtslage diesbezüglich nicht geklärt ist. Daneben kann bei Abwehrmaßnahmen, bei denen E-Mails gelöscht oder inhaltlich verändert werden,

die Gefahr einer strafbaren Datenveränderung nach § 303a StGB in Betracht gezogen werden. Die Komplexität dieser Fragen erfordert eine differenzierte Betrachtung.

(1) Virenfilterung

Erfolgt die Virenfilterung aufgrund eines positiven Prüfergebnisses des Virenscanners, besteht in der Regel eine konkrete Gefahr für die Datensicherheit in der betroffenen Einrichtung. Aus § 109 Abs. 1 TKG und der allgemeinen Verpflichtung datenverarbeitender Stellen zur Gewährleistung der Datensicherheit aus den Datenschutzgesetzen (z. B. § 9 BDSG, § 10 DSG NW) ergibt sich die Pflicht, technische und organisatorische Schutzmaßnahmen zur Gewährleistung der Datensicherheit zu ergreifen. Vor diesem Hintergrund ist im Regelfall selbst die Löschung positiv gescannter E-Mails gerechtfertigt. Somit ist die Maßnahme selbst dann, wenn einer der genannten Straftatbestände eingreift, durch die in der Regel gegebene Rechtfertigung nicht strafbar.

Allerdings ist bei einer Löschung oder sonstigen Vereitelung des Zugangs aus Gründen der Verhältnismäßigkeit die Benachrichtigung der Beteiligten geboten, damit Absender und Empfänger wenigstens Kenntnis davon erlangen können, dass die Übermittlung fehlgeschlagen ist und auf welchem Grund das Scheitern beruht.

Wird die Löschung erwogen, ist zudem zu berücksichtigen, dass dadurch der Einrichtung zeitkritische Informationen verloren gehen können. Als Alternative bietet sich diesbezüglich eine Quarantänelösung an, bei der ein Abruf der verseuchten E-Mails über ein gesichertes Web-Interface zumindest theoretisch möglich bleibt.

(2) Spamfilterung

Schwieriger gestaltet sich die Situation bei der Filterung unerwünschter Werbe-Mails, dem sogenannten Spam. Die Probleme beginnen hier anders als bei der Virenfilterung bereits bei der zuverlässigen Erkennung von Spam-Mails. Die Optimierung inhaltsbezogener Filterprogramme wird laufend durch entsprechende Gegenmaßnahmen der Versender von Spam unterlaufen. Damit scheidet eine auch nur annähernd eindeutige Erkennung von Spam bislang noch aus.

Zuverlässiger bei der Erkennung von Spam sind Verfahren, die an die Herkunft einer E-Mail von einem möglicherweise unsicheren Server anknüpfen. Oftmals werden nicht zureichend gesicherte Mailserver zur Verteilung von Spam-Mails missbraucht. Ergeben sich Hinweise auf Sicherheitsprobleme, wird der entsprechende Server gelistet. Die Folge ist, dass alle E-Mails mit Herkunft von diesem Server bei Anwendern nicht mehr angenommen werden, die sich der entsprechenden Liste zur Spamerkennung bedienen. Angesichts der Tatsache, dass nicht selten auch Mailserver von Wissenschafts- und Bildungseinrichtungen trotz nachweisbar fehlender für den Spamversand geeigneter Sicherheitslücken gelistet werden, erscheint die Transparenz und Zuverlässigkeit dieser Methode äußerst fraglich. Nicht zu vergessen ist, dass E-Mails von solchen Servern ohne weitere Differenzierung abgewiesen werden, so dass mit dem Höchstmaß der Erkennung ein Höchstmaß an Fehlerhaftigkeit einhergeht. Aus diesem Grund ist es unbedingt erforderlich, dass im Falle der Nutzung eines solchen „Blacklisting“-Dienstes ein sorgfältiger und zuverlässiger Anbieter mit einem transparenten Verfahren ausgewählt wird. Nur so kann nachvollzogen werden, wann und warum ein Server gelistet wird und es ist möglich, einen fehlerhaft gelisteten Server wieder zu entfernen.

Neben dem Problem der möglichst sicheren Erkennung von Spam stellt sich die Frage der weitergehenden Vorgehensweise gegen Spam. In Betracht gezogen wird hierbei zumeist die

Nichtannahme, die Markierung oder die Löschung spamverdächtiger E-Mails. Bei Maßnahmen, die zu einer Vereitelung der Zustellung von E-Mails führen, ist zu beachten, dass hierdurch bei einer erlaubten Privatnutzung möglicherweise in geschützte Kommunikationsvorgänge eingegriffen wird. Dies betrifft nicht nur den Fall von falsch erkannten Spam-Mails, sondern auch das in Betracht zu ziehende private Interesse am Empfang von Werbemails. Solange die E-Mail durch das Rechenzentrum noch nicht zum Empfang angenommen wurde (Header oder zumindest Body also noch nicht auf dem Empfänger-Server liegen), ist eine Nichtannahme der Mail jedoch strafrechtlich nicht relevant. Die rechtlich sicherste Lösung ist in jedem Fall die Markierung der E-Mails mit dem ermittelten Spam-Wert, die zusammen mit einem entsprechenden Mailprogramm die eigenständige Ausfilterung durch den Nutzer ermöglicht. Bei der Markierung von E-Mails ist aus rechtlichen Gründen unbedingt darauf zu achten, dass die Markierung im Header und nicht im Subject (Betreff) der E-Mail erfolgt.

Ist die Nutzung des einrichtungsinternen E-Mail-Dienstes nur zu Dienstzwecken erlaubt, kommt die Anwendung der telekommunikationspezifischen Datenschutzvorschriften in §§ 91 ff. TKG nicht in Betracht. Auch das in § 88 TKG geregelte Fernmeldegeheimnis findet in diesem Fall keine Anwendung. Die auf das Fernmeldegeheimnis Bezug nehmende Strafnorm in § 206 Abs. 2 Nr. 2 StGB ist somit ebenfalls nicht einschlägig. Zu beachten ist, dass der Ausschluss der Privatnutzung ausdrücklich und unmissverständlich gegenüber den Nutzern erfolgen sollte, damit keine Grauzonen entstehen können.

Wenn dies beachtet wird, stellen sich ansonsten in Bezug auf die Spam- und Virenfilterung durch die Einrichtung keine spezifischen Rechtsprobleme.

III. Angebot von abrufbaren Inhalten

1. Einführung

Wird über das Internet abrufbarer Inhalte auf Webservern bereitgestellt, sind auch im Bereich der Hochschulen und Forschungseinrichtungen eine Reihe von rechtlichen Vorgaben zu beachten. Im folgenden Kapitel des Rechtsguides sollen in diesem Zusammenhang relevante Rechtsfragen dargestellt werden. Nicht behandelt werden rechtliche Fragen bei der Bereitstellung von Speicherplatz für Content von Dritten, wie dies beispielsweise bei studentischen Webseiten oder Foren/Blogs der Fall ist. Die diesbezüglich auftretenden rechtlichen Fragestellungen werden im Kapitel „Bereitstellung von Speicherplatz für fremde Inhalte“ behandelt.

2. Rechtliche Anforderungen an Webangebote

a) Informationspflicht beim Betrieb von Telemedien

(1) Grundanforderungen für Telemedien

Das Telemediengesetz (TMG) sowie einzelne Normen des Rundfunkstaatsvertrags (RStV) enthalten die wirtschafts- und inhaltsbezogenen Grundanforderungen für Telemedien.

§ 5 TMG, Geschäftsmäßige Telemedien

§ 5 TMG statuiert wie die alten Regelungen im Teledienstegesetz (TDG) und Mediendienste-Staatsvertrag (MDStV) umfassende Informationspflichten (auch „Impressumspflicht“ genannt), die zu mehr Transparenz von Angeboten im Internet führen sollen. Nach der seit dem 1.3.2007 geltenden Rechtslage setzt die Informationspflicht nach dem TMG voraus, dass es sich um geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien handelt. Nach der Gesetzesbegründung sollen damit solche Telemedien vom Anwendungsbereich ausgenommen werden, die – wie z. B. private Homepages – ohne den Hintergrund einer Wirtschaftstätigkeit bereitgehalten werden. Da Hochschulen beispielsweise im Rahmen von Drittmittelprojekten vor einem wirtschaftlichen Hintergrund tätig werden, fallen diese tendenziell weiterhin unter die Pflicht zur Anbieterkennzeichnung. Aufgrund der Vielfältigkeit der Betätigungsfelder dürfte zudem in der Regel eine hinreichende Abgrenzung nicht möglich sein. Sollte diese möglich sein, gelten für das Impressum zumindest die Anforderungen aus § 55 Abs. 1 Rundfunkstaatsvertrag (RStV). Gleiches gilt für die Tätigkeit von Forschungseinrichtungen.

Somit müssen die Seiten von Hochschulen und Forschungseinrichtungen grundsätzlich auch weiterhin die gesetzlich vorgesehenen Informationen unter einem leicht auffindbaren Reiter „Impressum“ oder „Kontakt“ enthalten. Der Nutzer des Webangebots soll möglichst mit einem Klick auf die Maustaste die Möglichkeit zur Kenntnisnahme der Anbieterinformationen haben. Mehrfaches Klicken oder Scrollen sollte dem Nutzer erspart bleiben, um möglichem Ärger vorzubeugen. Folgende Daten müssen nach § 5 TMG ständig verfügbar gehalten werden:

- Name und ladungsfähige Anschrift, bei juristischen Personen zusätzlich der Vertretungsberechtigte (Beispiel: Rektor der Hochschule)
- E-Mail-Adresse und zumindest die Angabe einer Telefonnummer
- Falls vorhanden: Umsatzsteueridentifikationsnummer
- Gegebenenfalls: Angaben zur zuständigen Aufsichtsbehörde, wenn der Teledienst im Rahmen einer Tätigkeit angeboten oder erbracht wird, die der behördlichen Zulassung bedarf
- Gegebenenfalls: Berufsbezeichnung, Zugehörigkeit zu einer Kammer und die Bezeichnung von berufsrechtlichen Regelungen und Beschreibung, wie diese zugänglich sind
- Gegebenenfalls: Handels-, Vereins-, Partnerschafts- oder Genossenschaftsregister mit Registernummer

Als Vertretungsberechtigter ist bei Hochschulen auf jeden Fall der Rektor zu nennen, da er der gesetzliche Vertreter der Hochschule ist. Bei Instituten und Lehrstühlen, die ihre Webseiten in eigener Verantwortung erstellen, kann zusätzlich der Institutsleiter beziehungsweise der Lehrstuhlinhaber genannt werden.

§ 55 Abs. 1 RStV, alle Telemedien

Auch wenn das Angebot keine Dienste enthält, die in der Regel gegen Entgelt erbracht werden, können aufgrund des Verweises in § 5 Abs. 2 TMG nach anderen Rechtsvorschriften weitergehende Informationspflichten bestehen. Dies ist auf Grund von § 55 Abs. 1 RStV der Fall, wonach Anbieter von Telemedien, die nicht ausschließlich persönlichen oder familiären Zwecken dienen, folgende Informationen im Impressum verfügbar zu halten haben:

- Namen und Anschrift sowie

- Bei juristischen Personen auch Namen und Anschrift des Vertretungsberechtigten

Selbst wenn es somit an der Voraussetzung der Geschäftsmäßigkeit im Sinne von § 5 TMG fehlt, muss das Impressum nach § 55 Abs. 1 RStV zumindest diese Angaben enthalten, wobei als Vertretungsberechtigter bei Hochschulen wiederum in der Regel der Rektor anzugeben ist.

(2) - Telemedien mit journalistisch-redaktionell gestalteten Angeboten

Für journalistisch-redaktionell gestaltete Angebote, in denen vollständig oder teilweise Inhalte periodischer Druckerzeugnisse in Text oder Bild wiedergegeben oder in denen in periodischer Folge Texte verbreitet werden, gelten zusätzlich die Anforderungen aus § 55 Abs. 2 RStV. Als erstes Gericht hat das Landgericht Hamburg konstatiert, dass hierzu auch Online-Foren zählen können (LG Hamburg, Urteil vom 27.4.2007 – Az. 324 O 600/06). Gänzlich geklärt ist der Anwendungsbereich dieser Vorschrift jedoch noch nicht. Gemäß § 55 Abs. 2 RStV muss bei derartigen Angeboten zusätzlich ein für den Inhalt Verantwortlicher mit Name und Anschrift benannt werden. Bei mehreren Verantwortlichen muss gekennzeichnet werden, wer für welchen Teil des Angebots verantwortlich ist. Als Verantwortlicher kann nur benannt werden, wer voll geschäftsfähig ist, seinen ständigen Aufenthalt im Inland hat, nicht infolge Richterspruchs die Fähigkeit zur Bekleidung öffentlicher Ämter verloren hat und unbeschränkt strafrechtlich verfolgt werden kann.

b) Jugendschutz – Jugendschutzbeauftragter (§ 7 JMStV)

Die Voraussetzungen für die Pflicht zur Bestellung eines Jugendschutzbeauftragten sind nunmehr im JMStV (Jugendmedienschutz-Staatsvertrag) der Länder geregelt. Nach § 7 Abs. 1 S. 2 JMStV erstreckt sich die Pflicht, einen Jugendschutzbeauftragten zu bestellen, auf alle geschäftsmäßigen Anbieter von Telemediendiensten. Davon umfasst sind alle Angebote, die ernsthaft und für eine gewisse Dauer betrieben werden. Eine Gewinnerzielungsabsicht wird im Gegensatz zum früheren Gesetz über die Verbreitung jugendgefährdender Schriften (GjS) nicht mehr gefordert. Der Anwendungsbereich ist jedoch nach dem JMStV wesentlich enger als früher nach dem GjS, da gemäß § 7 Abs. 1 S. 2 JMStV nur Anbieter von Suchmaschinen und solche Anbieter von Telediensten, die tatsächlich jugendgefährdende oder entwicklungsbeeinträchtigende Inhalte bereitstellen, zur Bestellung eines Jugendschutzbeauftragten verpflichtet werden. Damit entfällt die Pflicht zur Bestellung eines Jugendschutzbeauftragten für Anbieter, die aufgrund der Struktur ihres Angebotes Vorsorge dafür getroffen haben, dass entsprechende Inhalte nicht in ihrem Angebot vorkommen. Im Falle der Verpflichtung zur Bestellung eines Jugendschutzbeauftragten besteht unter bestimmten Umständen die Möglichkeit, die Aufgaben auf eine Einrichtung der freiwilligen Selbstkontrolle zu übertragen. Diese Möglichkeit besteht nur für Anbieter mit weniger als 50 Mitarbeitern und weniger als 10 Mio. Zugriffen im Monatsdurchschnitt eines Jahres (vergleiche § 7 Abs. 2 JMStV). Besteht eine Bestellungspflicht, so bestimmen § 7 Abs. 1 S. 3 und S. 4 JMStV, welche Angaben über den Beauftragten auf welche Art zur Verfügung gestellt werden müssen.

c) Geschäftliche Angebote

Bei geschäftlichen Angeboten ist besonderes das Haftungsrisiko im Bereich des gewerblichen Rechtschutzes, insbesondere des Wettbewerbs- und Markenrechts, zu beachten. Aufgrund der Rechtsprechung, die bei Rechtsverletzungen einen Anspruch auf Ersatz der Kosten für eine erstmalige anwaltliche Abmahnung gewährt, werden Ansprüche auf diesem Gebiet sehr häufig durchgesetzt. Voraussetzung für marken- und wettbewerbsrechtliche Ansprüche ist eine Tätigkeit im geschäftlichen Verkehr. Dies ist jede Tätigkeit, die irgendwie der Förderung eines eigenen oder fremden Geschäftszwecks dient. Die Entgeltlichkeit eines Angebots ist nicht unbedingt erforderlich, maßgeblich ist allein der geschäftliche Zweck, der z.B. auch in der Gewinnung von neuen Kunden für ein anderes (zukünftiges) Angebot liegen kann. Ist ein Angebot der Hochschule als eigener Inhalt dem geschäftlichen Verkehr zuzuordnen, so besteht keine Haftungserleichterung. Dies gilt insbesondere bei Kooperationen von Hochschulen mit Wirtschaftsunternehmen oder bei ausgelagerten Forschungsprojekten und Praxisgruppen, die ihre Dienste oder Produkte offen am Markt anbieten und damit in Wettbewerb mit anderen Unternehmen treten. In solchen Fällen ist eine Einhaltung der strengen Regeln des Wettbewerbsrechts sicherzustellen und eine Verletzung von Markenrechten zu vermeiden.

d) Werbung und Sponsoren-Logos

Bei einigen Institutionen ist der Wunsch entstanden, Werbung auf ihren Webseiten zu platzieren, um Kosten zu sparen oder Einnahmen zu erzielen. Dies soll z.B. in der Form geschehen, dass ein Unternehmen die Internetseiten der Hochschule kostenlos gestaltet, dafür aber Werbung in Form von Bannern oder Sponsoren-Logos auf die Seiten setzt.

Die dabei für Telemedien zu beachtenden Vorgaben sind in § 6 TMG und § 58 RStV enthalten. Bei kommerzieller Kommunikation haben Anbieter von Telemedien über die Informationspflichten von § 5 TMG (siehe oben) hinausgehende Pflichten. Demnach muss eine kommerzielle Kommunikation zunächst klar als solche zu erkennen sein. Des Weiteren muss die natürliche oder juristische Person, in deren Auftrag eine solche kommerzielle Kommunikation erfolgt, eindeutig identifizierbar sein. Angebote zur Verkaufsförderung wie Preisnachlässe, Zugaben und Geschenke müssen unzweifelhaft als solche erkennbar sein und die Bedingungen für ihre Inanspruchnahme müssen leicht zugänglich sein sowie klar und unzweideutig angegeben werden. Preisausschreiben oder Gewinnspiele mit Werbecharakter müssen ebenfalls klar als solche erkennbar und die Teilnahmebedingungen leicht zugänglich sein sowie unmissverständlich und eindeutig angegeben werden. Darüber hinaus ergeben sich aus § 58 RStV die weiteren inhaltlichen Anforderungen, dass Werbung vom übrigen Inhalt der Angebote getrennt sein muss und dass in der Werbung keine unterschwelligen Techniken eingesetzt werden dürfen. Wichtig ist daher eine strikte Trennung der eigenen Inhalte von der Werbung. Sponsoren-Logos und Werbebanner müssen eindeutig gekennzeichnet werden, etwa als "Anzeige" oder "gesponsert von: …“. Dies ist deshalb wichtig, weil sich aus der äußeren Gestaltung und dem Layout von Webseiten oft keine eindeutige Abgrenzung ergibt, so dass Werbung und Inhalt leicht ineinander greifen. Werbung birgt eine gewisse Gefahr von Rechtsverletzungen in sich, insbesondere können Verstöße gegen das Wettbewerbsrecht oder gegen das Markenrecht vorliegen. Aufgrund der Rechtsprechung bezüglich der Haftung für Hyperlinks kann dabei eine Mitverantwortung selbst für den Inhalt der Seiten des Anbieters, auf die ein Link verweist, nicht von vornherein ausgeschlossen werden. Bevor ein Link gesetzt wird, sollten die Inhalte der Werbung zumindest auf offensichtliche

(das heißt auch für Laien erkennbare) Rechtsverstöße hin überprüft werden. Sinnvoll ist auch eine Klarstellung auf einer Leitseite oder ähnliches., dass es sich bei den Anzeigen um Angebote von Fremdanbietern handelt, für deren Inhalt die Universität nicht verantwortlich ist. Ein Ausschluss von jeglicher (Mit-)Verantwortung kann dadurch allerdings nicht erzielt werden. Vielmehr muss sich die ausreichende Distanzierung tatsächlich aus den Gesamtumständen ergeben, so vor allem aus der Gestaltung der Seite, der Auswahl der Links und ihrer Platzierung.

3. Das Urheberrecht – eine kurze Einführung für Webseitengestalter

Die meisten Rechtsverletzungen im Internet betreffen das Urheberrecht. Sofort denkt man hier an Musiktauschbörsen und so genannte „Raubkopien“. Aber schon ein sorglos auf die eigene Webseite kopiertes Passfoto von einem Fotografen, die Anfahrtsskizze mit der gescannten Straßenkarte oder die zusammen geschnipselte Hintergrundmusik können dazu führen, dass Schadensersatzansprüche in erschreckender Höhe fällig werden. Wer vorsätzlich das Urheberrecht verletzt, muss darüber hinaus auch mit einer strafrechtlichen Verfolgung rechnen.

Jeder, der mit einer eigenen persönlich-geistigen Leistung ein Werk erschafft, genießt als dessen Urheber automatisch den Schutz des Urhebergesetzes (UrhG), ohne dass es einer Anmeldung, Eintragung oder ähnliches bedarf. Der Werkcharakter beginnt nach der Theorie der „kleinen Münze“ dabei nicht erst beim Buch, bei der ganzen Oper oder beim Gemälde – auch eine kleine Grafik, eine Webseitengestaltung oder eben die Online-Straßenkarte können urheberrechtlich geschützte Werke sein, sofern ihnen eine gewisse geistige Leistung zugrunde liegt. Nicht geschützt ist dagegen die reine Idee, solange sie noch nicht in Werkform – etwa durch Programmieren der Webseite – wahrnehmbar gemacht worden ist. Kein Werk in diesem Sinne ist etwa das ohne künstlerische Ambitionen geknipste Foto oder der Gesang einer Popdiva – dennoch gelten hierfür die dem Urheberrecht verwandten Leistungsschutzrechte, die weitestgehend genauso behandelt werden. Die dann bestehenden Rechte unterteilen sich im deutschen Urheberrecht in eine persönlichkeitsrechtliche und eine verwertungsrechtliche Seite.

a) Verwertungsrechte

(1) Zustimmung des Urhebers zum Gebrauch

Die Verwertungsrechte sorgen dafür, dass der Urheber selbst entscheiden kann, was mit seinem Werk passieren soll. Sie geben ihm das alleinige und ausschließliche Recht, das Werk zum Beispiel zu veröffentlichen, es zu kopieren oder es via Internet öffentlich zugänglich zu machen. Natürlich steht dahinter letztlich der Gedanke, dass der Urheber für sein Werk, das er der Allgemeinheit zur Verfügung stellt, auch entlohnt werden soll. Er kann daher über seine Verwertungsrechte in der Form verfügen, dass er anderen gegen eine Vergütung Nutzungsrechte, sogenannte Lizenzen, einräumt. Ein Nutzungsrecht zur Vervielfältigung und Verbreitung eines Schriftstückes ermächtigt damit zum Beispiel einen Verlag, den Text eines Autors zu drucken und zu veröffentlichen, im Gegenzug dafür erhält der Autor ein Honorar. Das Nutzungsrecht zur Zugänglichmachung im Internet kann der Autor dagegen z. B. einem anderem einräumen oder es selbst behalten. Die einzelnen Verwertungsrechte sind also voneinander unabhängig und können auch getrennt vergeben beziehungsweise genutzt werden.

Nutzungsrechte können in einfacher oder ausschließlicher Form erteilt werden. Wer ein einfaches Nutzungsrecht besitzt, darf damit das Werk in der vereinbarten Form nutzen, muss aber damit rechnen, dass auch andere ein solches einfaches Nutzungsrecht eingeräumt bekommen. Mit einem ausschließlichen Nutzungsrecht ist man dagegen alleiniger Inhaber der Rechte zur jeweiligen Werknutzung und kann anderen – selbst dem Urheber – die Nutzung verbieten. Gleichzeitig kann der Inhaber eines ausschließlichen Nutzungsrechtes jedoch selbst – mit Zustimmung des Urhebers – einfache Nutzungsrechte erteilen.

Ausschließliche Nutzungsrechte liegen in der Regel auch den sogenannten „Wahrnehmungsverträgen" zugrunde, die Urheber mit den Verwertungsgesellschaften abschließen. Damit ermächtigen sie die Gesellschaften, den Nutzern der Werke Nutzungsrechte in Form von Lizenzen einzuräumen und dafür Geld einzuziehen. Verwertungsgesellschaften gibt es für viele verschiedene Werkkategorien – so z.B. die GEMA, die VG Wort, die GVL und viele mehr. . Wenn erst die Einräumung eines Nutzungsrechtes eine Werknutzung erlaubt, bedeutet dies auch, dass jeder, der ein Werk ohne Nutzungsrecht verwendet, das Urheberrecht des jeweiligen Urhebers verletzt.

Eine Werknutzung liegt auch dann vor, wenn ein Werk nach eigenen Vorstellungen bearbeitet oder umgestaltet wird. Das ist etwa bei einer Verfremdung von bestehenden Gestaltungskonzepten oder bei der Bearbeitung fremder Grafikelemente oder Bilder der Fall. Hier ist stets die Einwilligung des Urhebers erforderlich, es sei denn, das andere Werk wird „frei benutzt". Unter einer freien Benutzung ist die Verwendung eines Werkes in einem eigenen selbstständigen Werk dann zu verstehen, wenn das ursprüngliche Werk hinter dem neuen Werk verblasst und nahezu nicht mehr als das ursprüngliche Werk wahrnehmbar ist. Eine freie Bearbeitung eines im Internet gefundenen Comicbildes läge also dann vor, wenn Grundzüge der Comicfigur in einer eigenständigen Bildgeschichte aufgingen. Für diese Art der Bearbeitung wäre eine Einwilligung nicht erforderlich. Das Grundprinzip, wonach vom Urheber für einige Verwertungshandlungen Nutzungsrechte erteilt werden, für andere dagegen nicht, liegt auch den Creative Commons-Lizenzen zugrunde. Hinter dem Begriff Creative Commons verbirgt sich eine Organisation, die verschiedene Lizenzvertragsmodelle für Urheber anbietet und dabei das Ziel verfolgt, einen fairen Ausgleich zwischen Urheberinteressen und einem freien Informationsfluss zu schaffen. Der Urheber, der die Verwertung seiner Werke selbst in die Hand nehmen möchte und insoweit die Dienste der Verwertungsgesellschaften nicht in Anspruch nimmt, hat hier die Wahl zwischen verschieden strengen Modellen. So kann er die Vervielfältigung und Verbreitung seiner Werke allen interessierten Nutzern erlauben, sofern diese ihn als Rechtsinhaber nennen. Gleichzeitig kann er aber auch eine gewerbliche Nutzung seiner Werke oder die Bearbeitung durch andere ausschließen. Unter einer solchen Creative Commons-Lizenz stehen zu großen Teilen auch die Angebote, die unter „flickr.com" veröffentlicht sind. Allerdings ist bei der Übernahme etwa von Bildern auf „flickr.com" stets zu überprüfen, ob die jeweils verwendete Lizenz die beabsichtigte Form der Verwendung (z.B. eine kommerzielle) tatsächlich erlaubt.

(2) Zustimmungsfreier Gebrauch - Schranken des Urheberrechts

Keine Regel gilt ohne Ausnahme – so ist auch das Urheberrecht nicht unbeschränkt anwendbar. Zahlreiche Ausnahmeregelungen, die Schranken des Urheberrechts, sorgen dafür, dass die Verwendung eines Werks nicht zustimmungspflichtig ist, wenn bestimmte Voraussetzungen erfüllt sind. Zurückzuführen ist dies auf das Regelungsziel des Urheberrechts, wonach die Urheber einerseits

nicht zum Verhungern verdammt sein dürfen, andererseits aber auch bestimmte Informationen der Allgemeinheit zukommen sollen, ohne dass ein Urheber dies verhindern kann. Diese „Schranken“ sind als Ausnahmeregelungen sehr eng auszulegen. Die wohl bekannteste Urheberrechtsschranke ist die der Privatkopie in § 53 Abs. 1 UrhG, wonach einzelne Vervielfältigungen für den privaten Gebrauch auch ohne ein entsprechendes Nutzungsrecht zulässig sind. Auch künftig gilt dies weiterhin sowohl für analoge als auch für digitale Kopien. Voraussetzung ist hier aber, dass die Kopiervorlage nicht von offensichtlich rechtswidriger Herkunft ist und dass die Kopien nicht zu einem Erwerbszweck genutzt werden. Eine Musikdatei, die ohne entsprechende Nutzungsrechte in einer P2P-Tauschbörse zugänglich gemacht wurde, darf damit genauso wenig kopiert werden wie ein Computerspiel, das zuvor unter Umgehen eines Kopierschutzes dupliziert worden ist. Ebenso ist die Kopie der privat erworbenen CD unzulässig, wenn diese Kopie anschließend bei eBay verkauft werden soll. Die kopierte CD, die der Schwester zum Geburtstag geschenkt werden soll, ist dagegen vom privaten Gebrauch noch mit umfasst. Anders als dies häufig vermutet wird, handelt es sich bei der Privatkopierschranke jedoch nicht um ein „Recht“, das eingeklagt werden könnte. So findet die Privatkopie ihrerseits ihre Schranken in technischen Schutzmaßnahmen wie etwa Kopierschutzmechanismen. Auch diese schützen das Urheberrecht, sodass auch derjenige, der unter Umgehung eines wirksamen Kopierschutzes eine vermeintliche Privatkopie herstellt, eine Urheberrechtsverletzung begeht.

Auch die journalistische Arbeit wird in § 49 UrhG durch Schranken des Urheberrechts begünstigt. So ist etwa die Internet-Veröffentlichung von Zeitungsartikeln und Rundfunkkommentaren zu aktuellen politischen, wirtschaftlichen oder religiösen Tagesfragen zulässig, sofern diese nicht mit einem Rechtevorbehalt versehen sind. Allerdings ist hierfür eine angemessene Vergütung zu zahlen, die wiederum durch die Verwertungsgesellschaften geltend gemacht werden. Wenn bei einer Berichterstattung über Tagesereignisse Werke wahrnehmbar sind, so ist auch dies in gebotenem Umfang zulässig. Dies betrifft etwa Kunstwerke, die im Zusammenhang mit einem Bericht über eine Ausstellungseröffnung zu sehen sind. Weitere Schranken betreffen etwa Schulunterricht und Forschung.

Eine weitere Schranke in § 51 UrhG betrifft das Zitatrecht. Es erlaubt im Rahmen des sogenannten „Kleinzitats“ Stellen eines bereits veröffentlichten Werkes in ein neues (Sprach-)Werk aufzunehmen und damit eigene Ansichten aussagekräftig zu untermauern. Voraussetzung hierfür ist jedoch die Schaffung eines eigenen urheberschutzfähigen Werkes und die inhaltliche Auseinandersetzung mit dem Zitierten. An einem Werk, das heißt an einer eigenen geistigen Schöpfung fehlt es, wenn sich etwa eine Webseite darauf beschränkt, Textstellen lediglich zu sammeln und für „gut“ oder „schlecht“ zu befinden. Bei einem selbst geschriebenen Text, der eine bestimmte eigene Aussage transportiert, kann dagegen ein Zitat zulässig sein, sofern es dem Zitatzweck dient. Der Zitatzweck liegt darin, eine eigene Aussage zu stützen und führt zum einen dazu, dass unbedingt eine inhaltliche Auseinandersetzung mit dem Zitierten erfolgen muss. Zum anderen hat der Zitatzweck auch Auswirkungen auf die zulässige Länge der Zitatstelle. Erlaubt ist insofern nur, was tatsächlich erforderlich ist. Sobald jedoch im äußeren Erscheinungsbild das Zitierte einen gleichen oder gar größeren Raum einnimmt als die inhaltliche Auseinandersetzung mit dem Zitat, kann man davon ausgehen, dass es sich nicht mehr um ein zulässiges Zitat handelt. In jedem Fall gilt bei einem Zitat die Pflicht, die Quelle des Zitierten mit anzugeben.

b) Das Urheberpersönlichkeitsrecht

Anders als die verwertungsrechtliche Seite, die dem Urheber sein Einkommen sichern soll, schützt das Urheberpersönlichkeitsrecht die persönliche Beziehung des Urhebers zu seinem Werk. So verpflichtet es etwa den Nutzer eines Werkes, den Namen des Urhebers nach dessen Wunsch zu nennen oder zu verschweigen. Bei Zitaten zwingt es zur Quellenangabe. Gleichzeitig schützt das Urheberpersönlichkeitsrecht das Werk vor Entstellung und sichert dem Urheber das Recht, bei „gewandelter Überzeugung" ein erteiltes Nutzungsrecht wieder zurückzurufen. Anders als die in Form von Nutzungsrechten übertragbaren Verwertungsrechte bleibt das Urheberpersönlichkeitsrecht immer beim Urheber und kann daher niemals verkauft oder übertragen werden. Spannend kann die Frage der Urhebernennung etwa dann werden, wenn auf einer Webseite ein Link „Inline" gesetzt wird, das heißt wenn fremde (urheberrechtlich geschützte) Inhalte nicht in einem separaten Fenster mit zugehöriger Webadresse, sondern im Frame der verlinkenden Webseite auftauchen. Dann ist nicht mehr erkennbar, zu wem beziehungsweise zu welcher eigentlich verlinkten Webseite die Inhalte gehören. Das Urheberpersönlichkeitsrecht auf Namensnennung ist damit verletzt.

4. Haftung

Aufgrund der Vielzahl der zu beachtenden Vorgaben bei der Bereitstellung eines eigenen Webangebots, besteht ein gesteigertes Haftungsrisiko. In der Praxis besonders häufig sind zivilrechtliche Ansprüche aufgrund einer Verletzung des Urheberrechts. Aber auch beleidigende sowie andere rechtswidrige Inhalte können neben zivilrechtlichen Ansprüchen auch eine strafrechtliche Verantwortlichkeit nach sich ziehen. Im Folgenden sollen daher die Grundlagen einer möglichen Haftung bezogen auf die Situation an Hochschulen und Forschungseinrichtungen näher beleuchtet werden.

a) Haftung für eigene Inhalte

Für die eigenen Inhalte ist die Hochschule nach den allgemeinen Gesetzen voll verantwortlich, § 7 Abs. 1 TMG. Die Hochschule haftet also zivilrechtlich für alle Rechtsverstöße auf ihren Webseiten, während strafrechtlich der jeweilige Autor persönlich verantwortlich ist. Eigene Inhalte sind jedenfalls alle offiziellen Seiten und Angebote der Hochschule und der zugehörigen Institutionen wie z.B. Fakultäten und Institute. Es kommt nicht darauf an, wer die Dateien tatsächlich erstellt hat, z.B. Mitarbeiter der Hochschule oder ein privates Unternehmen im Auftrag der Hochschule. Maßgeblich ist, ob aus der gesamten Gestaltung bei dem Benutzer der Eindruck erweckt wird, dass es sich um ein Angebot der Hochschule handelt. Erforderlich ist aber, dass die Verbreitung der Inhalte auf die Hochschule zurückzuführen ist. Erstellt etwa ein Student eigenmächtig eine Seite, die wie eine offizielle Seite der Hochschule aussieht, so gilt diese Seite natürlich nicht als eigener Inhalt der Hochschule.

Zu beachten ist, dass man sich auch fremde Inhalte zu Eigen machen kann, indem man etwa durch die besondere Form eines Hyperlinks eine Verbindung schafft oder die Inhalte direkt in eigene Seiten übernimmt und hierdurch für einen Außenstehenden der Eindruck entsteht, es handle sich um einen eigenen Inhalt des Seitenbetreibers. Bei der Bezugnahme auf fremde Inhalte sollte deshalb darauf geachtet werden, dass die Eigenschaft als Fremdangebot hinreichend deutlich wird.

b) Haftung für Hyperlinks

Sonderprobleme in Bezug auf die vorgenannten Grundsätze ergeben sich bei Verweisen auf fremde Webseiten. Zwar handelt es sich im Grundsatz um fremde Inhalte, auf die verwiesen wird, der eigentliche Verweis ist jedoch Bestandteil des eigenen Webangebots. Inwieweit nur der Verweis auf ein fremdes Angebot auf der eigenen Webseite zu einer Verantwortlichkeit des Verweisenden führen kann, ist derzeit eine der zentralen rechtlichen Fragen im Internet.

Vorschriften zur rechtlichen Verantwortlichkeit für Hyperlinks finden sich weder im TMG noch in sonstigen Gesetzeswerken. Dabei handelt es sich keineswegs um ein Versehen, vielmehr wurde bewusst auf eine spezielle Regelung über die Haftung für Hyperlinks verzichtet. Auch in der Mitteilung der Kommission zur „Strategie für einen europäischen digitalen Binnenmarkt“ vom 6.5.2015 bleibt die Frage der rechtlichen Beurteilung der Linkhaftung offen. Aufgrund des Fehlens einer Spezialregelung, wie etwa in § 10 TMG für den Host-Provider, gelten die allgemeinen Haftungsgrundsätze, wobei die spezifischen Besonderheiten von Hyperlinks im Rahmen der richterlichen Würdigung berücksichtigt werden können. Die Haftungsgrundsätze für Hyperlinks basieren daher auf europäischer Rechtsprechung und sind somit Ausfluss des Richterrechts.

Wie weit eine Haftung für Hyperlinks nach den allgemeinen Grundsätzen reichen kann und welche Einschränkungen aufgrund der Besonderheiten von Hyperlinks geboten sind, ist seit jeher in Literatur und Rechtsprechung heftig umstritten. Der EuGH hat schließlich im Rahmen eines Vorabentscheidungsverfahrens entschieden, dass die Verlinkungshandlung auf einen rechtmäßigen Inhalt keine Urheberrechtsverletzung darstellt und somit eine Haftung ausgeschlossen ist (EuGH, Urteil vom 13.2.2014 – C-466/12). Nachdem zunächst jedoch weiterhin unklar war, wie eine Verlinkung auf einen rechtswidrigen Inhalt urheberrechtlich zu behandeln ist, wurde diese Frage nun auch durch den EuGH (EuGH, Urteil vom 8.9.2016 – Rs. C-160/15) entschieden. Inhaltlich geht es in dieser Entscheidung um die Verlinkung einer Webseite, auf welche Fotos ohne Zustimmung des Rechteinhabers hochgeladen wurden. Der EuGH wich mit seiner Entscheidung von den Schlussanträgen des Generalanwalts ab und machte eine Haftung des Link-Setzenden von dessen Kenntnis respektive dem Kennenmüssen von der Rechtswidrigkeit der verlinkten Inhalte abhängig. Das bedeutet, dass der Link-Setzende nur haftet, wenn er Kenntnis hatte beziehungsweise unter üblichen Umständen Kenntnis hätte habe müssen, dass die Inhalte, auf die verlinkt wurde, ohne Erlaubnis des Rechteinhabers in das Internet eingestellt wurden. Fehlt diese Kenntnis oder das Kennenmüssen scheidet eine Haftung des Link-Setzenden hingegen aus, da keine öffentliche Wiedergabe im Sinne des UrhG vorliegt. Das Gericht führte weiter aus, dass die Kenntnis bei kommerziell tätigen Websites/Link-Setzern vermutet wird. Für einen Ausschluss der Haftung ist also eine Widerlegung dieser Vermutung erforderlich. Der EuGH gestaltet die Haftung von kommerziellen und nichtkommerziellen Link-Setzern also unterschiedlich aus.

Es ist somit bei der Frage einer Haftung bei Verlinkung auf rechtswidrige Inhalte zu unterscheiden, ob Kenntnis von der Rechtswidrigkeit des Inhalts besteht oder nicht. Im Strafrecht ist grundsätzlich vorsätzliches Handeln erforderlich, das heißt nur bei Kenntnis besteht eine Verantwortung. Daneben kommt bei Kenntnis eine zivilrechtliche Haftung auf Unterlassung beziehungsweise Schadensersatz in Betracht.

Zivilrechtlich kann auch der in Unkenntnis von der Rechtswidrigkeit des Inhalts vorgenommene Verweis mittels Hyperlink bei der Verletzung von Prüfpflichten zu einer Inanspruchnahme auf Beseitigung beziehungsweise Unterlassen führen. Hintergrund hierfür ist die so genannte allgemeine Störerhaftung, bei der berücksichtigt wird, dass der Link-Setzende das rechtswidrige Handeln eines Dritten durch die Verweisung objektiv unterstützt. Mit der Inanspruchnahme auf Unterlassung/Beseitigung soll der unterstützende Effekt der Linksetzung beseitigt werden. Auch wenn über die Störerhaftung nur eine Inanspruchnahme auf Unterlassen oder Beseitigung in Betracht kommt (das heißt im Ergebnis die Entfernung des Hyperlinks), kann eine Inanspruchnahme erhebliche finanzielle Konsequenzen haben. Kommt es zu einer anwaltlichen Abmahnung oder gar zu einem gerichtlichen Verfahren, fallen zusätzliche Kosten an, die bei den derzeit üblichen Streitwerten durchaus erheblich sein können.

Aus der bisherigen Rechtsprechung zur Haftung für Hyperlinks lässt sich für die Praxis folgende Richtschnur ableiten:

- Bei einer Verlinkung auf rechtswidrige Inhalte ist entscheidend, ob der Link-Setzende Kenntnis von der Rechtswidrigkeit hatte oder unter normalen Umständen zumindest hätte haben müssen (sogenannte Kennenmüssen). Bei Webseiten mit Gewinnerzielungsabsicht, die eine Verlinkung setzen, wird diese Kenntnis vermutet. Eine Widerlegung der Vermutung ist jedoch möglich. Demnach sollten Hyperlinks nicht gesetzt werden, wenn Kenntnis von der Rechtswidrigkeit des Inhalts auf der verlinkten Seite besteht (z. B. nationalsozialistische Propagandaseiten oder Tauschbörsen). Eine Ausnahme ist lediglich dann gegeben, wenn das Setzen des Hyperlinks auf einen bestimmten Inhalt unter eine gesetzliche Privilegierung fällt.
- Bei fehlender Kenntnis von der Rechtswidrigkeit verlinkter Inhalte kommt es im Rahmen der Störerhaftung darauf an, ob zumutbare Prüfungspflichten beim Setzen oder bei der Aufrechterhaltung des Links verletzt wurden (Grundlegend: BGH, Urteil vom 1.4.2004 – Az. I ZR 317/01 – Schöner Wetten, MMR 2004, 529). Der Umfang der Prüfungspflichten richtet sich dabei nach dem Gesamtzusammenhang, in dem der Hyperlink verwendet wird, dem Zweck des Hyperlinks sowie danach, welche Kenntnis der Link-Setzende von Umständen hat, die dafür sprechen, dass die Webseite oder der Internetauftritt, auf die der Link verweist, rechtswidrigem Handeln dient und welche Möglichkeiten er hat, die Rechtswidrigkeit dieses Handelns in zumutbarer Weise zu erkennen. Im Ergebnis kommt es damit ganz wesentlich auf die subjektive Erkennbarkeit für den Link-Setzenden an. Es wird deshalb von keinem juristischen Laien erwartet, dass er vor dem Setzen eines Hyperlinks das fremde Angebot auf etwaige Marken- oder Urheberrechtsverletzungen überprüft, da er damit in der Regel überfordert sein dürfte. Anders sieht die Situation jedoch dann aus, wenn sehr nahe liegende Umstände auf der fremden Webseite auf ein rechtswidriges Handeln hindeuten. Mit anderen Worten: Wenn der gesunde Menschenverstand seine Zweifel an der Rechtmäßigkeit eines fremden Inhalts anmeldet, sollte eine nähere Prüfung im Vorfeld erfolgen oder auf die Setzung eines Hyperlinks lieber ganz verzichtet werden. Ernsthafte Zweifel sind beispielsweise bei dem damaligen Streaming-Portal *kino.to* gegeben, wo aktuelle Kinofilme kostenlos angeboten wurden. Die fehlende Zustimmung des Rechteinhabers, die Filme öffentlich zugänglich zu machen und kostenlos anzubieten, war für einen durchschnittlichen Internetnutzer ersichtlich.

Jedoch auch dann, wenn beim Setzen des Hyperlinks keine Prüfungspflichten verletzt werden, kann eine Störerhaftung begründet sein, wenn ein Hyperlink aufrechterhalten bleibt, obwohl eine nunmehr zumutbare Prüfung, insbesondere nach einer Abmahnung oder Klageerhebung ergeben hätte, dass mit dem Hyperlink ein rechtswidriges Verhalten unterstützt wird. Im Klartext heißt das, dass man auch bei einer vorher fehlenden Erkennbarkeit spätestens nach dem Hinweis (Abmahnung, Klageerhebung) auf eine mögliche Rechtswidrigkeit des verlinkten Inhalts die Pflicht zu einer näheren Überprüfung hat. Wird der Link trotzdem aufrechterhalten und unterbleibt eine nähere Prüfung, ist die Prüfungspflicht nach Ansicht der zitierten BGH-Entscheidung verletzt. Handelt es sich tatsächlich um einen rechtswidrigen Inhalt, besteht nach der gegenwärtigen Rechtsprechung eine Störerhaftung des Link-Setzenden.

- Weiterhin nicht geklärt ist, ob und inwieweit der Link-Setzende zu einer regelmäßigen Überprüfung auf nachträgliche Veränderungen des verlinkten Inhalts verpflichtet ist. Im Bereich des Strafrechts kommt ohnehin erst eine Haftung ab Kenntnis in Betracht. Bei der zivilrechtlichen Haftung kann dagegen nach einigen Rechtsauffassungen eine Pflicht zur regelmäßigen Überprüfung der Inhalte bestehen, so dass eine Haftung bei nachträglicher Veränderung des Inhalts der verlinkten Seite trotz Unkenntnis von dem neuen Inhalt möglich ist. Es spricht jedoch einiges dafür, dass auch hier in Bezug auf die Prüfungspflichten die oben dargestellten Kriterien des BGH anzulegen sind. Auch andere Gerichte haben in der letzten Zeit entschieden, dass der verlinkte Inhalt nachträglich nicht daraufhin zu überprüfen ist, ob er noch immer rechtmäßig ist, wenn diese Prüfung zum Zeitpunkt der Einrichtung des Links vorgenommen wurde. Erst bei Vorliegen eindeutiger Anhaltspunkte für oder bei Kenntnis von der Rechtswidrigkeit besteht eine erneute Prüf- und gegebenenfalls Löschungspflicht. Beispielhaft sei auf die Entscheidung des OLG München (OLG München, Urteil vom 29.4.2008 – Az. 18 U 5645/07) hinzuweisen. Danach bestehe eine nachträgliche Prüfungspflicht grundsätzlich nicht, solange es keinen besonderen Anlass für den Link-Setzer gebe, von einer Änderung der fremden Inhalte beziehungsweise von deren nachträglich eingetretener Rechtswidrigkeit auszugehen. Somit bewirkt der Hinweis auf eine inzwischen eingetretene Rechtswidrigkeit nur, dass die Prüfungspflicht entsteht. Da bis zu diesem Zeitpunkt eine solche Pflicht nicht bestand und daher auch nicht verletzt werden konnte, begründet der Hinweis des möglicherweise Verletzten für sich gesehen noch keinen Kostenerstattungsanspruch.
- Der BGH hat bereits in einer im letzten Jahr erschienenen Entscheidung zum Lauterkeitsrecht ein „notice and take down“-Verfahren für Verlinkungen angenommen (BGH, Urteil vom 18.6.2015 – Az. I ZR 74/14). Der Link-Setzende soll nach Ansicht des BGH haften, wenn er Kenntnis von der Rechtsverletzung hat oder in Kenntnis gesetzt wird und nicht reagiert. Es sei nicht erforderlich, dass eine klare Rechtsverletzung vorliegt. Der Link-Setzenden trage das Risiko der rechtlichen Beurteilung und wird die gesamte Prüfpflicht auferlegt. Eine derartige Lösung würde die Interessen des Link-Setzenden weitgehend zurückstellen und ihm wie bereits oben erwähnt zu starke Prüfpflichten auferlegen. Es sollte im Sinne des TMG auf eine offensichtliche Rechtswidrigkeit abgestellt werden.

c) Haftung beim „Framing“

Ein weiteres Sonderproblem in diesem Zusammenhang ergibt sich bei dem sogenannten „embedded Linking“ oder auch „Framing“. Hierbei findet keine Weiterleitung auf eine fremde Seite statt, sondern die Inhalte werden mit Hilfe eines Rahmens direkt in die Seite des Linkverwenders eingebaut. Der Inhalt liegt immer noch auf einem fremden Server und wird bei Abruf von dort angefordert.

Für den Nutzer einer Webseite kann der Eindruck entstehen, dass die Inhalte von dem Webseitenbetreiber selbst zur Verfügung gestellt wurden, obwohl sie von einer Drittwebseite stammen. Jedoch betont der EuGH in seiner Rechtsprechung, dass dieser Anschein bei der urheberrechtlichen Beurteilung keine Rolle spiele. Zudem sei das Einbetten eines rechtmäßigen Inhaltes mit Hilfe der Framing-Technik urheberrechtlich zulässig und die Haftung des Nutzers, welcher sich der Framing-Technik bedient, sei ausgeschlossen (EuGH, Beschluss vom 21.10.2014 – Rs. C-348/13).

Offen bleibt, ob eine solche Einbindungsfreiheit auch besteht, wenn ein rechtswidriger Inhalt eingebunden wird. Nach derzeitiger Ansicht des BGH liegt bei einer solchen Konstellation eine Urheberrechtsverletzung seitens des Link-Setzenden vor (BGH, Urteil vom 9.7.2015 – Az. I ZR 46/12). Dieser muss für seine Verlinkungshandlung haften. Das gilt nach dem jüngsten Urteil des EuGH in diesem Rechtskontexts (EuGH, Urteil vom 8.9.2016 – Rs. C-160/15) wohl zumindest bei Kenntnis beziehungsweise Kennenmüssen von der Rechtswidrigkeit. Die dort aufgeführten Grundsätze wird man auch auf die Haftung beim „Framing“ übertragen können. Insoweit kann zur Haftung beim Framing auf die obige Richtschnur verwiesen werden. Es ist zu einem sorgfältigen Umgang mit unsicheren Quellen zu raten. Bei Unsicherheiten sollte auf eine Einbindung verzichtet oder ein Einverständnis des Rechteinhabers eingeholt werden.

d) Sonderfall: Ehrverletzende Äußerungen auf Webseiten/Gegendarstellung

Über das Internet können Äußerungen und Tatsachen verbreitet werden, die die persönliche Ehre von Menschen verletzen. Da die Veröffentlichung auf einer Webseite eine ähnliche Wirkung haben kann wie bei einem Presseerzeugnis, bestimmt § 56 RStV einen Anspruch des Betroffenen auf Gegendarstellung bezüglich Tatsachenbehauptungen auf der Webseite, wenn es sich dabei um Telemedien mit journalistisch-redaktionell gestalteten Angeboten handelt, in denen insbesondere vollständig oder teilweise Inhalte periodischer Druckerzeugnisse in Text oder Bild wiedergegeben werden.

Die wenigsten Webseiten von Hochschulen erfüllen diese Anforderungen, weil sie keine redaktionell gestalteten Beiträge enthalten, sondern der Inhalt in erster Linie der individuellen Information zu bestimmten Fragen dient. Um solche Telemedien handelt es sich aber z.B., wenn der Inhalt einer Universitätszeitung zum Abruf im Internet bereitgestellt wird. Der Gegendarstellungsanspruch ist nur einschlägig bei Tatsachenbehauptungen, nicht jedoch bei Meinungsäußerungen. Darüber hinaus bestehen keine weiteren Voraussetzungen; insbesondere ist nicht erforderlich, dass die behauptete Tatsache tatsächlich falsch ist. Nur in bestimmten Ausnahmefällen entfällt der Anspruch gemäß § 56 Abs. 2 RStV.

Ganz allgemein kann ferner der Betroffene die Unterlassung (das heißt die Entfernung des beanstandeten Textes) von ehrverletzenden Äußerungen auf Webseiten jeglicher Art gemäß §§ 12, 862, 1004 BGB analog verlangen. Ob es sich um abfällige Werturteile (Beleidigungen) oder Tatsachenbehauptungen handelt, ist dabei unerheblich. Erforderlich ist aber immer eine Äußerung, die tatsächlich die Ehre der betroffenen Person verletzt. Dies ist bei der Behauptung wahrer Tatsachen regelmäßig nicht der Fall, außer sie beziehen sich auf die Privat- oder Intimsphäre des Betroffenen. Bei Tatsachenbehauptungen kommt es also anders als beim Gegendarstellungsanspruch auf die Wahrheit der Behauptungen an. Wird eine unwahre ehrenrührige Tatsache über eine Person behauptet, kann neben dem Anspruch auf Unterlassung auch ein Anspruch auf Widerruf gemäß §§ 12, 862, 1004 BGB analog bestehen, das heißt die äußernde Person muss auf derselben Webseite die unwahre Behauptung widerrufen.

e) Wer haftet?

(1) Zivilrechtliche Haftung

Die bei der Bereitstellung von Inhalten in Betracht kommenden zivilrechtlichen Ansprüche sind überwiegend auf Schadensersatz und Unterlassung (das heißt meistens Sperrung der rechtsverletzenden Inhalte) gerichtet. Typische Fälle, die solche Ansprüche auslösen, sind z. B. die Verletzung von Urheber- oder Markenrechten sowie ehrverletzende Äußerungen. Soweit das Rechenzentrum für derartige Rechtsverletzungen (mit-) verantwortlich ist, haftet grundsätzlich die Einrichtung/Hochschule beziehungsweise deren Rechtsträger als juristische Person. Ein Mitarbeiter, der beispielsweise eine Webseite erstellt und dabei eine Rechtsverletzung begangen hat, haftet in der Regel nicht persönlich, wenn dies in Ausübung seiner Diensttätigkeit geschah. Bei Beamten folgt dies aus den Grundsätzen der Amtshaftung gemäß Art. 34 Grundgesetz (GG); Angestellte haben grundsätzlich einen Haftungsfreistellungsanspruch gegen den Arbeitgeber. Davon unberührt bleiben allerdings eventuelle Haftungsrückgriffe der Hochschule gegen den verantwortlichen Mitarbeiter aus dem Dienstverhältnis. Rückgriffe kommen in Betracht, wenn Dienstpflichten vorsätzlich oder in grobem Maß verletzt wurden und der Hochschule dadurch ein Schaden entstanden ist.

(2) Strafrechtliche Verantwortlichkeit

Strafrechtlich können nur natürliche Personen verantwortlich sein, nicht die Hochschule als solche. Für Inhalte auf den offiziellen Seiten der Hochschule ist strafrechtlich der jeweilige Autor voll verantwortlich. Es kommt aber nicht allein darauf an, wer eine Seite tatsächlich erstellt hat. Die Verantwortung für Verstöße gegen Strafgesetze trägt auch der Auftraggeber, wenn für ihn Seiten durch andere Personen erstellt wurden, deren Inhalt er kennt.

(3) Haftung für Organisationseinheiten der Hochschulen

Hinsichtlich der Haftung für eigene Inhalte ist zwischen dem Innen- und dem Außenverhältnis zu unterscheiden. Intern sind natürlich die Fachbereiche, Institute und sonstigen Organisationseinheiten selbst für den Inhalt der von ihnen gestalteten Internet-Seiten verantwortlich. Im Außenverhältnis tritt die Hochschule jedoch als eine einzige Anstalt des öffentlichen Rechts auf, die interne Aufteilung in verschiedene Einheiten ist im Verhältnis zu anderen Personen unerheblich. So bestimmt z.B. § 26 Abs. 2 S. 1 Hochschulgesetz NW, dass der Fachbereich – unbeschadet der Gesamtverantwortung der

Hochschulen und der Zuständigkeiten der zentralen Hochschulorgane und Gremien – für sein Gebiet die Aufgaben der Hochschule erfüllt. Daher haftet die Hochschule zivilrechtlich für jede Rechtsverletzung, die von einer Internet-Seite einer ihrer untergeordneten Organisationseinheiten ausgeht. Hinsichtlich einer Verpflichtung zum Schadensersatz oder zur Unterlassung kann nicht auf die eigenständige Gestaltung der Seiten durch die Einheit verwiesen werden, selbst wenn diese einen eigenen Server betreibt. Derartige Hinweise auf den Seiten entfalten keine Wirkung. Gegenüber außenstehenden Personen haftet immer die Hochschule.

Soweit Aufgaben von Einrichtungen wahrgenommen werden, die keine organisatorischen Untergliederungen der Hochschulen sind, sondern selbständige juristische Personen des öffentlichen Rechts (wie z.B. Studierendenwerke), sind auch hier diese selbst und nicht etwa die Hochschule als Diensteanbieter i.S.d. § 2 Satz 1 Nr. 1 TMG anzusehen und können als solche haftbar gemacht werden.

f) Rechtliche Bedeutung von Disclaimern

Angesichts der oben dargelegten Haftungsrisiken findet sich auf vielen Internetangeboten ein Haftungsausschluss (sogenannte Disclaimer). Hierdurch soll eine Haftung für die Vollständigkeit, Richtigkeit, Aktualität etc. der angebotenen Inhalte ausgeschlossen werden. Derartige Haftungsausschlüsse, die sich auf die eigenen Online-Inhalte beziehen, sind in der Regel rechtlich ohne Bedeutung, schaden jedoch auch nicht. Wichtiger ist die deutliche Abgrenzung der eigenen Inhalte zu fremden Inhalten, die auf dem eigenen Server bereitgehalten werden (Web-Hosting), und zu fremden externen Angeboten, auf die per Hyperlink verwiesen wird. Allerdings muss sich die Distanzierung von fremden Inhalten aus der Gestaltung der Seite und der Links ergeben; eine entsprechende Klarstellung im Disclaimer kann nur eines von vielen Merkmalen sein, um ein „Zueigenmachen“ fremder Inhalte zu verhindern. Der Seitenbetreiber kann eine ausreichende Distanzierung unter anderem dadurch erreichen, dass er die Links in einer eigenen Rubrik aufführt und nicht in Zusammenhang mit eigenen Aussagen stellt, oder indem er auf Seiten verlinkt, die zum jeweiligen Thema anderer Auffassung sind. Auch das Verlinken auf der Startseite („Surface-Linking“) statt auf einzelne Unterseiten oder Dokumente („Deep-Linking“) spricht für eine Distanzierung von einzelnen fremden Inhalten. Wird eine Distanzierung gewünscht, sollte auf ein Framing verzichtet und ein neues Browserfenster geöffnet werden, damit deutlich wird, dass es sich um eine externe Seite handelt.

5. Verdacht auf Straftaten

Die Einrichtungen eines Rechenzentrums können zur Begehung verschiedener Straftaten missbraucht werden. In Betracht kommen z. B. "Hacker"-Delikte wie das Ausspähen von Daten gemäß § 202a Strafgesetzbuch (StGB), Computersabotage gemäß § 303b StGB oder Computerbetrug gemäß § 263a StGB, die Verbreitung rechtswidriger Inhalte oder die Verbreitung beziehungsweise Verschaffung von Kinderpornographie gemäß § 184b StGB. Besteht der Verdacht, dass ein Benutzer über die Einrichtungen des Rechenzentrums Straftaten begangen hat, so sollten keine Ermittlungen auf eigene Faust angestellt werden. Es sollten nur Beweise gesichert werden (Ausdruck und Speicherung der Dateien, Informierung anderer Mitarbeiter als Zeugen etc.), aber keine neuen Beweise eigenmächtig ermittelt werden. Stattdessen ist frühzeitig die Polizei oder Staatsanwaltschaft zu

informieren, um gegebenenfalls Anzeige zu erstatten. Der weitere Verlauf des Ermittlungsverfahrens wird dann von der Staatsanwaltschaft bestimmt.

Ferner können die Mitarbeiter des Rechenzentrums in behördliche Maßnahmen dergestalt eingebunden werden, dass sie z.B. visuelle Wahrnehmungen beziehungsweise Beobachtungen des Nutzerverhaltens an die Staatsanwaltschaft oder Polizei zukünftig weitergeben. Diese Kooperationen im Sinne eines. "Augen-und-Ohren-offen-halten" ist unbedenklich. Bei einer weitergehenden Zusammenarbeit sollte eine Anordnung von der Staatsanwaltschaft beziehungsweise dem Behördenleiter eingeholt werden. Auf jeden Fall sollte beim Verdacht begangener oder bevorstehender Straftaten zunächst die zuständige Stelle informiert werden und die weitere Vorgehensweise abgestimmt werden.

6. Maßnahmen bei Beschwerden/Hinweisen auf rechtswidrige Inhalte

Durch interne Organisationsmaßnahmen muss sichergestellt werden, dass eingehende Hinweise und Beschwerden auf rechtswidrige Inhalte umgehend bearbeitet werden können. Bei einer eingehenden Beschwerde ist zunächst zu prüfen, ob die beanstandeten Inhalte tatsächlich der Institution zuzurechnen sind. Befindet sich der beanstandete Inhalt nicht im Einflussbereich der Hochschule oder Forschungseinrichtung, braucht nichts unternommen zu werden. Anders kann die Situation zu bewerten sein, wenn auf externe Inhalte verlinkt wird und die Links so in das eigene Angebot eingebettet werden, dass der Eindruck entsteht, die Hochschule mache sich die fremden Inhalte faktisch zu Eigen (siehe oben); in diesem Fall sind die verlinkten Inhalte zu überprüfen und die Links gegebenenfalls zu löschen. Befindet sich der beanstandete Inhalt auf den Servern der Einrichtung, muss auch dann etwas unternommen werden, wenn es sich um fremde Inhalte handelt, für die lediglich Speicherplatz zur Verfügung gestellt wird (Hosting, Foren, Blogs). Wird der Anbieter von Speicherplatz nach Erlangung der Kenntnis nicht unverzüglich tätig, um rechtswidrige Informationen zu entfernen oder den Zugang zu ihnen zu sperren, ist er nach § 10 TMG genauso verantwortlich, als würde es sich um seinen eigenen Inhalt handeln (siehe ausführlich Kapitel: Bereitstellung von Speicherplatz für fremde Inhalte). Handelt es sich um eigene Inhalte, die im Auftrag der Institution oder ihrer Mitglieder (z. B. Hochschullehrer) auf einem externen Server bereitgestellt werden, besteht aufgrund der Verantwortlichkeit für die eigenen Inhalte gemäß § 7 Abs. 1 TMG (siehe oben Haftung) ebenfalls Handlungsbedarf.

a) Vorläufige Sperrung und eingehende Prüfung

Handelt es sich um eigene Inhalte der Institution, ist die Begründetheit des Vorwurfs der Rechtswidrigkeit zu prüfen. Bestehen nach der Ansicht eines juristischen Laien auch nur geringste Zweifel an der Rechtmäßigkeit, so sollte die betroffene Datei umgehend vorläufig gesperrt werden. Die zeitweise Sperrung einer Datei mit rechtmäßigen Inhalten hat grundsätzlich keine negativen Konsequenzen, zumal wenn die Maßnahme durch eine entsprechende Regelung in der Benutzungsordnung gedeckt ist. Dagegen kann die unterbleibende Sperrung von rechtswidrigen Inhalten eine erhebliche Schadensersatzverpflichtung und eine Strafbarkeit der verantwortlichen Personen zur Folge haben. Nach erfolgter vorläufiger Sperrung sollte eine genaue Prüfung der Vorwürfe durch das Justitiariat erfolgen. Ist der beanstandete Inhalt nicht rechtswidrig, kann die Datei wieder freigegeben werden, ansonsten sollte sie natürlich endgültig vom Server entfernt

werden. Die weiteren Konsequenzen bestimmen sich nach der Lage des Einzelfalls. Dabei ist auch danach zu unterscheiden, um welche Art von Inhalten es sich handelte.

b) Interne Sanktionen

Soweit es sich um vorsätzliche Rechtsverstöße handelt, können gegen Mitarbeiter der Institution arbeitsrechtliche beziehungsweise disziplinarrechtliche Maßnahmen eingeleitet werden, gegen andere Mitglieder (insbesondere Studierende) können – soweit vorgesehen – Sanktionen aufgrund der Benutzungsordnung ergehen. Bei strafbaren Inhalten kann auch eine Strafanzeige gegen den Autor der Seite erstattet werden.

c) Abmahnungen durch Rechtsanwälte

Es kommt immer wieder vor, dass Hochschulen und andere wissenschaftliche Einrichtungen von Rechtsanwälten wegen angeblicher Rechtsverletzungen auf Internetseiten abgemahnt werden. Häufig werden solche Abmahnungen wegen der nicht lizenzierten Verwendung urheberrechtlich geschützter Elemente auf Webseiten ausgesprochen.

Dabei wird oft innerhalb einer kurzen Frist (z. B. 10 Tage) die Abgabe einer sogenannte strafbewehrten Unterlassungserklärung (Vertragliche Verpflichtung zur Unterlassung verbunden mit dem Versprechen zur Zahlung einer festgelegten Strafe für den Fall eines Verstoßes), der Ersatz der Kosten für die Tätigkeit des Anwalts und je nach Einzelfall Schadensersatz verlangt. Auch wenn kein Schadensersatz verlangt wird, kann eine anwaltliche Abmahnung mit erheblichen Kosten verbunden sein. Die dem Verletzten zu erstattenden Anwaltskosten bemessen sich nach der Höhe des Streitwerts. In Anbetracht dessen, dass insbesondere im Bereich des Urheberrechts schnell Streitwerte über 10.000 € erreicht werden, können hierbei Anwaltskosten im vierstelligen Bereich auflaufen. Erhält die Institution allerdings durch die Abmahnung erstmals Kenntnis von einem rechtswidrigen fremden Inhalt (insbesondere private Homepages von Studierenden) und wird dieser umgehend gesperrt, entfällt eine Verantwortlichkeit nach § 10 TMG, sodass kein Anspruch auf Schadensersatz besteht und auch eine strafrechtliche Verantwortlichkeit entfällt. Der Anspruch auf Unterlassung und somit auch der Anspruch auf Ersatz der Anwaltskosten durch die Institution ergeben sich dagegen aus der allgemeinen Störerhaftung, welche durch § 10 TMG nicht ausgeschlossen wird. Ob und wieweit Prüfungspflichten bestehen, ergibt sich daraus, wieweit diese der Institution zumutbar sind. Proaktive Kontrollen dürften zu umfassend und damit unzumutbar sein. Anders kann der Fall liegen, wenn bereits ähnlich Rechtsverletzungen begangen worden sind oder wenn die fremden Inhalte (z. B. Foren) ein Thema behandeln, welches Rechtsverletzungen erwarten lässt (hierzu näher Kapitel IV. Bereitstellung von Speicherplatz für fremde Inhalte).

Die gestellten Forderungen sollten keinesfalls voreilig erfüllt werden. Die Abgabe einer Unterlassungserklärung kann sehr gefährlich sein, weil selbst bei einer Zuwiderhandlung ohne Verschulden die meist beträchtliche Vertragsstrafe fällig werden kann. Zunächst sollte rechtlich geklärt werden, ob die behauptete Rechtsverletzung tatsächlich vorliegt. Bei Vorliegen einer Rechtsverletzung kann zudem noch geprüft werden, ob die Höhe der geltend gemachten Ersatzansprüche angemessen ist. In jedem Fall ist es zu empfehlen, das Justitiariat hinzuzuziehen.

7. Datenschutzrechtliche Anforderungen

a) Anfallende personenbezogene Daten auf der Ebene der Inhaltsdienste

Die §§ 11 ff. TMG regeln nunmehr die datenschutzrechtlichen Vorgaben für alle Telemedien. Eine abweichende Regelung enthält das TMG in § 11 Abs. 3 nur für Telemedien, die überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, wie E-Mail-Dienste und Internet-Access, für die primär die datenschutzrechtlichen Regelungen in §§ 91 ff. Telekommunikationsgesetz (TKG) für Anbieter von Telekommunikationsleistungen Anwendung finden (Siehe Kapitel II). Für im Netz angebotenen Content gelten aber die Vorgaben aus §§ 11 ff. TMG.

Nach diesen Vorgaben ist eine automatisierte Erfassung des Nutzerverhaltens über das Ende der jeweiligen Nutzung hinaus grundsätzlich unzulässig.

Nutzungsprofile für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Teledienste durch gezieltes „Logging“, dürfen nach § 15 Abs. 3 TMG nur bei der Verwendung von Pseudonymen erstellt werden. Der Nutzer hat hiergegen ein Widerspruchsrecht auf das er hingewiesen werden muss. Des Weiteren dürfen die so gewonnenen Nutzungsprofile nicht mit den Daten über den Träger des Pseudonyms zusammengeführt werden.

Im Übrigen gilt auch nach den datenschutzrechtlichen Vorgaben im TMG, dass alle personenbezogenen Nutzungsdaten, die während der Nutzung eines Dienstes entstehen, grundsätzlich nach dem Ende der jeweiligen Nutzung zu löschen sind, es sei denn, dass die weitere Verwendung der Daten durch eine gesetzliche Erlaubnis oder eine Einwilligung der betroffenen Person gedeckt ist.

Eine gesetzliche Erlaubnis besteht beispielsweise, soweit die Nutzungsdaten gemäß § 15 Abs. 4 TMG für Zwecke der Abrechnung mit dem Nutzer erforderlich sind. Die Abrechnungszwecke beziehen sich hierbei auf die Nutzung eines Dienstes (z. B. eines wissenschaftlichen Informationsdienstes) und nicht etwa auf Leistungen auf der Transportebene wie dem Internetzugang, welche durch das TKG erfasst werden (siehe hierzu Kapitel II: Datentransfer in Netzen und Übermittlung von E-Mails). In der Regel wird es zu Abrechnungszwecken ausreichen, die unter der für den Dienst zugeteilten Benutzerkennung in Anspruch genommenen entgeltlichen Dienstleistungen im Abrechnungszeitraum zu verwenden.

Liegen zu dokumentierende tatsächliche Anhaltspunkte vor, dass Dienste des Anbieters von bestimmten Nutzern in der Absicht in Anspruch genommen werden, das Entgelt nicht oder nicht vollständig zu entrichten, darf der Anbieter nach § 15 Abs. 8 TMG die personenbezogenen Daten dieser Nutzer über das Ende des Nutzungsvorgangs hinaus verarbeiten und nutzen, soweit dies für Zwecke der Rechtsverfolgung erforderlich ist. Für eine Erhebung und Nutzung über die bestehenden Erlaubnistatbestände hinaus, ist regelmäßig eine Einwilligung des Nutzers erforderlich, die den in § 4a BDSG genannten Voraussetzungen genügen muss. Unter den Voraussetzungen von § 13 Abs. 2 TMG kann die Einwilligung auch elektronisch erklärt werden. Für die Praxis der Rechenzentren im Deutschen Forschungsnetz bedeutet dies insbesondere, dass Interaktionen des Nutzers mit dem

jeweiligen Diensteanbieter regelmäßig nicht protokolliert werden dürfen. Damit sind sowohl Logfiles, die den Abruf eigener Web-Inhalte oder Dateien durch externe Nutzer aufzeichnen, als auch Logfiles, die den "click-stream" der eigenen Nutzer beim Abruf externer Angebote protokollieren, grundsätzlich unzulässig, soweit personenbezogene Daten gespeichert werden. Anonymisierte Abrufstatistiken sind hingegen unbedenklich (z.B. Protokollierung der Top- oder Second-Level-Domain oder der IP-Adresse des Abrufenden, soweit ein Rückschluss auf den jeweiligen Nutzer nicht ohne weiteres möglich ist).

Insgesamt noch unklar ist, welche Auswirkungen die EU-Datenschutzgrundverordnung auf die oben gemachten Ausführungen haben wird. Diese ist ab dem 25.05.2018 anwendbar.

b) Rechtliche Aspekte zum Umgang mit Mitarbeiterdaten im Internet

Zumeist als Service für interessierte externe Dritte gehen immer mehr Hochschulen und wissenschaftliche Einrichtungen dazu über, auch persönliche Daten von Beamten, Bediensteten, Angestellten und Arbeitern (im Folgenden Mitarbeiter) auf der Homepage zu veröffentlichen. Ein Recht dazu hat der Dienstherr/Arbeitgeber aufgrund des Dienst- beziehungsweise Arbeitsvertrages. Aber: Die Veröffentlichung stellt juristisch betrachtet eine „Übermittlung“ personenbezogener Daten dar. Demnach ist das Datenschutzrecht zu beachten, wonach die Daten nur mit vorheriger Einwilligung der betroffenen Mitarbeiter ins Internet gestellt werden dürfen. Eine Ausnahme vom Erfordernis der Einwilligung sehen jedoch auch die Datenschutzgesetze vor. Entscheidend dafür sind einerseits die Funktion des Mitarbeiters und andererseits die konkreten Angaben.

Regelungen zum Umgang mit Mitarbeiterdaten enthalten das Bundesdatenschutzgesetz (BDSG) und die Datenschutzgesetze der Bundesländer. Für die Publikation von Mitarbeiterdaten auf der Homepage haben die internetspezifischen Datenschutzregelungen in §§ 11 ff. TMG keine Relevanz, da dort für diesen Sachverhalt keine speziellen Regelungen getroffen sind. Zu beachten ist, dass das BDSG für alle öffentlichen Stellen des Bundes (§ 1 Abs. 2 Nr. 1 BDSG) gilt. Darunter fallen beispielsweise bundesunmittelbare Körperschaften und Stiftungen des Bundes. Auch sogenannte „nicht-öffentliche“ Stellen haben das BDSG zu beachten. Darunter fallen alle Unternehmen, Organisationen und Einrichtungen, die in einer privatrechtlichen Form betrieben werden.

Für Hochschulen (Universitäten und Fachhochschulen) gilt im Regelfall nicht das BDSG; sie müssen vielmehr die Vorgaben des jeweiligen Datenschutzgesetzes ihres Bundeslandes beachten. Zwar stimmen BDSG und die Landesdatenschutzgesetze in vielen Punkten überein, es gibt aber auch zahlreiche Abweichungen. Für die Mitglieder des DFN-Verein hat die Unterscheidung zur Konsequenz, dass jedes Mitglied individuell anhand der Rechtsform ermitteln muss, ob das BDSG oder das jeweilige Landesdatenschutzgesetz zur Anwendung kommt.

IV. Rechtslage bei der Zurverfügungstellung von Speicherplatz für fremde Inhalte

1. Einführung

Dieses Kapitel widmet sich rechtlichen Fragen, die sich im Zusammenhang mit der Bereitstellung von Speicherplatz für fremde Inhalte häufig stellen. Im Hochschulbereich kommt dies unter anderem im Zusammenhang mit dem Angebot von Speicherplatz auf den Hochschulservern für private Seiten von Studierenden oder studentischen Initiativen und Cloud-Speicher-Diensten wie „sciebo“ vor. Aber auch bei Meinungsforen oder Handelsplattformen wird innerhalb eines eigenen Webangebots Speicherplatz für fremde Inhalte bereitgestellt. In den genannten Fällen unterliegen die Einrichtungen den rechtlichen Vorgaben für Host-Provider. Im Rahmen der Tätigkeit der Host-Provider wird durch die gesetzlichen Grundlagen berücksichtigt, dass mit dem „Hosting“ im Kern nur eine technische Dienstleistung erbracht wird. Die Verantwortlichkeit für die rechtskonforme Gestaltung der Inhalte und die Einhaltung der rechtlichen Anforderungen an Webangebote (z. B. Impressumspflicht) obliegt grundsätzlich demjenigen, der den Inhalt auf dem zur Verfügung gestellten Speicherplatz als Anbieter bereitstellt. Dieser Grundsatz erfährt dennoch einige Durchbrechungen. Diese sollen im Folgenden zusammen mit weiteren wichtigen rechtlichen Aspekten dargestellt werden.

2. Haftung

Der Gesetzgeber hat bei der reinen Bereitstellung von Speicherplatz berücksichtigt, dass im Kern eine technische Leistung erbracht wird und die Verantwortung für die darauf gespeicherten Inhalte im Grundsatz demjenigen zugewiesen, der den Speicherplatz für das Angebot eigener Inhalte nutzt. Die Haftung des Host-Providers ist seit dem 1.3.2007 im Telemediengesetz (TMG) geregelt.

a) Grundsatz: Nichtverantwortlichkeit für fremde Inhalte auf eigenen Servern

Der Grundsatz der Nichtverantwortlichkeit für fremde Inhalte auf eigenen Servern ist in § 10 TMG geregelt. Danach sind Diensteanbieter nicht für fremde Informationen verantwortlich, die sie für einen Nutzer speichern, also z. B. für die Inhalte privater Homepages von Studierenden oder für Beiträge in Newsgroups, sofern das Rechenzentrum einen eigenen Newsserver betreibt, auf dem diese Inhalte gespeichert werden. Für die Inhalte ist vielmehr der Autor des jeweiligen Beitrags verantwortlich. Aus diesem Grund ist es wichtig, im Rahmen der Haftung zwischen eigenen und fremden Inhalten zu unterscheiden, auch wenn diese Abgrenzung im Einzelfall Schwierigkeiten bereiten kann. Dies ist etwa der Fall, wenn private Seiten von Studierenden im Corporate-Design der Hochschule ohne ein Impressum angeboten werden, aus dem die Anbietereigenschaft des Studierenden hervorgeht. Beim Angebot eines Meinungsforums wird dagegen in der Regel für jeden Außenstehenden erkennbar sein, dass die dort veröffentlichten Beiträge Meinungsäußerungen Dritter wiedergeben. Allerdings hat das Landgericht Hamburg selbst in einem solchen Fall entschieden, dass Informationen, die eine dritte Person auf dem Internetauftritt des Seitenbetreibers einstellt, wie eigene Informationen des Diensteanbieters zu behandeln sind (LG Hamburg, Urteil vom 27.4.2007 – Az. 324 O 600/06). Diese Entscheidung sorgte für großes Aufsehen, da sie de facto den Forenbetreibern die Haftungsprivilegierung des Host-Providers aberkennt. Die herrschende Ansicht in der Rechtsprechung lehnt diese Ansicht daher ab und wendet die Haftungsprivilegien auch auf diese an.

b) Ausnahmen in § 10 TMG

Der Grundsatz der Nichtverantwortlichkeit unterliegt jedoch wichtigen Einschränkungen. In Bezug auf Nutzer, die dem Anbieter unterstehen oder von ihm beaufsichtigt werden, gilt er nicht, § 10 S. 2 TMG. Dies ist z.B. der Fall, wenn zwischen Nutzer und Diensteanbieter ein Arbeitsverhältnis besteht. Ein weiterer Anwendungsfall ist insbesondere für den Schulbereich anzunehmen, wenn etwa eine Schule ihren Schülern zu Lernzwecken Speicherplatz zur Verfügung stellt. Bei Studierenden kann im Gegensatz zu Schülern grundsätzlich nicht angenommen werden, dass sie der Aufsicht der Hochschule unterstehen, weshalb der Grundsatz der Nichtverantwortlichkeit weiterhin anwendbar bleibt. Daneben bestehen noch weitere Einschränkungen. Diese sind darin begründet, dass der Anbieter durch seine Tätigkeit die Verbreitung der fremden Inhalte ermöglicht und diese damit auch technisch verhindern kann. § 10 S. 1 TMG bestimmt daher, dass der Anbieter nur dann nicht verantwortlich ist, wenn er

- keine Kenntnis von der rechtswidrigen Handlung oder Information hat. Im Falle von Schadensersatzansprüchen genügt jedoch bereits, dass er Tatsachen oder Umstände kennt, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird. Hierbei ist hervorzuheben, dass der Anbieter aufgrund von § 7 Abs. 2 TMG keinerlei Pflichten hat, gespeicherte fremde Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. In der Regel wird der Anbieter daher die Kenntnis durch Hinweise Dritter erlangen. Wichtig hierbei ist, dass ein außenstehender Hinweisgeber nicht die interne Organisation zu beachten braucht. Es genügt, wenn er z. B. ein Schreiben an "das Rechenzentrum" richtet. Durch eine geeignete Organisation ist sicherzustellen, dass eingehende Hinweise auf rechtswidrige Inhalte jederzeit an einen bestimmten Mitarbeiter weitergeleitet werden, der in der Lage ist, Dateien gegebenenfalls umgehend zu sperren.

- Kenntnis erlangt hat, aber unverzüglich und damit ohne schuldhaftes Zögern tätig geworden ist, um diese Informationen zu entfernen oder den Zugang zu ihnen zu sperren.

Vereinfacht gesagt ist der Anbieter dann nicht verantwortlich, wenn er keine Kenntnis hat oder die entsprechenden Inhalte nach Erlangung der Kenntnis ohne schuldhaftes Zögern entfernt oder sperrt. Für eine Organisation, die entsprechende Maßnahmen ermöglicht, ist deshalb Sorge zu tragen. Anderenfalls besteht die Gefahr, dass die Einrichtung für die fremden Inhalte wie für einrichtungseigene Inhalte haftet, obwohl sie auf die inhaltliche Gestaltung keinen Einfluss hatte. Hier baut sich somit ein enormes Haftungsrisiko auf, das mit relativ einfachen internen organisatorischen Maßnahmen vermieden werden kann.

c) Ausnahme: Haftung auf Unterlassen trotz Nichtverantwortlichkeit

Trotz der grundsätzlichen Nichtverantwortlichkeit in Bezug auf fremde Inhalte kann für den Diensteanbieter eine Pflicht zur Beseitigung und Unterlassung bestehen, da er durch die Überlassung von Speicherplatz einen mitursächlichen Beitrag zur Rechtsverletzung geleistet hat. Dies klingt zwar aufgrund der bisherigen Schilderung zum Grundsatz der Nichtverantwortlichkeit befremdlich, lässt sich jedoch damit begründen, dass oftmals eine andauernde Rechtsverletzung nicht durch ein Vorgehen gegen den eigentlichen Verursacher beendet werden kann, sondern nur mittels Vorgehen gegen denjenigen, der zur technischen Unterbindung in der Lage ist. Auch wenn diese Begründung

zunächst plausibel klingt, sind aufgrund der abgestuften Regelungen zur Verantwortlichkeit im TMG durchaus Zweifel angebracht, ob für eine darüber hinausgehende Inanspruchnahme auf Unterlassung ein Bedürfnis besteht. Nach den vorgenannten Grundsätzen muss ein Anbieter ohnehin nach Kenntniserlangung sofort etwas unternehmen, um eine eigene Haftung zu verhindern. Trotzdem sind die Gerichte in letzter Zeit mehr und mehr dazu übergegangen, Unterlassungs- und Beseitigungsansprüche auch bei einer an sich gegebenen Nichtverantwortlichkeit anzunehmen (grundlegend: BGH, Urteil vom 11.3.2004 – Az. I ZR 304/01, MMR 2004, 668).

Als Grundlage für eine Haftung auf Unterlassen oder Beseitigung wird die Regelung in § 7 Abs. 2 S. 2 TMG herangezogen, nach der Diensteanbieter auch im Falle der Nichtverantwortlichkeit zur Entfernung oder Sperrung der Nutzung von Informationen „nach den allgemeinen Gesetzen“ verpflichtet bleiben. Als solches allgemeines Gesetz kommt die sogenannte allgemeine Störerhaftung (§§ 823, 1004 Bürgerliches Gesetzbuch (BGB)) in Betracht. Nach Ansicht des Bundesgerichtshofs ist auch bei gegebener Nichtverantwortlichkeit eine verschuldensunabhängige Haftung als sogenannten Störer nicht ausgeschlossen (BGH, Urteil vom 11.3.2004 – Az. I ZR 304/01, MMR 2004, 668). Dies bedeutet, dass auch jemand, der nicht unmittelbar an einer Rechtsverletzung beteiligt ist, aber durch seine Tätigkeit einen für deren Erfolg mitursächlichen Beitrag leistet, zur Beseitigung dieses Beitrags verpflichtet sein kann. Beim Hosting besteht dieser Beitrag in der Regel in der Zurverfügungstellung von Speicherplatz für rechtsverletzende Inhalte. Die Pflicht zur Beseitigung wird in diesen Fällen regelmäßig durch die Sperrung oder Entfernung der fraglichen Inhalte zu erfüllen sein. Die Rechtsprechung berücksichtigt den Umstand, dass die Diensteanbieter die Rechtsverletzungen nicht selbst vornehmen und nimmt eine Haftung auf Unterlassen beziehungsweise Beseitigung nur in solchen Fällen an, in denen zumutbare Prüfungspflichten verletzt wurden (BGH, Urteil vom 11.3.2004 – Az. I ZR 304/01, MMR 2004, 668). Dabei ist wiederum zu berücksichtigen, dass nach § 7 Abs. 2 S. 1 TMG grundsätzlich keine Verpflichtungen zur Nachforschung oder Überwachung bestehen (siehe auch: OLG Düsseldorf, Urteil vom 26.4.2006 – Az. 15 U 180/05). Eine Prüfungs- oder Überwachungspflicht kann jedoch dann entstehen, wenn Umstände wie z. B. der Hinweis eines Dritten Anlass zu einer Prüfung geben oder Rechtsverletzungen auf dem jeweiligen Internetauftritt wahrscheinlich sind. Die Zumutbarkeit solcher Pflichten bestimmt sich nach den Umständen des Einzelfalls und ist in der Rechtsprechung sehr umstritten. Eine Rolle bei der Bestimmung der Intensität der Prüfungspflichten spielen unter anderem der zu betreibende Aufwand, der zu erwartende Erfolg und der Aspekt, ob der Betreiber mit oder ohne Gewinnerzielungsabsicht seine Dienste anbietet (siehe auch KG, Beschluss vom 10.7.2009 – Az. 9 W 119/08). Bei einem konkreten Hinweis dürfte die Zumutbarkeit jedoch in der Regel gegeben sein. Bei Hinweisen auf rechtsverletzende Inhalte sollte das Justitiariat umgehend zur weiteren Prüfung eingeschaltet und der fragliche Inhalt bis zur Klärung vorübergehend gesperrt werden (siehe oben ; § 10 TMG). Ob die Kenntnisnahme einer klaren Rechtsverletzung dazu führt, dass der Rechtsverletzer nicht nur das konkrete Angebot unverzüglich sperren, sondern auch Vorsorge treffen muss, dass es möglichst nicht zu weiteren derartigen Verletzungen kommt, ist in der Rechtsprechung umstritten. Bejaht wurde eine proaktive Prüfungspflicht durch das Oberlandesgericht Hamburg (OLG Hamburg, Urteil vom 4.2.2009 – Az. 5 U 167/07) sowie das Landgericht Köln im Fall einer Persönlichkeitsrechtsverletzung (LG Köln, Urteil vom 30.7.2008 – Az. 28 O 189/08).Das Landgericht Berlin (LG Berlin, Beschluss vom 10.9.2009 – Az. 27 S 7/09), das Oberlandesgericht Düsseldorf (OLG Düsseldorf, Urteil vom 7.6.2006 – Az. I-15 U 21/06) und das Amtsgericht München (AG München, Urteil vom 6.6.2008 – Az. 142 C 6791/08) haben eine entsprechende Pflicht hingegen abgelehnt. Zu beachten ist dabei, dass bei Betreibern eines Usenet-Dienstes oder bei Sharehostern, die die Inanspruchnahme ihres Dienstes

mit der Möglichkeit von Rechtsverletzungen aktiv und offensiv bewerben, deutlich gesteigerte Prüfungspflichten angenommen werden (vergleiche unter anderem BGH, Urteil vom 12.7.2012 – Az. I ZR 18/11, WM 2013, 388; BGH, Urteil vom 15.8.2013 – Az. I ZR 79/12, NJOZ 2014, 301 und OLG Hamburg, Urteil vom 14.1.2009 – Az. 5 U 113/07).

Wegen der rechtlichen Unsicherheiten ist es ratsam, zu überlegen, ob es Vorsorgemaßnahmen gegen weitere Verletzungen gibt, die zumutbar getroffen werden könnten. Bei Markenrechtsverletzungen kann ein Filter eingesetzt werden, welcher durch Eingabe von Suchbegriffen Verdachtsfälle aufspürt, die dann gegebenenfalls manuell zu überprüfen sind (BGH, Urteil vom 11.3.2004 – Az. I ZR 304/01). Ansonsten bleibt es aber dabei, dass die Prüfungspflichten nicht so weit gehen dürfen, dass das gesamte Geschäftsmodell in Frage gestellt wird. Unzumutbar wäre es, von dem Plattformbetreiber zu verlangen, jedes Angebot vor der Veröffentlichung zu überprüfen.

Hervorzuheben ist, dass der nach § 10 TMG nicht verantwortliche Provider höchstens auf Unterlassung beziehungsweise Beseitigung in Anspruch genommen werden kann und er bei Verletzung seiner Prüfungs- und Überwachungspflichten für die Abmahngebühren aufkommen muss. Weitere Schadensersatzansprüche bestehen im Fall der Nichtverantwortlichkeit aber nicht (BGH, Urteil vom 11.3.2004 – Az. I ZR 304/01, MMR 2004, 668).

d) Sonderfall: Meinungsforen

Im Grundsatz gelten die vorgenannten Erwägungen entsprechend für den im Rahmen von Meinungsforen zur Verfügung gestellten Speicherplatz. Im Zusammenhang mit Meinungsforen ist jedoch im Einzelnen noch unklar, unter welchen Voraussetzungen Prüfungspflichten und Verantwortlichkeiten des Betreibers entstehen können. Das Landgericht Hamburg ging in einer Entscheidung vom 2. Dezember 2005 (LG Hamburg, Urteil vom 2.12.2005 – Az. 324 O 721/05, MMR 2006, 491) von einer verschärften Haftung für die Verbreitung von Beiträgen in Foren aus. In dem zu entscheidenden Fall hatten Teilnehmer eines Forums in Reaktion auf eine kritische Berichterstattung dazu aufgerufen, den Server des kritisierten Unternehmens durch massenhafte Downloads lahmzulegen. Das Landgericht Hamburg verurteilte den Betreiber des Forums als Störer auf Unterlassung und nahm in seiner Begründung sogar an, dass die bloße Verbreitung des Beitrages für eine Haftung auf Unterlassen als Störer ausreichen soll, weil damit eine besondere Gefahrenquelle eröffnet werde. Die Kammer hielt es in der Entscheidung deshalb sogar für zumutbar, Foren in der Weise einzurichten, dass jeder Beitrag vorab auf die rechtliche Zulässigkeit seines Inhalts geprüft wird. Inwieweit dies mit der Regelung aus § 7 Abs. 2 S. 1 TMG über das Nichtbestehen einer Nachforschungspflicht in Einklang zu bringen ist, ließ das Gericht offen. Diese weitgehende Vorprüfpflicht wurde vom Oberlandesgericht Hamburg in der Berufung entschieden abgelehnt. Eine generelle Verpflichtung zu einer vorherigen „Eingangskontrolle“ sei im Hinblick auf die grundgesetzlich garantierte Freiheit der Meinungsäußerung nicht möglich (OLG Hamburg, Urteil vom 22.8.2006 – Az. 7 U 50/06). Ebenso nahmen der Bundesgerichtshof (BGH, Urteil vom 25.10.2011 – Az. VI ZR 93/10, GRUR 2012, 311) und das Oberlandesgericht Düsseldorf (OLG Düsseldorf, Urteil vom 26.4.2006 – Az. 15 U 180/05) in ihren Entscheidungen zu der Thematik eine weitaus sachgerechtere Haltung zur Behandlung von Foren ein, indem Betreiber von Foren vergleichbar einem Host-Provider behandelt werden. Das Landgericht Hamburg bestätigte seine Auffassung bezüglich eines strengen Haftungsmaßstabs für Forenbetreiber noch einmal und befürwortet eine proaktive Prüfpflicht (LG Hamburg, Urteil vom 27.4.2007 – Az. 324 O 600/06): Ein Beitrag sei dem Betreiber erst dann nicht mehr zurechenbar, wenn sich aus den Umständen mit hinreichender Deutlichkeit ergibt, dass der

Inhaber der Domain dessen Verbreitung gerade nicht wünscht, obwohl er ihn in den Internetauftritt aufgenommen hat. Dies setze voraus, dass der Betreiber der Internetseite sich von der streitigen Äußerung nicht pauschal, sondern konkret und ausdrücklich distanziert. Dieses Urteil läuft de facto auf eine Pflicht des Forenbetreibers zur Vorabkontrolle hinaus, was sich mit der bisherigen Rechtsprechung des Bundesgerichtshofs wohl kaum vereinbaren lässt und dementsprechend nicht von anderen Gerichten bestätigt wurde. Dennoch ist die Rechtslage noch nicht vollständig geklärt, auch weil noch keine höchstrichterliche Entscheidung ergangen ist.

Reichweite und Umfang einer allgemeinen Kontrolle sind also nach wie vor unsicher. Erlangt der Forenbetreiber von rechtsverletzenden Beiträgen Kenntnis, sollte er zunächst den entsprechenden Eintrag überprüfen. Liegt nach seiner Auffassung eine Rechtsverletzung vor, muss der Beitrag unverzüglich gelöscht werden. Eine laufende Kontrolle der Foreneinträge ist nicht zwingend erforderlich. Ist es in einem Thread hingegen bereits zu Rechtsverletzungen gekommen, sollte er kontrolliert werden. Gleiches gilt bei Threads mit einem besonders heiklen Inhalt. Ist der Betreiber für einen bestimmten Zeitraum nicht in der Lage, das Forum zu kontrollieren, sollte er den Betrieb für diese Zeit einstellen (siehe hierzu *Rinken*, „Diffamierung statt Diskussion“, DFN-Infobrief Recht vom November 2008).

e) Wer haftet?

(1) Zivilrechtliche Haftung

Die in Betracht kommenden zivilrechtlichen Ansprüche sind überwiegend auf Beseitigung (das heißt meistens Sperrung und/oder Löschung der rechtsverletzenden Inhalte) und Unterlassung (Vermeidung vergleichbarer Rechtsverletzungen in der Zukunft) gerichtet. Typische Fälle, die solche Ansprüche auslösen, sind z. B. die Verletzung von Urheber- oder Markenrechten sowie ehrverletzende Äußerungen. Soweit das Rechenzentrum für derartige Rechtsverletzungen (mit-) verantwortlich ist, haftet grundsätzlich die Einrichtung/Hochschule beziehungsweise deren Rechtsträger als juristische Person. Als solche haftet die Hochschule im Übrigen in der Regel auch für Fachbereiche und Institute. Die Mitarbeiter haften grundsätzlich nicht persönlich, wenn sie in Ausübung ihrer Diensttätigkeit gehandelt haben, was bei Beamten aus den Grundsätzen der Amtshaftung gemäß Art. 34 GG und § 839 BGB folgt. Angestellte haben dagegen einen Haftungsfreistellungsanspruch gegen ihren Arbeitgeber. Davon unberührt bleiben eventuelle Haftungsrückgriffe der Hochschule gegen den verantwortlichen Mitarbeiter aus dem Dienstverhältnis. Solche Rückgriffe kommen in Betracht, wenn Dienstpflichten vorsätzlich oder in grobem Maße verletzt wurden und der Hochschule dadurch ein Schaden entstanden ist.

Soweit Aufgaben von Einrichtungen wahrgenommen werden, die keine organisatorischen Untergliederungen der Hochschulen sind, sondern selbständige juristische Personen des öffentlichen Rechts (wie z.B. Studierendenwerke), sind auch hier diese selbst und nicht etwa die Hochschule als Diensteanbieter i.S.d. § 2 Satz 1 Nr. 1 TMG anzusehen und können als solche haftbar gemacht werden.

(2) Strafrechtliche Verantwortlichkeit

Strafrechtlich können nur natürliche Personen verantwortlich sein, nicht die Hochschule als solche. Möglich ist beispielsweise eine Strafbarkeit wegen rechtswidriger Inhalte, die von anderen Personen erstellt wurden, aber auf den Servern des Rechenzentrums zum Abruf bereitgehalten werden, sofern

die Dateien nach Erlangung der Kenntnis von diesen Inhalten nicht unverzüglich gesperrt werden. Welche Personen davon betroffen sind (z. B. Rektor, Leiter des Rechenzentrums oder Dekan einer Fakultät), ist eine Frage des Einzelfalls. Als verantwortliche Personen kommen jedenfalls auch die Leiter der Rechenzentren in Betracht, weil und soweit sie eine Sperrung und Löschung von Dateien mit rechtswidrigen Inhalten veranlassen und umsetzen können. Eine Verantwortung für solche fremden Inhalte kommt aber erst dann in Betracht, wenn die verantwortlichen Personen des Rechenzentrums von ihnen Kenntnis erhalten. Auch hier gilt, dass grundsätzlich keine Pflicht zur Durchsuchung aller Dateien auf rechtswidrige Inhalte besteht.

Weitere Informationen hierzu finden sich in der Wissensbasis.

3. Verdacht auf Straftaten

a) Verdacht

Besteht der Verdacht, dass ein Benutzer über die Einrichtungen des Rechenzentrums – etwa durch die Verbreitung rechtswidriger Inhalte – Straftaten begangen hat, so sollten keine Ermittlungen auf eigene Faust angestellt werden. Es sollten nur Beweise gesichert (Ausdruck und Speicherung der Dateien, Informierung anderer Mitarbeiter als Zeugen etc.), aber keine neuen Beweise eigenmächtig ermittelt werden. Stattdessen ist frühzeitig die Polizei oder Staatsanwaltschaft zu informieren, um gegebenenfalls Anzeige zu erstatten. Der weitere Verlauf des Ermittlungsverfahrens wird dann von der Staatsanwaltschaft bestimmt.

b) Einbindung in Ermittlungsverfahren und Prävention

Ferner können die Mitarbeiter der Rechenzentren in behördliche Maßnahmen dergestalt eingebunden werden, dass sie z. B. visuelle Wahrnehmungen beziehungsweise Beobachtungen des Nutzerverhaltens an die Staatsanwaltschaft oder Polizei zukünftig weitergeben. Diese Art der Kooperation im Sinne eines "Augen-und-Ohren-offenhalten" ist unbedenklich. Bei einer weitergehenden Zusammenarbeit sollte eine Anordnung von der Staatsanwaltschaft beziehungsweise dem Behördenleiter eingeholt werden. Auf jeden Fall sollte bei einem Verdacht begangener oder bevorstehender Straftaten zunächst die zuständige Stelle informiert und die weitere Vorgehensweise abgestimmt werden.

4. Maßnahmen bei Beschwerden/Hinweisen auf rechtswidrige Inhalte

Es ist unerlässlich, durch interne Organisationsmaßnahmen sicherzustellen, dass eingehende Hinweise und Beschwerden bzgl. rechtswidriger Inhalte umgehend bearbeitet werden. Erfolgt keine rechtzeitige Sperrung tatsächlich rechtswidriger Inhalte, geht das Haftungsprivileg für fremde Inhalte nach § 10 TMG (siehe oben) verloren. Die Einrichtung haftet dann für diese Inhalte, als seien es ihre eigenen. In diesem Fall droht somit nicht nur eine Haftung auf Beseitigung und Unterlassen in Gestalt einer Pflicht zur Sperrung oder Entfernung der Inhalte, sondern unter Umständen auch eine Haftung auf Schadensersatz oder gar eine strafrechtliche Verantwortlichkeit der in der Einrichtung verantwortlichen Personen.

a) Organisatorische Maßnahmen

Ergeben sich durch Zufall oder aufgrund von Hinweisen Anhaltspunkte für rechtswidrige Inhalte auf dem zur Verfügung gestellten Speicherplatz, muss sichergestellt werden, dass die Einrichtung hierauf

ohne nennenswerte Verzögerungen mittels Sperrung oder Entfernung der Inhalte reagieren kann. Dies setzt zunächst voraus, dass Informationen über solche Inhalte umgehend an eine zuständige Person weitergeleitet werden, die entsprechende Maßnahmen veranlassen darf. Aufgrund der rechtlichen Relevanz sollte zudem immer das Justitiariat in den Vorgang einbezogen werden. Bestehen auch nur geringste Zweifel an der Rechtmäßigkeit der fraglichen Inhalte, sollte die betroffene Datei umgehend vorläufig gesperrt werden. Zur rechtlichen Absicherung einer vorübergehenden Sperrung empfiehlt es sich, eine Regelung in die Benutzungsordnung aufzunehmen, dass bei tatsächlichen Anhaltspunkten für ein Bereithalten rechtswidriger Inhalte auf den Servern des Rechenzentrums die Möglichkeit besteht, die Inhalte bis zur hinreichenden Klärung der Rechtslage zu sperren (siehe § 7 Abs. 3 Musterbenutzungsordnung). Auch wenn eine solche explizite Regelung nicht besteht, sollte aufgrund der eingangs skizzierten möglichen massiven Folgen eine vorübergehende Sperrung erfolgen.

b) Konsequenzen nach erfolgter Überprüfung

Ergibt eine Überprüfung, dass der beanstandete Inhalt nicht rechtswidrig ist, kann die Datei wieder freigegeben werden. Ansonsten sollte sie natürlich endgültig vom Server entfernt werden. Die weiteren Konsequenzen bestimmen sich nach der Lage des Einzelfalls. Soweit es sich um vorsätzliche Rechtsverstöße handelt, kommen gegenüber Nutzern beispielsweise Sanktionen aufgrund der Benutzungsordnung in Betracht. Bei strafbaren Inhalten wie z. B. Kinderpornografie kann auch eine Strafanzeige gegen den Autor der Seite erstattet werden.

c) Abmahnungen durch Rechtsanwälte

Auch im Zusammenhang mit der Speicherung fremder rechtswidriger Inhalte kommt es vor, dass Einrichtungen eine anwaltliche Abmahnung erhalten. Dabei werden oftmals – genau wie bei einer abgemahnten Rechtsverletzung durch einrichtungseigene Inhalte – die Abgabe einer strafbewehrten Unterlassungserklärung, eventuell Schadensersatz und die Erstattung von Anwaltskosten geltend gemacht. Insbesondere bei Abmahnungen im Zusammenhang mit fremden rechtswidrigen Inhalten ist dringend zu raten, auf keinen Fall voreilig die gestellten Forderungen zu erfüllen. Handelt es sich um fremde Inhalte, für die lediglich der Speicherplatz zur Verfügung gestellt wird, haftet die Einrichtung nur unter den oben dargestellten engen Voraussetzungen. Erhält die Einrichtung somit durch die Abmahnung erstmalig Kenntnis von möglicherweise rechtsverletzenden Inhalten und sperrt diese umgehend, besteht in der Regel kein Anspruch auf Unterlassung. Bei der Verletzung von Prüfungs- oder Überwachungspflichten müssen jedoch gegebenenfalls die Kosten für die Abmahnung übernommen werden.

V. (Gewerbliche) Schutzrechte

1. Einführung

Das folgende Kapitel widmet sich wichtigen Einzelfragen zu Schutzrechten im Rahmen der Tätigkeit von Rechenzentren in Einrichtungen von Wissenschaft und Forschung. Zu den für die Einrichtungen besonders relevanten Bereichen der Schutzrechte zählen das Patentrecht, das Markenrecht, das Namensrecht und das Urheberrecht. Eine übergreifende Darstellung dieses Bereichs könnte ganze Lehrbücher füllen, weshalb sich die vorliegende Darstellung auf Grundlagen und wesentliche

Einzelaspekte beschränken muss. Wichtige auf die jeweilige Tätigkeit bezogene Aspekte werden zudem an den jeweils relevanten Stellen in den anderen Kapiteln behandelt.

2. Wichtige Schutzrechte

a) Patentrecht

Das im Patentgesetz (PatG) geregelte Patentrecht verfolgt den Schutz innovativer Erfindungen technischer Natur. Schutz kann demnach jede technische Leistung genießen, die neu ist (§ 3 PatG), gewerblich anwendbar ist (§ 5 PatG), auf erfinderischer Tätigkeit beruht (§ 4 PatG) und bei der die Gewährung eines Patents nicht von vornherein ausgeschlossen ist (§ 1 Abs. 2, 3 PatG). Formelle Voraussetzung für die Gewährung eines Patents ist die Anmeldung der Erfindung beim Deutschen oder Europäischen Patentamt. Wird das Patent erteilt und gehen binnen drei Monaten keine Einsprüche gegen das Patent ein, kann der Inhaber des Patents für eine Dauer von zwanzig Jahren ab Anmeldung seine Rechte aus dem Patent geltend machen. Nach Ablauf der 20 Jahre ist die Erfindung zur Benutzung frei. Das Patent bewirkt, dass allein der Patentinhaber befugt ist, die patentierte Erfindung zu nutzen. Ohne Zustimmung des Inhabers dürfen somit Dritte ein Erzeugnis, das Gegenstand eines Patents ist, nicht herstellen, anbieten, in Verkehr bringen, gebrauchen oder zu diesen Zwecken besitzen (§ 9 Abs. 1 S. 2 PatG). Das Gleiche gilt für patentierte Verfahren und daraus resultierende Produkte. Zudem dürfen nach § 10 Abs. 1 PatG Mittel, die sich auf ein wesentliches Element der Erfindung beziehen, nicht in Verkehr gebracht werden. Erlaubt bleiben nach § 11 Nr. 1 und Nr. 2 PatG Handlungen im privaten Bereich zu nichtgewerblichen Zwecken und Handlungen zu Versuchszwecken.

b) Urheberrecht

Das im Urheberrechtsgesetz (UrhG) geregelte Urheberrecht schützt künstlerische oder wissenschaftlich-technische Leistungen, die eine gewisse Originalität und Kreativität repräsentieren. Unter den Schutz können bei ausreichender Originalität, an die nicht allzu hohe Anforderungen gestellt werden, auch Webseiten oder Teile von diesen fallen. Anders als beispielsweise im Patentrecht besteht der Schutz durch das Urheberrecht unabhängig von einer Anmeldung, der Anbringung eines Copyright-Vermerks oder anderer Formalitäten. Der Schutz beginnt mit der Schöpfung des Werkes und endet 70 Jahre nach dem Tod des Urhebers. Die bloße Idee, ohne eine irgendwie erfolgte Manifestation, unterliegt keinem urheberrechtlichen Schutz. Der Schutz erstreckt sich einerseits auf die wirtschaftliche Verwertung der Schöpfung durch den Urheber, andererseits auf seine persönliche Beziehung zu seinem Werk. Somit kann der Urheber wirtschaftliche Verwertungshandlungen wie z. B. die ungenehmigte Vervielfältigung oder öffentliche Aufführung verbieten. Ebenso kann der Urheber Bearbeitungen an seinem Werk verbieten oder auf die Nennung seines Namens bestehen. In Bezug auf das Verbotsrecht im Zusammenhang mit der wirtschaftlichen Verwertung bestehen jedoch zu Gunsten von Allgemeinwohlbelangen – insbesondere für Wissenschaft und Bildung – gewichtige Ausnahmen (sogenannte Schranken des Urheberrechts). In deren engen Grenzen dürfen Werke auch ohne Zustimmung des Urhebers zu den dort bestimmten Zwecken verwendet werden. Werden Rechte des Urhebers verletzt, kann dieser Unterlassungs- oder Schadensersatzansprüche gegen den Verletzer geltend machen.

c) Markenrecht

Das im Markengesetz (MarkenG) geregelte Markenrecht schützt Marken, geschäftliche Bezeichnungen und geografische Herkunftsangaben. Als Marke können nach § 3 MarkenG alle Zeichen, insbesondere Wörter, Abbildungen, Buchstaben, Zahlen, Hörzeichen geschützt werden, die geeignet sind, Waren oder Dienstleistungen eines Unternehmens von denjenigen eines anderen Unternehmens zu unterscheiden. Als geschäftliche Bezeichnungen werden nach § 5 MarkenG Unternehmenskennzeichen und Werktitel geschützt. Unternehmenskennzeichen sind hierbei Zeichen, die im geschäftlichen Verkehr als Name, als Firma oder als besondere Bezeichnung eines Geschäftsbetriebs oder eines Unternehmens benutzt werden. Werktitel sind die Namen oder besonderen Bezeichnungen von Druckschriften, Filmwerken, Tonwerken, Bühnenwerken oder sonstigen vergleichbaren Werken. Nach § 4 MarkenG entsteht der Markenschutz einerseits durch die Eintragung eines Zeichens als Marke in das vom Patentamt geführte Markenregister. Andererseits kann ein Markenrecht auch durch die Benutzung eines Zeichens im geschäftlichen Verkehr, soweit das Zeichen innerhalb beteiligter Verkehrskreise als Marke Verkehrsgeltung erworben hat, oder durch notorische Bekanntheit der Marke im Sinne der Pariser Übereinkunft zum Schutz des gewerblichen Eigentums entstehen. Der Erwerb des Markenrechtsschutzes und des Schutzes geschäftlicher Bezeichnungen gewährt dem Inhaber ein ausschließliches Recht (§§ 14, 15 MarkenG). Die Verletzung des Ausschließlichkeitsrechts führt zu Ansprüchen gegen den Verletzer auf Unterlassung, Schadensersatz, Auskunft und Vernichtung.

d) Namensrecht

§ 12 Bürgerliches Gesetzbuch (BGB) garantiert den namensrechtlichen Schutz. Wird das Recht zum Gebrauch eines Namens dem Berechtigten von einem anderen bestritten oder wird das Interesse des Berechtigten dadurch verletzt, dass ein anderer unbefugt den gleichen Namen gebraucht, so kann der Berechtigte von dem anderen Beseitigung der Beeinträchtigung verlangen. Bei zu erwartenden weiteren Beeinträchtigungen kann der Berechtigte auf Unterlassung klagen. Als Quelle des namensrechtlichen Kennzeichnungsschutzes ist § 12 BGB die allgemeinere Regelung im Verhältnis zum Markengesetz, so dass bei einem fehlenden Schutz durch das Markenrecht zumindest ein Schutz über das Namensrecht in Betracht gezogen werden kann, was insbesondere in Bezug auf Hochschulen und Forschungseinrichtungen Bedeutung erlangt. Geschützt sind sowohl Namen natürlicher Personen, Berufs- und Künstlernamen als auch die Namen juristischer Personen. Für Hochschulen und Forschungseinrichtungen besonders relevant ist, dass auch öffentlich-rechtliche Körperschaften gegen eine unbefugte Nutzung ihres Namens durch § 12 BGB geschützt sind (BGH, GRUR 1964, S. 38 ff.). Eine Namensfunktion kann überdies auch Domain-Namen zukommen (vergleiche BGH GRUR 2002, S. 622, 624). § 12 BGB schützt diesbezüglich vor allem vor der Namensanmaßung. Eine Namensanmaßung ist insbesondere bei der sogenannten Zuordnungsverwirrung gegeben, wenn der unrichtige Eindruck erweckt wird, dass der Namensträger dem Gebrauch seines Namens zugestimmt hat (BGH, NJW 1983, S. 1186). Die Beurteilung, ob eine Verletzung des Namensrechts vorliegt, hängt allerdings häufig von den Umständen des konkreten Einzelfalls ab. Der in seinem Namensrecht Verletzte kann ebenfalls Unterlassung, Beseitigung und gegebenenfalls Schadensersatz verlangen.

3. Praxisrelevante Einzelaspekte

a) Patent-/Urheberrechtsschutz von Software

Immer wieder kommt es zu spektakulären Abmahnaktionen oder Rechtsstreitigkeiten wegen angeblicher Verletzungen von Patentrechten an Software. Dann stellt sich die Rechtslage oft sehr

komplex dar. Dies liegt einerseits an den internationalen Sachverhalten mit unterschiedlicher Patentierungspraxis bei Software, andererseits an dem Problem der Bestimmung der Reichweite der Schutzwirkung eines Patents im konkreten Fall. Im Hinblick auf den Schutz von Software gilt es jedoch zu beachten, dass Software auch bei fehlender Patentierbarkeit regelmäßig durch das Urheberrecht geschützt ist. Der Begriff der „Freien Software“ ist daher missverständlich, da ihre Freiheit nicht von einem fehlenden rechtlichen Schutz herrührt, sondern von dem durch die Lizenzierung gestatteten Gebrauch.

(1) Patentfähigkeit von Software

In Deutschland sind Programme für Datenverarbeitungsanlagen nach § 1 Abs. 3 Nr. 3 Patentgesetz (PatG) nicht als schutzfähige Erfindungen anzusehen. Entsprechendes ergibt sich auf europäischer Ebene aus Art. 52 Abs. 1 lit. c Europäisches Patent Übereinkommen (EPÜ), auf dem § 1 Abs. 3 Nr. 3 PatG beruht. Der Ausschluss der Patentfähigkeit gilt jedoch nur insoweit, als für Software „als solche“ Schutz begehrt wird (Vergleiche § 1 Abs. 4 PatG). Aufgrund dieser Einschränkung wird davon ausgegangen, dass Computerprogramme für sich allein betrachtet nicht patentfähig sein können, dass aber ein Patentschutz möglich ist, wenn sie Grundlage oder Ziel einer Lehre zum technischen Handeln sind (Loewenheim in: Schricker, Urheberrechtsgesetz, Vor. §§ 69a ff. Rn. 8 mit Verweis auf: Benkard, Patentgesetz, § 1 Rn. 107 m. w. N.).

In den Mitgliedstaaten der EU hat sich aufgrund der unbestimmten Ausnahme mit dem Wortlaut „als solche“ eine unterschiedliche Praxis im Hinblick auf die Patentfähigkeit von Computerprogrammen herausgebildet. Durch eine „Softwarepatentrichtlinie“ sollte die Praxis der Patentierung in den Mitgliedstaaten vereinheitlicht werden. Das Vorhaben ist jedoch gescheitert.

(2) Urheberrechtsschutz von Software

Computerprogramme genießen aber grundsätzlich urheberrechtlichen Schutz. Für sie gelten die besonderen Bestimmungen in §§ 69a ff. UrhG. Urheber des Computerprogramms ist immer der Programmierer. Wird das Programm von einem Arbeitnehmer in Wahrnehmung seiner Aufgaben oder nach den Anweisungen seines Arbeitgebers geschaffen, so ist nach § 69b Abs. 1 UrhG trotz der Urhebereigenschaft des Arbeitnehmers ausschließlich der Arbeitgeber zur Ausübung aller vermögensrechtlichen Befugnisse an dem Computerprogramm berechtigt, sofern nichts anderes vereinbart ist. Der Schutz des Urheberrechts umfasst sowohl Betriebs- als auch Anwendungsprogramme und erfasst neben dem Quellcode auch den Maschinenprogrammcode (Hoeren in: Möhring/Nicolini, Urheberrechtsgesetz, § 69a Rn. 5). Zudem kommt es nicht darauf an, ob die Programmierung in komplexen Sprachen wie Java oder in einer einfachen HTML-Programmierung erfolgt (Loewenheim in: Schricker, Urheberrechtsgesetz, § 69a Rn. 3). Für den Schutz ebenfalls belanglos ist, ob es sich um Standard- oder Individualsoftware handelt (Loewenheim a.a.O.). Der Urheberrechtsschutz umfasst nach § 69a Abs. 1 UrhG zudem das Entwurfsmaterial, insbesondere auch das Flussdiagramm (Loewenheim a.a.O. Rn. 5). Die Benutzeroberfläche, Handbücher, Bedienungsanleitungen oder Wartungsbücher gehören nicht zu dem Computerprogramm, können jedoch einen eigenständigen urheberrechtlichen Schutz genießen.

Für den Umfang der erlaubten Nutzung geschützter Programme sind grundsätzlich die Lizenzbedingungen maßgeblich. Unabhängig von den Lizenzbedingungen ist der berechtigte Nutzer jedoch insbesondere zur Erstellung einer Sicherungskopie nach § 69d Abs. 2 UrhG und zur Dekompilierung nach Maßgabe des § 69e UrhG berechtigt. Nach § 69g Abs. 2 UrhG sind diesen Rechten entgegenstehende vertragliche Vereinbarungen (Lizenzbedingungen) nichtig.

b) Domain-Namen

Rechtliche Konflikte um Domain-Namen können für DFN-Mitgliedsinstitutionen in zweifacher Hinsicht relevant werden: Einerseits kann jede Institution innerhalb ihrer eigenen Second-Level-Domain eigene Sub-Domains vergeben. Andererseits sind auch DFN-Mitglieder, insbesondere Hochschulen, nicht vor Domain-Grabbern sicher.

(1) Haftung für eigene Sub-Domains

Durch die Einrichtung eigener Sub-Domains unterhalb der Second-Level-Domain einer Institution können Rechte Dritter verletzt werden, wenn hierdurch in fremde Namens- oder Markenrechte eingegriffen wird. Dies kann sich einerseits auf die Verwendung der Domain als WWW-Adresse auswirken, wenn die entsprechende URL mit vorrangigen Namens- oder Markenrechten Dritter kollidiert (Beispiel: "www.bundeskanzler-amt.dfn.de"). Überdies kann sich eine objektive Verwechslungsgefahr bei der Verwendung der Sub-Domains innerhalb von E-Mail-Adressen ergeben (Beispiel: "bundeskanzler@bundeskanzler-amt.dfn.de"). In beiden Fallkonstellationen ist der Inhaber der jeweiligen Second-Level-Domain grundsätzlich für alle Namens- und Markenverstöße durch Sub-Domains innerhalb des eigenen Namensraums verantwortlich. Aus diesem Grund ist – insbesondere bei größeren Institutionen mit selbständigen Organisationseinheiten – auf hinreichend klare Kompetenzzuweisungen zwischen Rechenzentrum und den jeweiligen Untereinheiten (Fakultäten, Institute, Lehrstühle etc.) zu achten, um bei evtl. Rechtsverstößen durch selbst ausgewählte Sub-Domains umgehend reagieren zu können.

(2) Domain-Grabbing bei Hochschul-Domains

Auch Hochschulen können Opfer eines Domain-Grabbers werden, der Domains reserviert, die sich an die Hochschul-Domain anlehnen (z.B. uni-ms.de). Sein alleiniges Ziel ist hierbei zumeist, die so belegte Domain gewinnbringend zu veräußern. Bei Begriffen die sich an die Hochschul-Domain anlehnen, verletzt der Grabber regelmäßig das Namensrecht der Hochschule gemäß § 12 BGB. Diesbezüglich ist inzwischen allgemein anerkannt, dass auch der Domain-Name als namensartiges Kennzeichen in den Schutzbereich von § 12 BGB fällt (siehe oben). Lehnt sich der durch den Grabber registrierte Begriff an die für Hochschulen üblichen Namenskonventionen an, die zumeist aus der Bezeichnung der Hochschule fh- oder uni- in Verbindung mit der Ortsbezeichnung bestehen, liegt im Regelfall eine Namensanmaßung vor, die objektiv eine „Identitäts- oder Zuordnungsverwirrung“ erzeugt, wodurch schutzwürdige Interessen der Hochschule als Namensträgerin verletzt werden. Beispiele hierfür sind die Verwendung der Bezeichnungen uni-ms.de, unimuenster.de oder uni-muenster.eu in Anlehnung an die Bezeichnung uni-muenster.de für das Informationsangebot der Universität Münster. Bestehen wie zumeist keine prioritätsälteren Rechte des Grabbers an der Bezeichnung, besteht als Rechtsfolge aus § 12 BGB ein verschuldensunabhängiger Beseitigungs- und Unterlassungsanspruch, der auf die sofortige und endgültige Freigabe der Domain gerichtet ist. Die direkte Übertragung der Domain kann hingegen nicht verlangt werden. Allerdings kann die Reservierung für die Hochschule nach Freigabe der Domain durch einen sogenannte Dispute-Eintrag bei der zuständigen Registrierungsstelle abgesichert werden. Wird eine Namensrechtsverletzung zu Lasten der Hochschule festgestellt, kann somit die Freigabe der Domain durch eine Abmahnung des Domain-Inhabers erreicht werden, in der er zur sofortigen Freigabe der Domain und Abgabe einer strafbewehrten Unterlassungserklärung aufgefordert wird.

Münster, März 2017

Forschungsstelle Recht im DFN

Die Forschungsstelle Recht ist ein Projekt an der WESTFÄLISCHEN WILHELMS-UNIVERSITÄT, Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Zivilrechtliche Abteilung unter Leitung von Prof. Dr. Thomas Hoeren, Leonardo-Campus 9, D-48149 Münster, E-Mail: recht@dfn.de