RECHTSGUIDE
der Forschungsstelle Recht im DFN

Inhaltsverzeichnis

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 Nutzungsverhältnis

a. Einführung

Mit der Bereitstellung von Diensten der Informations- und Kommunikationstechnik (IuK-Dienste) entsteht ein sogenanntes Nutzungsverhältnis. Hieraus folgen für Hochschulen und Forschungseinrichtungen eine Vielzahl von (rechtlichen) Fragen, für die ein Regelungsbedürfnis besteht.

So sollten die Einrichtungen Regeln aufstellen, die eine möglichst störungsfreie, ungehinderte und sichere Nutzung der Kommunikations- und Datenverarbeitungsstruktur gewährleisten. Kommerzielle IuK-Anbieter regeln dies im Rahmen des Vertragsverhältnisses mit dem Kunden üblicherweise durch Allgemeine Geschäftsbedingungen (AGB). Im Arbeitsverhältnis können Regelungen durch Dienstvereinbarungen getroffen werden. Insbesondere bei Hochschulen gestaltet sich dies meist schwieriger, da sie die IuK-Dienste regelmäßig zur Erfüllung ihrer Aufgaben als Körperschaft des Öffentlichen Rechts erbringen und in diesem Rahmen nicht ohne weiteres Verträge schließen können. Das Nutzungsverhältnis ist meist öffentlich-rechtlich zu charakterisieren. In der Konsequenz sind die rechtlichen Fragen nicht vertraglich zu regeln, sondern durch eine Benutzungsordnung.

b. Benutzungsordnung zur Ausgestaltung des Nutzungsverhältnisses

Die Benutzungsordnung dienen der inhaltlichen Ausgestaltung des Verhältnisses zwischen der Einrichtung und der nutzenden Person, die die Dienste des Rechenzentrums in Anspruch nimmt. Hier sollte geregelt sein, welche grundlegenden Rechte und Pflichten dem Rechenzentrum und den zugelassenen Nutzenden zukommen und unter welchen Voraussetzungen Nutzer zugelassen oder von der Nutzung ausgeschlossen werden können. Sie sollte also die Ermächtigungsgrundlagen für hoheitliche Sanktionen enthalten. Weiter sollte geregelt sein, welche Zuständigkeiten innerhalb der Einrichtung hinsichtlich des Betriebs der IuK-Dienste bestehen. Benutzungsordnungen, Netzordnungen oder Nutzungsrichtlinien et cetera können entweder als Satzungen oder als Ordnungen im Sinne der Hochschulgesetze durch den Senat/Rektor der Hochschule erlassen werden. Alternativ kann der Leiter des Rechenzentrums sie als sogenannte Allgemeinverfügungen erlassen. Entsprechend kann sich dann um eine Rechtsnorm oder eine Verwaltungsnorm handeln.

Als Rechtsnorm

Als Satzung beziehungsweise förmliche Ordnungen erlassene Benutzungsordnungen sind verbindliche Rechtsvorschriften. Die Einrichtung hat als verwaltungsrechtliche Personalkörperschaft des öffentlichen Rechts für ihre Selbstverwaltungsaufgaben die Kompetenz, selbst Rechtsvorschriften zu erlassen. Grundlage dafür ist das jeweilige Landeshochschulgesetz, das regelmäßig eine Vielzahl an Ermächtigungen für die Hochschulen enthält. Die Rechtsvorschriften binden alle Angehörigen der Hochschule und sonstigen Anstaltsnutzenden, 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.

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). 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 aus Art. 5 Abs. 3 GG.

Handlungsempfehlung

Die Benutzungsordnung in Gestalt einer Satzung (= Rechtsnorm) ist somit vorzugswürdig, da aus verfassungsrechtlichen Gründen ohnehin wesentliche Elemente als Rechtsnorm geregelt werden müssen.

c. Wichtige Einzelaspekte zum Nutzungsverhältnis

Im Folgenden werden einige wichtige Einzelaspekte zum Nutzungsverhältnis übergreifend dargestellt.

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 Nutzungsverhältnissen erfolgt die Zulassungsentscheidung durch einen Verwaltungsakt. Die Voraussetzungen ergeben sich zumeist aus der jeweiligen Benutzungsordnung. So sind regelmäßig die Angehörigen (Studierende, Mitarbeitende) der Hochschulen zugangsberechtigt.

Sollte etwa wegen Verstoß die Zulassung entzogen worden sein, kann die Zulassung auch neu beantragt werden. Hierbei ist gegebenenfalls in der Interessenabwägung zu beachten, dass die Nichtzulassung im Einzelfall zu Grundrechtsbeeinträchtigungen führen kann (Art 5 Abs. 3, Art. 12 GG).

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. Für die Einrichtungen stellt sich die Frage, ob hier eine Regelung notwendig ist.

Die Erlaubnis einer geringfügigen Privatnutzung kann 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.

Für den gänzlichen Ausschluss der Privatnutzung spricht, dass mit der Privatnutzung Vorgaben des Fernmeldegeheimnisses, also der Vertraulichkeit von Kommunikationsdaten, und des Datenschutzes relevant werden. 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.

Nutzungsausschluss bei Pflichtverletzung

Eine wichtige Frage, die jede Benutzungsordnung regeln muss, ist der Ausschluss von der Nutzung wegen Verstoßes gegen die Benutzungsordnung. In öffentlich-rechtlichen Nutzungsverhältnissen, in denen die Nutzenden durch eine öffentlich-rechtliche Verwaltungsentscheidung zur Nutzung zugelassen werden, stellt auch der Ausschluss eine öffentlich-rechtliche Verwaltungsentscheidung dar. Dieser Entscheidung muss durch eine Ermächtigungsgrundlage in der Benutzungsordnung abgedeckt sein, 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 (z. B. die Begehung von Straftaten mittels der Dienste).

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. In der Abwägung 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 werden kann. Abgesehen davon ist außer in Fällen sehr schwerwiegender Verstöße aus Gründen der Verhältnismäßigkeit geboten, die nutzende Person auf ihre Pflichtverletzung hinzuweisen, sodass diese die Gelegenheit hat, sie abzustellen. 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

a. 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.

b. 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 rechtswidriger Inhalte in ein soziales Netzwerk. Der Netzzugang ist somit Ausgangspunkt für legale und illegale Kommunikation über das Internet durch die angeschlossenen Nutzer. Für die Rechenzentren stellt sich dabei die Frage, ob und inwieweit aufgrund des zur Verfügung gestellten Netzzugangs eine Mitverantwortlichkeit für durch Nutzer begangene und somit fremde Rechtsverletzungen bestehen kann.

Beschränkte Verantwortlichkeit

Für die Haftung des Diensteanbieters verweist § 7 Abs. 1 Digitale-Dienste-Gesetz (DDG) auf die Art. 4 bis 8 Digital Services Act (DSA)[1]. Der DSA unterscheidet in den Art. 4 bis 8 DSA zwischen „reiner Durchleitung“ (Art. 4 DSA), „Caching“ Art. 5 DSA und Hosting (Art. 6 DSA).

[1] Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), Abl. EU L 277 vom 27.10.2022, S. 1.

Die Begriffe definiert der DSA in Art. 3 lit. g Ziffer i bis iii DSA. Die „reine Durchleitung“ besteht nach Art. 3 lit. g Ziffer i DSA in der Übermittlung vom Nutzer bereitgestellten Informationen in einem Kommunikationsnetz oder in der Vermittlung des Zugangs zu einem Kommunikationsnetz. „Caching“ ist nach Art. 3 lit. g Ziffer ii DSA als Leistung, die darin besteht, von einem Nutzer bereitgestellte Informationen in einem Kommunikationsnetz zu übermitteln, wobei eine automatische, zeitlich begrenzte Zwischenspeicherung dieser Informationen zu dem alleinigen Zweck erfolgt, die Übermittlung der Information an andere Nutzer auf deren Anfrage effizienter zu gestalten. Schließlich ist „Hosting“ definiert als Speichern der von einem Nutzer bereitgestellten Informationen in dessen Auftrag, Art. 3 lit. g Ziffer iii DSA.

Nach Art. 4 Abs. 1 DSA haftet der Diensteanbieter für die reine Durchleitung von Informationen nicht. Diese liegt vor, wenn der Diensteanbieter die Übermittlung der Informationen nicht veranlasst (lit. a), die Adressaten der übermittelten Informationen nicht auswählt (lit. b) und die übermittelten Informationen nicht auswählt oder verändert (lit. c). Nach Art. 4 Abs. 2 DSA gilt dies auch für den Fall einer zeitlich begrenzten Zwischenspeicherung, die lediglich einer Übermittlung der Informationen dient, wobei die Informationen nicht länger gespeichert werden dürfen, als es für die Übermittlung üblicherweise erforderlich ist. § 7 Abs. 3 S. 1 DSA stellt Diensteanbieter auch von Schadensersatz-, Beseitigungs- und Unterlassungsansprüchen des Nutzers frei, sofern der Diensteanbieter nicht nach Art. 4 DSA haftet. Das gilt auch hinsichtlich aller Kosten für die Geltendmachung und Dursetzung dieser Ansprüche.

Art. 5 Abs. 1 DSA bestimmt für das Caching, dass der Diensteanbieter nicht für die Informationen haftet, wenn er die Voraussetzungen des Art. 5 Abs. 1 DSA erfüllt: Der Diensteanbieter darf die Informationen nicht verändern (lit. a), er muss die Bedingungen für den Zugang zu den Informationen beachten (lit. b), er hat die Regeln für die Aktualisierung der Informationen, die weithin in der Branche anerkannt und verwendet werden beachten (lit. c), darf die zulässige Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Informationen, die weithin in der Branche anerkannt und verwendet werden nicht beeinträchtigen und er muss zügig handeln, um von ihm gespeicherte Informationen zu entfernen oder den Zugang zu ihnen zu sperren, sobald er tatsächliche Kenntnis davon erhält, dass die Informationen am ursprünglichen Ausgangsort der Übermittlung aus dem Netz entfernt wurden oder der Zugang zu ihnen gesperrt wurde oder eine Justiz- oder Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat (lit. e).

Für Hosting haftet ein Diensteanbieter nach Art. 6 Abs. 1 DSA ebenfalls nicht für die von einem Nutzer bereitgestellten Informationen, sofern er keine tatsächliche Kenntnis von einer rechtswidrigen Tätigkeit oder rechtswidrigen Inhalten hat und sich in Bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder rechtswidrige Inhalte offensichtlich hervorgeht, (lit. a) oder sobald er diese Kenntnis oder dieses Bewusstsein erlangt, zügig tätig wird, um den Zugang zu den rechtswidrigen Inhalten zu sperren oder diese zu entfernen (lit. b).

Hochschulen und Forschungseinrichtungen, die ihren Angehörigen einen Netzzugang zur Verfügung stellen, sind von diesen Haftungserleichterungen umfasst. Nach Art. 8 DSA sind Anbieter von Vermittlungsdiensten nicht allgemein dazu verpflichtet die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hindeuten.

Anspruch auf Sperrung bei Rechtsverletzung

Nach § 8 Abs. 1 DDG hat der Inhaber eines Rechts am geistigen Eigentum einen Anspruch gegen den Diensteanbieter auf die Sperrung der Nutzung von Informationen, um die Wiederholung der Rechtsverletzung zu verhindern. Voraussetzung dafür ist, dass durch einen Nutzer ein Recht am geistigen Eigentum verletzt und dabei der digitale Dienst des Diensteanbieters zur Übermittlung in einem Kommunikationsnetz oder zur Vermittlung des Zugangs zu einem Kommunikationsnetz in Anspruch genommen wurde. Die Erstattung vor- und außergerichtlicher Kosten ist nach § 8 Abs. 3 DDG ausgeschlossen.
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 absoluten, also gegenüber jedermann geltenden, Rechten in Betracht, zu denen beispielsweise Urheberrechte und Markenrechte zählen.[2] Wegen einer Verletzung der Persönlichkeitsrechte besteht gegenüber Access-Providern kein Anspruch.[3] Grundlage eines möglichen Anspruchs des Verletzten ist die sogenannte Störerhaftung, die im Wege einer analogen Anwendung des § 1004 Abs. 1 S. 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 Verletzer des Rechts 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.[4] Die erforderliche Eigenschaft als Störer kann ebenso 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.

[2] *Schiff*, in: Heldt/Legner, DDG, § 8 Rn. 7.
[3] *Schiff*, in: Heldt/Legner, DDG, § 8 Rn. 8.
[4] *Schiff*, in: Heldt/Legner, DDG, § 8 Rn. 12.

Für anlassbezogene Prüfpflichten dagegen ist die entscheidende Frage stets, ob die begehrte Unterbindung weiterer Rechtsverletzungen zumutbar ist. Dies bedarf einer Abwägung bei der vorrangig die grundrechtlich geschützten Interessen der Beteiligten zu berücksichtigen sind. Dies sind in der Regel beim Access-Provider die unternehmerische Freiheit (Art. 16 GRCh, Art. 12 GG), und beim Rechteinhaber das geistige Eigentum (Art. 17 Abs. 2 GRCh, Art. 14 GG) und aufseiten des Dritten die Informationsfreiheit (Art. 11 Abs. 1 S. 2 GRCh, Art. 5 Abs. 1 S. 1 GG). In Bezug auf eine Sperrung des Internetzugangs sind im Hochschulbereich und in Forschungseinrichtungen bei Maßnahmen gegen Wissenschaftler oder Studierende zudem die Wissenschaftsfreiheit (Art. 13 S. 2 GRCh, Art. 5 Abs. 3 GG) und die Berufsfreiheit (Art. 15 GRCh, Art. 12 GG) in die Entscheidung über eine Sperrung einzubeziehen. 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. Wer haftet?

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 § 1 Abs. 4 Nr. 5 DDG 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, sind diese selbst und nicht etwa die Hochschule als Diensteanbieter im Sinne des § 1 Abs. 4 Nr. 5 DDG anzusehen und können haftbar gemacht werden.

Strafrechtliche Verantwortlichkeit

Strafrechtlich können nur einzelne Personen persönlich verantwortlich sein, nicht die Hochschule 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.

c. 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, Computerbetrug nach § 263a StGB, die Verbreitung rechtswidriger Inhalte, die Beleidigung §§ 185 StGB oder die Verbreitung pornographischer Inhalte nach § 184 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.

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.

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.

Verkehrsdaten

Verkehrsdaten sind Daten, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind, § 3 Nr. 70 TKG. 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 § 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. 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). Eine grundsätzliche Verpflichtung zur Speicherung besteht dabei allerdings nicht und die Etablierung eines Löschkonzepts empfiehlt sich schon aus datenschutzrechtlichen Gründen. Bei einem auf zukünftige Kommunikationsvorgänge gerichteten Auskunftsersuchen müssen die betreffenden Daten entsprechend des richterlichen Beschlusses aufgezeichnet und an die Behörden weitergegeben werden.

Bestandsdaten

Bestandsdaten sind Daten eines Endnutzers, die erforderlich sind für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste, § 3 Nr. 6 TKG. 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 § 174 Telekommunikationsgesetz (TKG). Nach § 174 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 § 174 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 Auskunft darüber gegeben 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. Die Verpflichtung zur Herausgabe erfasst sämtliche vorliegenden Daten, auch wenn diese datenschutzrechtswidrig noch nicht gelöscht wurden. Die Etablierung eines Löschkonzepts empfiehlt sich daher auch vor diesem Hintergrund.

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. Die Polizei- und Ordnungsbehörden werden in einem solchen Fall nicht repressiv als Strafverfolgungsbehörde tätig, sondern vielmehr präventiv um eine Gefahr für die öffentliche Sicherheit und/oder Ordnung (beispielsweise einen Verstoß gegen die Rechtsordnung)

abzuwehren. 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 § 174 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.

Einbindung in Ermittlungsverfahren und Prävention

Ferner können die Mitarbeiter in Rechenzentren in behördliche Maßnahmen dergestalt eingebunden werden, dass sie zum Beispiel Beobachtungen des Nutzerverhaltens an die Staatsanwaltschaft oder Polizei zukünftig weitergeben. 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.

d. 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. 5 Abs. 1 S. 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.

e. Welche datenschutzrechtlichen Anforderungen sind zu beachten?

Soweit Rechenzentren durch den Netzzugang und den E-Mail-Dienst geschäftsmäßig Telekommunikationsdienste (TK-Dienste) erbringen, sind – neben den allgemeinen Datenschutzvorschriften – besondere Datenschutzvorschriften im Bereich der Telekommunikation zu beachten. Diese Vorschriften stehen gebündelt im Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG).

Situation bei ausgeschlossener Privatnutzung

Ist die Nutzung der TK-Dienste ausdrücklich nur zu dienstlichen Zwecken erlaubt (vollständiges Verbot der Privatnutzung für Beschäftige), werden die telekommunikationsrechtlichen Vorschriften zum Datenschutz und dem Schutz der Privatsphäre nach §§ 3 ff. TDDDG nicht angewendet.

Für ein geschäftsmäßiges Erbringen von Telekommunikationsdiensten nach § 3 Abs. 2 S. 1 Nr. 2 TDDDG braucht es ein nachhaltiges Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht. Die Hochschule wäre insofern nicht als TK-Diensteanbieter zu qualifizieren, weil es sich bei einer rein dienstlichen Nutzung um eine ausschließlich interne Erbringung des Dienstes der Hochschule handelt. Die Mitarbeitenden gelten in dem Fall nicht als außenstehende Dritte. Ein Ausschluss der Privatnutzung führt dazu, dass das Fernmeldegeheimnis nach § 3 TDDDG und die telekommunikationsspezifischen Datenschutzanforderungen des TDDDG keine Anwendung finden. Das Verbot der Privatnutzung muss in der Benutzungsordnung oder Dienstvereinbarung ausdrücklich und unmissverständlich erfolgen.

Aus dem Ausschluss der Privatnutzung folgt jedoch keine unbegrenzte Zugriffsmöglichkeit auf die Kommunikationsinhalte der Mitarbeitenden. Die Kenntnisnahme und Verwendung von TK-Inhalten gehen regelmäßig auch mit der Verarbeitung personenbezogener Daten einher. So sind die Vorschriften zum Schutz personenbezogener Daten der DSGVO, des BDSG und der Landesdatenschutzgesetze einzuhalten. Für die Verarbeitung personenbezogener Daten der Beschäftigten durch den Arbeitgeber braucht es demnach eine rechtliche Grundlage. Zusätzlich sind die Informationspflichten nach Art. 13 und 14 DSGVO sowie das Auskunftsrecht nach Art. 15 DSGVO einzuhalten. Die Daten müssen stets sicher hinterlegt und die damit in Kontakt kommenden Personen entsprechend geschult sein. Nutzende können also selbst bei einem Ausschluss der Privatnutzung nur über Stichproben hinaus überwacht werden, wenn konkrete Anhaltspunkte für Verstöße oder eine missbräuchliche Nutzung vorliegen.

Ein nationales Beschäftigtendatengesetz, das weitere Regelungen treffen könnte, ist in Planung, aber befindet sich bislang noch im Entwurfsstadium (https://www.itm.nrw/wp-content/uploads/2024/10/bdsg-beschdg.pdf).

Situation bei erlaubter Privatnutzung

Bei erlaubter oder geduldeter Privatnutzung werden die TK-Dienste von Hochschulen und Forschungseinrichtungen auf Dauer, also nachhaltig, auch Dritten angeboten. Die Beschäftigten sind in diesem Fall nicht mehr der Sphäre des Arbeitgebers zuzuordnen und eine Außenwirkung liegt vor. Eine Gewinnerzielungsabsicht des TK-Dienstes ist nicht erforderlich. Rechenzentren sind als Anbieter von geschäftsmäßig angebotenen TK-Diensten somit vom Kreis der Verpflichteten nach § 3 Abs. 2 S. 1 Nr. 2 TDDDG umfasst. Die telekommunikationsspezifischen Datenschutzvorschriften des TDDDG sind zu beachten. Relevant sind insbesondere Vorgaben zum Schutz der Privatsphäre nach den §§ 3 ff. TDDDG und dem Datenschutz nach den §§ 9 ff. TDDDG. Zusätzlich müssen sie als Erbringer von TK-Diensten technische und organisatorische Schutzmaßnahmen treffen, die sich aus dem TKG ergeben (§ 165 Abs. 1, Abs. 6 TKG).

Fernmeldegeheimnis

Das Fernmeldegeheimnis ist ein Grundrecht und in Art. 10 GG verankert. Alle TK-Diensteanbieter, die die TK-Dienste ganz oder teilweise geschäftsmäßig anbieten, sind nach § 3 Abs. 2 S. Nr. 2 TDDDG zur Wahrung des Fernmeldegeheimnisses verpflichtet. Dazu gehören auch konkrete Verhaltenspflichten nach § 3 Abs. 3 TDDDG. Demnach ist es verboten, vom Inhalt oder den näheren Umständen der Telekommunikation Kenntnis zu nehmen, sofern dies nicht zur Erbringung des TK-Dienstes oder den Betrieb des TK-Netzes einschließlich des Schutzes eines technischen Systems erforderlich ist. Hochschulrechenzentren sind von dieser Pflicht umfasst, sofern eine Privatnutzung der Dienste erlaubt bzw. geduldet ist. Die Einsichtnahme in E-Mail-Postfächer einzelner Nutzenden oder die Überwachung des Mail-Verkehrs durch die Systemadministration sind ohne Einwilligung der Betroffenen grundsätzlich unzulässig. Dieser allgemeine Schutz des Fernmeldegeheimnisses wird durch die Vorgaben zum Datenschutz und zur Datensicherheit ergänzt und konkretisiert.

Datenschutzrechtliche Vorgaben

Hochschulen und Forschungseinrichtungen haben bei erlaubter Privatnutzung die telekommunikationsspezifischen Datenschutzvorschriften zu beachten. Durchgängiger Grundsatz des Datenschutzrechts ist es, dass die Verarbeitung personenbezogener Daten nur erlaubt ist, wenn eine gesetzliche Erlaubnisnorm dies vorsieht oder eine Einwilligung der betroffenen Person vorliegt. Grundsätzlich wird hier zwischen Bestands-, Verkehrs- und Steuerdaten unterschieden.

(1) Bestandsdaten

Bestandsdaten sind Daten von Nutzenden, deren Verarbeitung für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertrags über die Dienstnutzung erforderlich sind. Dies sind beispielsweise Name, Anschrift des Users oder eine fest vergebene IP-Adresse. Sie betreffen keine konkreten Telekommunikationsvorgänge und sind nicht vom Fernmeldegeheimnis umfasst. Das TDDDG enthält in dem datenschutzrechtlich relevanten Teil 2 keine speziellen Regelungen zu Bestandsdaten, sodass sich eine Verarbeitung nach der DSGVO (allen voran Art. 6 Abs. 1 lit. b DSGVO) richtet.

(2) Verkehrsdaten

Verkehrsdaten sind Daten, die bei der Erbringung von TK-Diensten erhoben, verarbeitet oder genutzt werden (§ 3 Nr. 70 TKG). Darunter sind der Beginn und das Ende von Internetverbindungen, übermittelte Datenmengen, besuchte Webseiten oder dynamisch vergebene IP-Adressen zu verstehen. Im Unterschied zu den Bestandsdaten, fallen Verkehrsdaten regelmäßig und weitgehend automatisch bei einem tatsächlichen Telekommunikationsvorgang an. Da sie Aufschlüsse über die näheren Umstände der Kommunikation liefern können, werden sie insoweit vom Fernmeldegeheimnis erfasst und genießen zusätzlichen Schutz.

§§ 9-12 TDDDG enthalten spezielle Vorgaben zur Verarbeitung von Verkehrsdaten. Die Rechtslage ist entsprechend komplexer, wobei auch hier der allgemeine Grundsatz gilt, dass entweder eine gesetzliche Erlaubnis oder eine Einwilligung für die Verarbeitung der Daten bestehen muss.

§ 9 TDDDG führt verschiedene Erlaubnistatbestände für die Verarbeitung von Verkehrsdaten auf. Nach § 9 Abs. 1 S. 1 TDDDG dürfen die zum Aufbau und zur Aufrechterhaltung der Telekommunikation, zur Entgeltabrechnung oder zum Aufbau weiterer Verbindungen erforderlichen Daten verarbeitet werden. Die konkret umfassten Verkehrsdaten werden in § 9 Abs. 1 S. 1 Nr. 1-5 TDDDG aufgeführt. Die Befugnisse enthalten damit alle betrieblich notwendigen Daten für die Erbringung der Kommunikationsleistung. Nach dem Ende der jeweiligen Verbindung sind die Verkehrsdaten unverzüglich zu löschen, § 9 Abs. 1 S. 2 TDDDG. Eine Löschung umfasst nicht nur die Vernichtung der Daten, sondern kann auch eine technisch korrekt ausgeführte Anonymisierung bedeuten. Die Löschung 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. Werden Verkehrsdaten zu anderen Zwecken verarbeitet, ist dies gem. § 9 Abs. 1 S. 3 TDDDG unzulässig, es sei denn, andere rechtliche Vorschriften sehen eine Verarbeitung von Verkehrsdaten vor, § 9 Abs. 1 S. 4 TDDDG.

Im TDDDG bestehen folgende Befugnisse zur Verarbeitung von Verkehrsdaten, die für Hochschulen und Forschungseinrichtungen von Bedeutung sein können:

Eine (allein) theoretische Bedeutung hat die Erlaubnis nach § 10 TDDDG, demzufolge Verkehrsdaten nach Beendigung der Verbindung gespeichert und verwendet werden dürfen, soweit sie zur Ermittlung oder Abrechnung von Entgelten benötigt werden. In aller Regel ist die Internetnutzung für Studierende und Mitarbeitende an Hochschulen jedoch kostenlos und

es gibt keinerlei Abrechnung der in Anspruch genommenen Dienste. Sollte dies ausnahmsweise anders sein, ist zu beachten, dass die Daten zu diesem Zweck erforderlich sein müssen. Sofern keine interne Abrechnung stattfindet, 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 ab dem Zeitpunkt der Versendung der Rechnung gespeichert werden. Auch eine mögliche Mitteilung von Einzelverbindungsnachweisen nach § 11 TDDDG ist an die Entgeltlichkeit der TK-Dienste gebunden.

Von großer praktischer Relevanz ist allerdings die Erlaubnisnorm des § 12 TDDDG. Dieser erlaubt eine Verarbeitung von Verkehrsdaten, um Störungen von TK-Anlagen und dem Missbrauch von TK-Diensten zu begegnen. So darf der Diensteanbieter nach § 12 Abs. 1 S. 1 TDDDG zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an TK-Anlagen Verkehrsdaten verarbeiten. Nach § 12 Abs. 1 S. 2 TDDDG gilt dies auch für Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und TK-Diensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzenden führen können. Dabei ist stets zu prüfen, ob die Datenverarbeitung geeignet, erforderlich und im engeren Sinn verhältnismäßig ist, um abstrakten Gefahren für die Funktionstüchtigkeit des Telekommunikationsbetriebs entgegenzuwirken.

Für das „Erkennen“ von Störungen und Fehlern muss noch kein konkreter Verdacht bestehen, denn in der Regel findet das Erkennen in einem Stadium statt, in dem Anhaltspunkte für die Störungen und Fehler erst gewonnen werden müssen (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 gem. § 12 Abs. 2 TDDDG zu löschen, sofern keine 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; siehe auch: Leitfaden des BfDI für eine datenschutzgerechte Speicherung von Verkehrsdaten, 30.9.2022, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Themen/Telekommunikation/LeitfadenZumSpeichernVonVerkehrsdaten.pdf?__blob=publicationFile&v=4; Kritisch Braun, in: Geppert/Schütz, Beck’scher TKG-Kommentar, 5. Aufl. 2023, TTDSG § 12 Rn. 14). Nach sieben Tagen sind sie jedoch zu löschen, soweit keine anderen gesetzlichen Ermächtigungen vorliegen.

Im Fall einer nicht automatisierten Erhebung und Verwendung der Daten ist der Datenschutzbeauftragte des Diensteanbieters gem. § 12 Abs. 1 S. 4 TDDDG unverzüglich zu informieren.

Nach § 12 Abs. 4 TDDDG kann der Diensteanbieter bei Vorliegen tatsächlicher Anhaltspunkte auch Verkehrsdaten (gegebenenfalls sogar länger als sieben Tage) verarbeiten, die zum Aufdecken sowie Unterbinden einer rechtswidrigen Inanspruchnahme der TK-Netze 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 Datenverarbeitung muss der Sicherung des Entgeltanspruchs dienen. Für die weiteren Einzelheiten wird auf § 12 Abs. 4 TDDDG 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 § 12 Abs. 4 TDDDG für Hochschulen und Forschungseinrichtungen wegen der unentgeltlichen Zurverfügungstellung der Dienste eher gering sein.

Eine sonstige Verarbeitung von Verkehrsdaten außerhalb der gesetzlich eingeräumten Befugnisse bedarf der Einwilligung durch den Betroffenen. Diese Einwilligung muss den Voraussetzungen des Art. 4 Nr. 11, Art. 7 DSGVO genügen. Erforderlich ist eine eindeutig bestätigende Handlung, die das Einverständnis der betroffenen Person mit der Datenverarbeitung unmissverständlich zum Ausdruck bringt. Einer besonderen Form bedarf es nicht. Die bestätigende Handlung kann auch elektronisch zB durch „Anklicken“ eines Feldes im Internet oder auch mündlich erfolgen, sofern der Verantwortliche die Erteilung der Einwilligung nachweisen kann (vgl. Erwägungsgrund 32 der DSGVO).

(3) Steuerdaten

Die Bestimmungen zur Datenverarbeitung nach § 12 Abs. 1, Abs. 2 TDDDG gelten auch für Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung. Dies sind in der Regel Informationen zu technischen Übertragungsprotokollen, die unabhängig von den Kommunikationsinhalten übertragen werden und Aufschlüsse zu Schadprogrammen oder Malware geben können.

Technische Schutzmaßnahmen zur Datensicherheit

Nach § 165 Abs. 1 TKG haben TK-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 TK-Diensteanbieter und Betreiber von Netz-Servern und Routern. Im Hinblick auf das Fernmeldegeheimnis muss jeder Diensteanbieter verhindern, dass Eingriffe in das Fernmeldegeheimnis vorgenommen werden, die nicht von gesetzlichen Erlaubnistatbeständen gedeckt sind. Zusätzlich dürfen 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 Mitarbeitenden. Hierbei ist neben technischen

Schutzvorkehrungen vor allem an Zugangskontrollen für sensible Bereiche, Zugriffsbeschränkungen auf Datenbestände und an die Schulung der Mitarbeitenden in Bezug auf den Umgang mit personenbezogenen Daten zu denken.

Unter der „Verletzung des Schutzes personenbezogener Daten“ wird nach der Legaldefinition des § 3 Nr. 71 TKG eine Verletzung der Datensicherheit verstanden, die zum Verlust, zur unrechtmäßigen Löschung, Veränderung, Speicherung, Weitergabe oder sonstigen unrechtmäßigen Verwendung personenbezogener Daten führt, sowie der unrechtmäßige Zugang zu diesen.

Verlangt werden angemessene technische Schutzmaßnahmen nach § 165 Abs. 6 TKG, 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 § 165 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 Art. 32 DSGVO zum Schutz der personenbezogenen Daten, die Verpflichtung zu angemessenen Maßnahmen zur Datensicherheit in datenverarbeitenden Stellen. Hochschulen und Forschungseinrichtungen haben daher, unabhängig von ihrer Eigenschaft als Anbieter von TK-Diensten, Datenbestände gegen unerlaubte Zugriffe von innen wie außen durch angemessene Maßnahmen zu schützen. Art. 32 Abs. 1 lit. a bis lit. d DSGVO nennt Maßnahmen, die in jedem Fall in Betracht gezogen werden müssen. Die Liste ist allerdings nicht abschließend. Wichtige Beispiele von Maßnahmen sind auch hier ein wirksamer Passwortschutz, regelmäßige Updates, Schulungen der Mitarbeitenden und Maßnahmen zum Schutz der Informationsinfrastruktur vor Viren.

f. 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:

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.).

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 § 9 ff. TDDDG und das Fernmeldegeheimnis aus § 3 TDDDG 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 OLG 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.

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 § 165 Abs. 1 TKG und der allgemeinen Verpflichtung datenverarbeitender Stellen zur Gewährleistung der Datensicherheit aus den Datenschutzgesetzen (Art. 5 Abs. 1 lit. f DSGVO) 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.

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 von Einrichtungen 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 §§ 9 ff. TDDDG nicht in Betracht. Auch das in § 3 TDDDG 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

a. 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.

b. Rechtliche Anforderungen an Webangebote

Informationspflicht beim Betrieb von Telemedien

(4) Grundanforderungen für Telemedien

Das Digitale-Dienste-Gesetz (DDG) sowie einzelne Normen des Rundfunkstaatsvertrags (MstV) enthalten die wirtschafts- und inhaltsbezogenen Grundanforderungen für Telemedien.

§ 5 DDG statuiert wie die alten Regelungen im Telemediengesetz (TMG) und Mediendienste-Staatsvertrag (MDStV) umfassende Informationspflichten (auch „Impressumspflicht“ genannt), die zu mehr Transparenz von Angeboten im Internet führen sollen. 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 § 18 Abs. 1 Medienstaatsvertrag (MStV). 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 DDG 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.

Auch wenn das Angebot keine Dienste enthält, die in der Regel gegen Entgelt erbracht werden, können aufgrund des Verweises in § 5 Abs. 2 DDG nach anderen Rechtsvorschriften weitergehende Informationspflichten bestehen. Dies ist auf Grund von § 18 Abs. 1 Medienstaatsvertrag (MStV) 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 DDG fehlt, muss das Impressum nach § 18 Abs. 1 MStV zumindest diese Angaben enthalten, wobei als Vertretungsberechtigter bei Hochschulen wiederum in der Regel der Rektor anzugeben ist.

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.

c. 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.

Haftung für eigene Inhalte

Für die eigenen Inhalte ist die Hochschule nach den allgemeinen Gesetzen voll verantwortlich, Art. 4 und 5 Digital Services Act (DSA) bzw. §§ 7, 8 Digitale-Dienste-Gesetz (DDG). 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.

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 Art. 6 DSA, § 7 DDG 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 Hyperlinks 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 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 ihm (?) 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.

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.

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 NRW, 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. § 1 Abs. 4 Nr. 5 DDG anzusehen und können als solche haftbar gemacht werden.

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.

d. 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.

e. 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 Art. 6 DSA, § 7 DDG genauso verantwortlich, als würde es sich um seinen eigenen Inhalt handeln (siehe ausführlich Kapitel: Bereitstellung von Speicherplatz für fremde Inhalte).

f. 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.

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.

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 sogenannten „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 Art. 6 DSA bzw. § 7 DDG, 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 Art. 6 DSA bzw. § 7 DDG 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.

IV. Rechtslage bei der Zurverfügungstellung von Speicherplatz für fremde Inhalte

a. 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.

b. 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 privilegierte Haftung des Host-Providers ist seit dem 17.02.2024 im Digital Services Act (DSA) geregelt.

Grundsatz: Nichtverantwortlichkeit für fremde Inhalte auf eigenen Servern

Der Grundsatz der Nichtverantwortlichkeit für fremde Inhalte auf eigenen Servern ist in Art. 6 DSA geregelt. Danach sind Diensteanbieter im Grundsatz nicht für fremde Informationen verantwortlich, die sie für einen Nutzer speichern, also z. B. für die Inhalte privater Homepages von Studierenden.

Hierdurch wird eine Haftungsprivilegierung für einen rein passiven Hostprovider geregelt, der die Inhalte nicht erstellt, auswählt, sichtet oder kontrolliert. (NK-DSA/*F. Hofmann*, 1. Aufl. 2023, DSA Art. 6 Rn. 14) Er erbringt den Dienst auf neutrale Weise, indem er die bereitgestellten Informationen automatisch verarbeitet. (NK-DSA/*F. Hofmann*, 1. Aufl. 2023, DSA Art. 6 Rn. 14) Die Haftungsprivilegierung bezieht sich auf die strafrechtliche Verantwortlichkeit und privatrechtliche Schadensersatzansprüche. (NK-DSA/*F. Hofmann*, 1. Aufl. 2023, DSA Art. 6 Rn. 24) Gemäß Art. 6 Abs. 2 DSA soll die Haftungsprivilegierung jedoch nicht greifen, wenn der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird. Hierbei verlässt der Anbieter seine rein passive Rolle.

Ausnahmen in Art. 6 DSA

Art. 6 DSA spezifiziert jedoch auch die Fälle, in denen der Diensteanbieter seine passive Rolle verlässt.

Gemäß Art. 6 Abs. 1 DSA gilt die Privilegierung für den Hostprovider nur, sofern er a) keine tatsächliche Kenntnis von einer rechtswidrigen Tätigkeit oder rechtswidrigen Inhalten hat und sich in Bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder rechtswidrige Inhalte offensichtlich hervorgeht, oder b) sobald er diese Kenntnis oder dieses Bewusstsein erlangt, zügig tätig wird, um den Zugang zu den rechtswidrigen Inhalten zu sperren oder diese zu entfernen.

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.

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.

Art. 6 Abs. 4 DSA regelt hierzu, dass trotz der Haftungsprivilegierung von einem Diensteanbieter verlangt werden kann, eine Rechtsverletzung abzustellen oder zu verhindern. Damit kann auch vom Host-Provider verlangt werden, dass dieser rechtswidrige Inhalte entfernen muss und damit als Störer haftet. In seiner Rechtsprechung zu den nahezu inhaltsgleichen Vorschriften im Telemediengesetz (TMG) hat der BGH eine solche Haftung als mittelbarer Störer für denjenigen angenommen, der willentlich und adäquat kausal zur Rechtsverletzung beiträgt. Erforderlich ist die Verletzung von Verhaltenspflichten, insbesondere Prüfpflichten. (BGH, NJW 2022, 3072, 3074 ff.) Hierzu muss im Einzelfall entschieden werden, ob dem Diensteanbieter eine Prüfung der fremden Inhalte zumutbar ist. Der BGH hat hierzu in seiner Rechtsprechung zum TMG allerdings ausgeführt, dass ein Host-Provider grundsätzlich nicht verpflichtet ist, Informationen vor der Veröffentlichung auf Rechtsverletzungen zu überprüfen. Sobald er aber Kenntnis von einer Rechtsverletzung erlangt, ist er verantwortlich. Dann kann er auch verpflichtet sein, zukünftige gleichartige Störungen zu verhindern (BGH, NJW 2022, 3072, 3074; BGH, NJW 2018, 2324, 2327; BGH, NJW 2016, 2106, 2108). Damit kann ein Diensteanbieter über das Rechtsinstitut der Störerhaftung auch verpflichtet sein, proaktiv weitere Rechtsverletzungen in der Zukunft zu verhindern, sofern er über solche in der Vergangenheit informiert wurde. Das LG Düsseldorf hat angenommen, dass diese höchstrichterliche Rechtsprechung zum alten TMG auch unter Geltung des DSA in gleicher Weise fortgeführt werden kann. (LG Düsseldorf, Urteil vom 04.12.2024, 2a O 112/23).

Bei Hinweisen auf rechtsverletzende Inhalte sollte das Justitiariat daher umgehend zur weiteren Prüfung eingeschaltet und der fragliche Inhalt bis zur Klärung vorübergehend gesperrt werden (siehe oben; Art. 6 DSA). Die Kenntnisnahme einer klaren Rechtsverletzung kann auch dazu führen, dass der Rechtsverletzer nicht nur das konkrete Angebot unverzüglich sperren, sondern auch Vorsorge treffen muss, dass es möglichst nicht zu weiteren derartigen Verletzungen kommt. (BGH, Urteil vom 17. 8. 2011 – I ZR 57/09, GRUR 2011, 1038). Ob eine solche weite Prüfpflicht aufgrund vergangener Rechtsverletzungen anzunehmen ist, bestimmt sich aber jeweils nach den Umständen des Einzelalls.

Wegen der rechtlichen Unsicherheiten ist es ratsam, zu überlegen, ob es Vorsorgemaßnahmen gegen weitere Verletzungen gibt, die zumutbar getroffen werden könnten. Es bleibt 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 Art. 6 DSA 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 (zu § 7 TMG siehe BGH, Urteil vom 11.3.2004 – Az. I ZR 304/01, MMR 2004, 668).

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 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.

c. Verdacht auf Straftaten

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.

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.

d. 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 Art. 6 DSA (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.

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 Musterbenutzungsordnung). Auch wenn eine solche explizite Regelung nicht besteht, sollte aufgrund der eingangs skizzierten möglichen massiven Folgen eine vorübergehende Sperrung erfolgen.

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.

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.