DFN

Infobrief Recht

DFN-Infobrief Recht

Jahresband 2015

Impressum

Herausgeber: Verein zur Förderung eines
Deutschen Forschungsnetzes e. V.

DFN-Verein
Alexanderplatz 1, D-10178 Berlin
Tel: 030 - 88 42 99 - 0
Fax: 030 - 88 42 99 -370
E-Mail: dfn-verein@dfn.de
Web: www.dfn.de

Texte: Forschungsstelle Recht im DFN
Ein Projekt des DFN-Vereins an der Westfälischen
Wilhelms-Universität, Institut für Informations-,
Telekommunikations- und Medienrecht (ITM),
Zivilrechtliche Abteilung, unter Leitung von
Prof. Dr. Thomas Hoeren.
Leonardo-Campus 9,
D-48149 Münster
Mail: recht@dfn.de
Web: www.dfn.de/rechtimdfn/

ISSN 2194-3036

Redaktion: Christine Legner-Koch
Layout und redaktionelle Bearbeitung: Kai Hoelzner, Nina Bark
Umschlagfoto: Torsten Kersting / DFN-Verien
Druck: Laserline, Berlin

Liebe Leserinnen und Leser,

die Nutzung neuer Formen der Kommunikation und der Informationsverarbeitung führt zwangsläufig zu neuen, bislang wenig oder gar nicht bearbeiteten rechtlichen Fragestellungen. Dem DFN-Verein ist bewusst, dass Antworten auf solche Rechtsfragen von großer Bedeutung sind, um die neuen Formen der Kommunikation und der Informationsverarbeitung in die täglichen Prozesse von Forschung und Lehre erfolgreich und nutzbringend einbinden zu können.

Vor diesem Hintergrund erarbeitet die Forschungsstelle Recht im DFN eine Vielzahl von Stellungnahmen und Handlungsempfehlungen, die in periodischen digitalisierten Publikationen wie z. B. dem „DFN-Infobrief Recht“ an Abonnenten verschickt, auf den Webseiten des DFN-Vereins veröffentlicht und durch regelmäßige Seminare und Gastvorträge aktiv an die Nutzer des Wissenschaftsnetzes vermittelt werden. Die Publikationen sind in digitalisierter Form auf den Webseiten des DFN-Vereins archiviert und abrufbar unter der Adresse: http://www.dfn.de/rechtimdfn/

Mit dem vorliegenden „DFN-Infobrief Recht - Sammelband 2015“ werden diese digitalisierten Publikationen nun durch eine gedruckte Zusammenfassung ergänzt.

Wir würden uns freuen, wenn auf diesem Wege die Stellungnahmen und Handlungsempfehlungen der Forschungsstelle Recht im DFN eine weitere Sichtbarkeit erreichen und damit insbesondere auch den Mitgliedern des DFN-Vereins die eine oder andere bislang ungelöste rechtliche Fragestellung einer Beantwortung näher gebracht wird.

Wir wünschen Ihnen eine gewinnbringende Lektüre.

Ihr DFN-Verein

Inhalt

Funkstille in Deutschland

Warum offene WLAN kommen und die Störerhaftung für WLAN-Betreiber abgeschafft werden sollte

von Susanne Thinius

In keinem anderen Land, abgesehen von Russland, Italien und einigen Regimestaaten, sind die Regelungen zum WLAN (Wireless Local Area Network, drahtloses lokales Netzwerk) derart streng wie in Deutschland. Unter zwei Millionen WLAN-Spots in der Bundesrepublik gibt es lediglich 15.000 offene – eine geringe Zahl im weltweiten Vergleich. Der Grund überrascht nicht – so haften private Anbieter aufgrund der Störerhaftung für fremde (Urheber-) Rechtsverletzungen im Gegensatz zu kommerziellen Anbietern. Das könnte sich mit dem nun vorgelegten Gesetzesentwurf in Deutschland ändern – denn die Oppositionsparteien wollen die Störerhaftung für öffentliche WLANs abschaffen. Doch wie reagiert die Bundesregierung darauf?

Begriffserläuterungen

Zunächst sollen einige grundlegende Begriffe rund um die Haftung für fremde, durchgeleitete Informationen geklärt werden:

Kommunikationsnetze (im Sinne des § 8 Telemediengesetz, TMG) sind all diejenigen Netze, über die Signale übertragen werden können, gleichgültig ob kabelgebunden oder nicht. Der Begriff umfasst lokale kabelgebundene („LAN“, „Local Area Network“) und drahtlose („WLAN“, „Wireless LAN“) Netze.

Offen ist ein WLAN, wenn im Router, welcher den Zugang zum Internet herstellt, keine Zugangskontrolle aktiviert ist und praktisch jedermann in Reichweite des Routers Zugriff auf das Internet hat. Für diesen Fall kann der Anschlussinhaber für rechtswidrige Handlungen Dritter, die über seinen Anschluss begangen werden, haftbar gemacht werden, und zwar über das Konstrukt der Störerhaftung.

Als **Störer** kann grundsätzlich in Anspruch genommen werden, wer – ohne selbst Täter oder Teilnehmer einer Rechtsverletzung zu sein – in irgendeiner Weise willentlich und „adäquat kausal“ zur Verletzung des Rechts beiträgt. Der Betrieb eines nicht ausreichend gesicherten WLAN-Anschlusses ist adäquat kausal für Rechtsverletzungen Dritter, die diese unter Einsatz des fremdes Anschlusses begehen (so der Bundesgerichtshof, BGH, in seiner Entscheidung „Sommer unseres Lebens“ vom 12.5.2010, I ZR 121/08). Der BGH stellte fest, dass es privaten Anschlussinhabern zumutbar sein kann zu prüfen, ob ihre Anschlüsse durch ausreichende Sicherungsmaßnahmen vor Missbrauch durch Dritte geschützt sind. Die Sicherung kann durch Zugangskontrollen (Passwörter, Nutzernamen), Verschlüsselungen oder Viren-Updates gewährleistet werden. Eine fortlaufende Überprüfungspflicht der Sicherungsmaßnahmen verneinte der BGH allerdings.

Im Rahmen der **Störerhaftung** wird nur auf Unterlassen, nicht jedoch Schadenersatz gehaftet. Die Haftung beginnt mit Kenntnis von der konkreten Rechtsverletzung und hängt, wie bereits erwähnt, von der Verletzung konkreter Prüfungs- und Überwachungspflichten ab. Die Konkretisierung dieser Pflichten wurde bislang von den Gerichten uneinheitlich bewertet. Die Störerhaftung ist Richterrecht, es gibt keine gesetzliche Regelung dazu.

Das Telemediengesetz (TMG), welches Regelungen zur Haftung für fremde Rechtsverletzungen im Internet bereithält, erwähnt ferner den Begriff des **Diensteanbieters**. Diensteanbieter im Sinne des § 2 S. 1 Nr. 1 TMG ist „jede natürliche oder juristische Person, die eigene oder fremde Telemedien (Definition in § 1 TMG) zur Nutzung bereithält oder den

Zugang zur Nutzung vermittelt“. Die Regelung zielt in erster Linie auf Provider ab, also diejenigen Anbieter, die Dienste der Informationsgesellschaft (vorwiegend entgeltlich) erbringen. Es wird jedoch teilweise die Ansicht vertreten, dass jegliche Internetanschlussinhaber als Diensteanbieter zu qualifizieren sind, einschließlich Private sowie Hochschulen als öffentlich-rechtliche Körperschaften. Damit unterlägen sie den Haftungsregelungen des TMG. Der BGH äußert sich zur Dienstanbietereigenschaft von WLAN-Betreibern nicht. Es besteht also Rechtsunsicherheit bezüglich der Einordnung von Anbietern offener WLANs.

Bisherige und neue Regelungen zur Haftung von Anschlussinhabern

Diese Rechtsunsicherheit betrifft also die Fragen, ob Anbieter offener WLANs als Diensteanbieter beziehungsweise als Täter oder Störer haften. Bislang wurden sie von den Gerichten als Störer qualifiziert, da das sogenannte Providerprivileg aus § 8 TMG nicht für offene WLANs gelte. Als Störer haften sie grundsätzlich dann verschuldensunabhängig, wenn sie offene, ungeschützte WLAN-Spots anbieten. Zusätzlich zum Anspruch auf Unterlassen kann der Anspruch eines Anwalts auf Erstattung seiner Abmahnkosten hinzutreten. Geregelt ist diese Störerhaftung, wie bereits erwähnt, jedoch nicht. Wieso der BGH private Anbieter und kommerzielle Anbieter von WLAN unterschiedlich behandelt, ist nicht ersichtlich.

Kommerziellen beziehungsweise gewerblichen Anbietern wie der Telekom kommt hingegen § 8 TMG zugute. Nach dessen Absatz 1 sind Diensteanbieter für fremde Informationen, die sie in einem Kommunikationsnetz (gemeint ist auch WLAN) übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, wenn sie die Übermittlung nicht veranlasst haben, den Adressaten der übermittelten Informationen nicht ausgewählt beziehungsweise die Informationen nicht ausgewählt oder verändert haben. Zweck dieser Vorschrift ist es, automatisierte Vorgänge ohne bewusste Eingriffe in die durchgeleiteten Informationen von der Haftung freizustellen. In der Rechtsfolge wird der Provider von der Haftung nach zivilrechtlichen, strafrechtlichen und verwaltungsrechtlichen Vorschriften freigestellt.

Die soeben erläuterte Rechtsunsicherheit will die Regierungsopposition mit ihrem jüngst eingebrachten Gesetzesvorschlag begegnen, mit dem der ursprüngliche § 8 TMG überarbeitet und an die spezifischen Belange des Anbietens von offenem WLAN angepasst werden soll.

Konkret macht die Opposition den Änderungsvorschlag, § 8 TMG (bislang Absatz 1 und 2) um die Absätze 3 und 4 zu erweitern. Absatz 3 soll die Anwendbarkeit des Haftungsausschlusses („Providerprivileg“) auf gewerbliche und nichtgewerbliche Betreiber von Funknetzwerken erweitern, die sich an einen nicht im Voraus namentlich bestimmten Nutzerkreis richten (= öffentliche Funknetzwerke). Damit sind nun ausdrücklich auch WLAN-Netze gemeint. Anbieter von öffentlichem WLAN werden damit zu Diensteanbietern und profitieren von der Haftungsfreistellung. In Absatz 4 sieht der Gesetzesentwurf den Ausschluss der Haftung beziehungsweise den Ausschluss der Verantwortlichkeit auch für Unterlassungsansprüche und nicht lediglich Schadenersatzansprüche vor. Die Haftungsprivilegierung wird also auch diesbezüglich erweitert.

Reaktion der Bundesregierung

Die Bundesregierung ist hingegen der Ansicht, dass es keiner derartigen gesetzlichen Erweiterung im Hinblick auf Haftungsbeschränkungen bedarf, da die Rechtsprechung mit der Störerhaftung klar umgrenzte Sachverhalte geregelt hat. Für nicht kommerzielle Betreiber offener WLANs bedeutet dies weiterhin Rechtsunsicherheit. Mit einer Gesetzesänderung ist momentan dennoch nicht zu rechnen, auch wenn die Regierung bereits im Koalitionsvertrag ankündigte, die Potenziale von lokalen Funknetzen als Zugang zum Internet im öffentlichen Raum auszuschöpfen und die gesetzlichen Grundlagen für die Nutzung der offenen Netze und deren Anbieter zu schaffen.

Die Vorlage durch das Landgericht (LG) München I

Mit dem LG München I hat sich nun im September diesen Jahres (Beschluss vom 18.09.2014, Az. 7 O 14719/12) ein weiteres Gericht mit der Haftung für offene WLANs beschäftigt.

Der Kläger betrieb vorliegend ein frei zugängliches Netzwerk und erhielt eine Abmahnung, weil über seinen Anschluss Musiktitel illegal ins Netz gestellt wurden. Er begehrte die Feststellung, dass er nicht verpflichtet sei, Vorkehrungen zu treffen, damit über seinen Internetanschluss keine Rechts-

verletzungen mehr begangen werden. Das Gericht setzte das Verfahren aus und fragte den Europäischen Gerichtshof (EuGH), welche Sorgfaltspflichten der Betreiber eines freien WLAN (im Rahmen der Störerhaftung) treffen. Es geht dem Grunde nach um die Auslegung der Richtlinie über den elektronischen Geschäftsverkehr (2000/31/EG), welche wiederum für nationales Recht wegweisend ist.

Im Prinzip betrifft die Entscheidung damit all diejenigen Fragen, die auch schon die Opposition mit ihrem Gesetzesentwurf aufgeworfen hat. So soll vom EuGH beispielsweise geklärt werden, was ein Anbieten von Dienstleistungen „in der Regel gegen Entgelt“ bedeutet, was es bedeutet, einen „Zugang zu einem Kommunikationsnetz (z. B. dem Internet) zu vermitteln“, ob es für ein „Anbieten“ ausreicht, wenn ein Dienst der Informationsgesellschaft (beispielsweise offene WLANs) rein tatsächlich zur Verfügung gestellt wird oder ob es eines „Anpreisens“ bedürfe und was grundsätzlich unter dem Begriff „Diensteanbieter“ zu verstehen ist. Ferner soll geklärt werden, ob eine Haftungsfreistellung Unterlassungsansprüche und den Ersatz von Abmahnkosten umfasst und welche individuellen Schutzmaßnahmen vom Anschlussinhaber zu treffen sind. Die Entscheidung des EuGH wird mit Spannung erwartet.

Konsequenzen und Fazit

Die eingangs erläuterten Oppositionsvorschläge überzeugen, denn es ist nicht einzusehen, warum eine Haftungsfreistellung nur für große kommerzielle Provider und nicht für kleinere Anbieter gelten soll. Auch die Bundesregierung erkennt (bereits im Koalitionsvertrag), dass Rechtssicherheit für WLAN-Betreiber dringend geboten ist, handelt aber nicht. Das ist nicht nachvollziehbar. Es bleibt zu hoffen, dass der EUGH diesbezüglich Rechtssicherheit und die Regierung mit nationalem Recht entsprechend Abhilfe schafft. Ob die Einstellung der Bundesregierung zur Regelung offener WLANs auf lange Sicht Bestand hat und die Störerhaftung nicht sogar dem technischen Fortschritt und dem Ausbau von WLAN-Netzen in Deutschland entgegensteht, ist fraglich.

Das Internet ist ein wichtiger Teil der Infrastruktur für Gesellschaft und Wirtschaft, ohne Internet ist im digitalen Zeitalter kaum noch Entwicklung und Fortschritt möglich. Es ermöglicht freien Zugang zu Wissen, Information und Bildung. Offene WLANS bieten einen zusätzlichen Service für Gewerbetreibende und für die Vernetzung untereinander, beispielsweise in Kommunen, aber auch in der Wissenschaftswelt. Dies zu erreichen, sollte unkompliziert und ohne Haftungsrisiken möglich sein. Davon ist Deutschland leider noch weit entfernt. Es hat sich mittlerweile eine regelrechte Abmahnlobby entwickelt (mit Abmahnkosten in schwindelerregender Höhe), welcher Einhalt geboten werden muss, insbesondere dann, wenn Rechtsverletzungen durch Dritte über offene WLANs begangen werden. Hier gilt es, den Verbraucherschutz zu stärken. Auch Hochschulen, wenn auch nicht unbedingt als private, sondern öffentliche WLAN-Betreiber - sind vor Abmahnwellen nicht gefeit. Das gilt insbesondere für die Zukunft, auch wenn offene WLANS an deutschen Hochschulen noch nicht so weit verbreitet sind. Dieser Tendenz könnte durch klare gesetzliche Regelungen Einhalt geboten werden. Hierfür sind einheitliche Regelungen, ob für private, öffentliche oder gewerbliche Anbieter, unerlässlich.

Eine gesetzliche Regelung der Haftungsbegrenzung der WLAN-Betreiber, ob privat, öffentlich oder gewerblich, ist unerlässlich. Weder die Begrenzung des BGH auf Unterlassungsansprüche noch die fehlende gesetzliche Regelung der Störerhaftung sorgten bisher für die Schaffung notwendiger Rechtssicherheit.

Zu klären gilt es zudem, zu welchen Maßnahmen der WLAN-Betreiber zur Sicherung seiner Netze verpflichtet ist (Passwort für jeden einzelnen Nutzer oder ein einheitliches Passwort für das gesamte Netz, Häufigkeit der Änderung des Passwortes etc.). Denn die Ausführungen des BGH („Sommer unseres Lebens“) zu individuellen Prüfpflichten überzeugen an dieser Stelle ebenfalls nicht: aufgrund der Dynamik von Angriffen im Internet ist eine fortlaufende Anpassung der Sicherheitsmaßnahmen erforderlich, der Verzicht des BGH auf die Aktualisierung des Schutzes der Netze für alle Zeit erscheint daher nicht angemessen.

Den Hochschulen sei geraten, die Nutzer ihres WLANs über das Verbot von (Urheber-) Rechtsverletzungen und mögliche Sanktionen umfassend aufzuklären. Sollte es dennoch zu Haftungsansprüchen von außen kommen, können sie gegebenenfalls Regeressansprüche gegenüber den Rechtsverletzern geltend machen. Bei der Abgabe von Unterlassungserklärungen ist stets die Rechtsabteilung hinzuzuziehen, welche die Entwicklungen in der Rechtswelt nicht aus den Augen verlieren sollte.

Keine (individuelle) Antwort ist auch eine Antwort – aber reicht das aus?

LG Koblenz und LG Berlin konkretisieren Anforderungen an Angabe einer E-Mail-Adresse im Impressum

von Florian Klein

Dass Anbieter von Informationsangeboten im Internet einer Impressumspflicht unterliegen, ist mittlerweile gemeinhin bekannt. Das „Wie" der Umsetzung dieser Informationspflichten wirft dagegen deutlich mehr Fragen auf. Nun haben sich das Landgericht (LG) Koblenz (Urteil vom 3.11.2014 – Az. 15 O 318/13) und das LG Berlin (Urteil vom 28.8.2014 – Az. 52 O 135/13) zu der Frage geäußert, wann eine im Impressum angegebene E-Mail-Adresse eine unmittelbare Kommunikation ermöglicht und dabei Vorgaben gemacht, wie mit eingehenden Nutzeranfragen umzugehen ist. Insbesondere dem alleinigen Einsatz automatisierter Antwort-E-Mails erteilten die Richter eine Absage.

I. Hintergrund

Das Thema Impressumspflichten hat sich in letzter Zeit zu einem wahren Dauerbrenner in der – zumeist instanzgerichtlichen – Rechtsprechung entwickelt. Unter welchen Umständen und in welcher Form ein Impressum vorzuhalten ist, war bereits Gegenstand zahlreicher Beiträge im DFN-Infobrief Recht (siehe zum Beispiel Overbeck, „Ich bin dann mal weg und mein Name bitte auch!" in DFN-Infobrief Recht 7/2013) und soll deshalb hier nicht mehr im Detail erörtert werden. Festzuhalten ist, dass gemäß § 5 Telemediengesetz (TMG) jeder Anbieter von geschäftsmäßigen, in der Regel gegen Entgelt angebotenen Telemedien bestimmte Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar bereithalten muss. Als Telemedium sieht das TMG jeden elektronischen Informations- und Kommunikationsdienst an, sofern dieser nicht als Telekommunikationsdienst oder Rundfunk zu qualifizieren ist. Hierunter fallen quasi alle Online-Auftritte, also insbesondere Webseiten im Internet, auf denen Informationen oder sonstige Inhalte bereitgehalten werden. Betreibt eine Hochschule ein Informationsangebot im Internet, wie z. B. die Hochschulwebseite, unterliegt sie dafür somit der Impressumspflicht des § 5 TMG. Dies ist auch nicht aufgrund des Erfordernisses eines geschäftsmäßigen, in der Regel gegen Entgelt angebotenen Telemediums anders zu beurteilen. Über dieses Kriterium sollen nämlich primär rein privat angebotene Telemedien, die jeglichen Bezug zum Wirtschaftsleben vermissen lassen, von der Impressumspflicht ausgenommen werden. Zu den vorzuhaltenden Pflichtangaben gehören gem. § 5 Abs. 1 Nr. 2 TMG Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit dem Diensteanbieter ermöglichen, einschließlich der Adresse der elektronischen Post. Trotz der auf den ersten Blick noch relativ klaren Anforderungen dieser Norm, steckt der Teufel einmal mehr im Detail. Insofern hatten bereits einige Gerichte darüber zu entscheiden, inwiefern Telefon- und Telefaxnummern oder Online-Kontaktformulare ausreichend oder sogar erforderlich sind.

II. Die Entscheidungen der Gerichte

In zwei aktuellen landgerichtlichen Verfahren ging es nun insbesondere um die Frage, inwiefern automatisierte E-Mails als Antwort auf Nachrichten, die an die im Impressum angegebene E-Mail-Adresse des Diensteanbieters geschickt werden, als unmittelbare Kommunikation angesehen werden können.

1. Urteil des LG Koblenz

Im Fall, der dem LG Koblenz zur Entscheidung vorlag, hatte der Bundesverband der Verbraucherzentralen und Verbraucherverbände das Vorgehen des Anbieters des Online-Dienstes WEB.DE beanstandet, weil dieser auf Test-Kontaktmails an die im Impressum angegebene E-Mail-Adresse „info@web.de“ nur mit einer automatisierten Antwort-E-Mail reagierte, die folgenden Inhalt aufwies:

„Bitte wenden Sie sich mit Ihrem Anliegen erneut an den zuständigen Ansprechpartner.“ Es folgte danach eine Auflistung diverser Links und am Ende hieß es: „Wir freuen uns, wenn wir Ihnen weiterhelfen konnten und wünschen Ihnen weiterhin gute Kommunikation mit WEB.DE… Diese E-Mail wurde durch ein automatisiertes System erzeugt. Individuelle Anfragen zu Diensten und Produkten von WEB.DE können über diese E-Mail-Adresse nicht bearbeitet werden.“

In Übereinstimmung mit dem klägerischen Begehren entschied das LG Koblenz, dass eine solche Antwort den Forderungen des § 5 Abs. 1 Nr. 2 TMG nach einer direkten Kommunikation per E-Mail nicht gerecht wird und der Telemedienanbieter keine automatisierten Antworten verschicken darf, in denen bloß allgemeine Hinweise auf weitere Informationsquellen auf der Webseite oder auf telefonische Kontaktmöglichkeiten enthalten sind. Zur Begründung führte das Gericht aus, dass unter Kommunikation der Austausch von aufeinander bezogenen Informationen zu verstehen sei. Dies sei bei der verwendeten automatisierten Antwort-E-Mail weder tatsächlich der Fall noch vom Diensteanbieter intendiert. Stattdessen werde dem Verbraucher unmissverständlich klar gemacht, dass eine individuelle Beantwortung der Anfrage nicht erfolge und dass die als Eingangsbestätigung verschickte E-Mail abschließend sei. Dies zeige sich insbesondere an den ebenfalls enthaltenen Sätzen „Wir freuen uns, wenn wir Ihnen weiterhelfen konnten.“ und „Gerne informieren wir Sie über die nächsten Schritte“. Dazu komme schließlich noch, dass ausweislich des E-Mail-Textes individuelle Anfragen über diese E-Mail-Adresse gerade nicht bearbeitet werden könnten. Weil somit bereits das Vorliegen einer Kommunikation im Sinne einer individuellen Antwort auf die Anfragen der Verbraucher verneint wurde und die angegebene vermeintliche Kommunikationsmöglichkeit nicht den Anforderungen des § 5 Abs. 1 Nr. 2 TMG entsprach, gab das LG Koblenz dem Begehren der Klägerin statt, den Diensteanbieter zur Unterlassung der Angabe einer solchen zur Einleitung eines Kommunikationsprozesses ungeeigneten E-Mail-Adresse zu verpflichten.

2. LG Berlin

Auch das Verfahren vor dem LG Berlin ging auf eine Klage des Bundesverbandes der Verbraucherzentralen und Verbraucherverbände zurück und befasste sich mit der Kommunikationsmöglichkeit über die im Impressum angegebene E-Mail-Adresse. Beklagte war der bekannte Suchmaschinenanbieter Google Inc. Google hielt auf seiner Internetseite google.de im Impressum als Kontaktmöglichkeit die E-Mail-Adresse „support-de@google.com“ vor. Versuchte man, darüber Kontakt zu Google aufzunehmen, erhielt man nur eine automatisierte Antwort-E-Mail, in der darauf hingewiesen wurde, dass Anfragen, die an diese Adresse geschickt werden, nicht gelesen und zur Kenntnis genommen werden können. Stattdessen wurde anschließend unter Angabe eines Links auf Online-Kontaktformulare in der Google Hilfe verwiesen, sowie zahlreiche Links zu speziellen Support-Seiten für einzelne Google Produkte angegeben.
Ähnlich wie das LG Koblenz sah auch das LG Berlin eine solche automatisierte allgemeine Antwort-E-Mail und das Fehlen der Möglichkeit, eine individuelle Kommunikation mit einem Google-Mitarbeiter über die angegebene E-Mail-Adresse aufzunehmen, als nicht ausreichend an, um den Anforderungen an eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation im Sinne des § 5 Abs. 1 Nr. 2 TMG zu genügen.

Erforderlich sei die Angabe einer funktionierenden E-Mail-Adresse, die gewährleiste, dass der Inhalt eingehender E-Mails vom Adressaten zur Kenntnis genommen werde. Zulässig sei dabei auch die Angabe mehrerer E-Mail-Adressen im Impressum, beispielsweise um unterschiedliche Geschäftsfelder mit je einer eigenen Kontaktadresse abzudecken. Unverzichtbar sei aber, dass es sich dabei tatsächlich um E-Mail-Adressen und nicht bloß um Online-Kontaktformulare handle.

Eine Verpflichtung der Anbieter, Anfragen oder Beschwerden von Verbrauchern in einer bestimmten Weise zu behandeln, könne dem Gesetz allerdings nicht entnommen werden. Auch erzwinge das TMG nicht unbedingt eine Antwort oder gar eine bestimmte Qualität der Antwort. Insofern genüge schon die abstrakte Möglichkeit, dass Kommunikation aufgenommen

werde und eine Reaktion erfolge, wobei sogar ein Nichtantworten eine Reaktion sein könne. Von Kommunikation könne aber dann nicht mehr gesprochen werden, wenn das Nichtantworten Prinzip sei. So lag es jedoch bei den von Google versendeten Antwort-E-Mails, die besagten, dass die eingehenden E-Mails nicht zur Kenntnis genommen würden und dass auf diese E-Mail nicht geantwortet werden könne. Ebenfalls unzureichend sei die Weitervermittlung an andere Kanäle mittels der automatisierten Antwort-E-Mail. Die Richter beanstandeten dabei nicht die Verwendung vorformulierter Textbausteine im Rahmen der Antwort-E-Mail, sondern die Tatsache, dass Kommunikation über E-Mail gänzlich verweigert wurde und erst über die auszufüllenden Online-Kontaktformulare die Chance auf einen direkten Austausch mit einem Mitarbeiter gewährt wurde. Hierdurch werde dem Gericht zufolge keine Pflicht für Google aufgestellt, jede einzelne E-Mail von einem Mitarbeiter individuell prüfen und bearbeiten zu lassen. Es dürfe lediglich nicht von Anfang an feststehen, dass keine einzige über die angegebene Adresse eingehende E-Mail gelesen werde, weil dann keinesfalls von Kommunikation die Rede sein könne. Wie die eingehenden E-Mails letztlich gefiltert und kanalisiert würden, bleibe Googles Entscheidung vorbehalten. Auch erfordere Kommunikation keine individuell reflektierte Antwort, sondern könne im Einzelfall über vorformulierte Standardschreiben erfolgen, eine Kontaktaufnahme müsse aber auf dem angegebenen Weg per E-Mail und nicht bloß auf irgendeinem anderen Wege möglich sein.

III. Fazit und Konsequenzen für die Hochschulpraxis

Da auch Hochschulen der Impressumspflicht des § 5 TMG unterliegen, lassen sich aus den beiden Urteilen wertvolle Schlüsse über die Ausgestaltung der Kommunikationsmöglichkeiten mittels der im jeweiligen Impressum angegebenen E-Mail-Adresse ziehen. Von der schlichten Zusendung automatisierter Antwort-E-Mails sollte unbedingt Abstand genommen werden, insbesondere wenn darin nur Hinweise darauf enthalten sind, dass E-Mails an die betreffende E-Mail-Adresse nicht zur Kenntnis genommen werden und man sich über andere Wege an den Diensteanbieter wenden soll. Sofern die Anzahl der über die angegebene Kontaktadresse eingehenden E-Mails es zulässt, sollte bestenfalls jede E-Mail tatsächlich auch von einem zuständigen Hochschulmitarbeiter gelesen und beantwortet werden. Sollte dies nicht möglich sein, muss zumindest gewährleistet sein, dass die abstrakte Möglichkeit besteht, darüber Kontakt zu einem Mitarbeiter zu erhalten, der sich um das Anliegen des Nutzers kümmert. Der Verwendung vorformulierter Textbausteine zur Arbeitserleichterung steht dabei nichts im Wege, sodass nicht jede Nutzeranfrage mit einem individuellen Schreiben beantwortet werden muss. Auch das zusätzliche Angebot eines Kontaktformulars oder ein zusätzlicher Verweis auf Hilfe-Seiten kann durchaus empfehlenswert sein, um Nutzeranfragen schon von vornherein leichter zu kanalisieren bzw. um häufig von Nutzern gesuchte Informationen leicht zugänglich zu machen. Wichtig ist dabei allerdings, dass solche Angebote nur neben die Kommunikationsmöglichkeit über die angegebene E-Mail-Adresse treten dürfen und nicht als kompletter Ersatz für die E-Mail-Kommunikation vorgesehen werden.

Gefällt mir?!

Oberverwaltungsgericht Schleswig zum Betrieb von Facebook-Fanpages

von Philipp Roos

Das soziale Netzwerk Facebook ist vielen Datenschützern ein Dorn im Auge. Dies beruht darauf, dass im Rahmen der Nutzung von Facebook eine erhebliche Anzahl datenschutzrelevanter Vorgänge festzustellen ist. Dabei geht es immer wieder um die Frage, ob Facebook datenschutzkonform handelt bzw. überhaupt dem deutschen Datenschutzrecht unterfällt. Lediglich in Irland wird ein Firmensitz unterhalten. Allerdings nutzen auch unstreitig nationalem Datenschutzrecht unterliegende Unternehmen die Dienste von Facebook, indem sie sog. Fanpages auf Facebook betreiben. Vor dem Oberverwaltungsgericht Schleswig (OVG Schleswig) ging es nun um die Frage, ob die Betreiber derartiger Facebook-Fanpages datenschutzrechtliche Verantwortung tragen.

I. Hintergrund

Wer sich sozialen Netzwerken verwehrt, gilt als wenig „hip" und „out". Weiterhin verpassen Unternehmen die vielen wirtschaftlichen Chancen, die eine Betätigung in derartigen Netzwerken bietet. Insofern kann es für jedes Unternehmen ratsam sein, eine Facebook-Fanpage zu betreiben. Fanpages sind spezielle Benutzeraccounts, die bei Facebook eingerichtet werden können, um eigene Inhalte zu präsentieren. Facebook bietet den Betreibern von Fanpages zusätzlich die kostenfreie Möglichkeit, anonymisierte Benutzerstatistiken zu erhalten, bei denen es sich um eine Art Reichweitenanalyse handelt.

Solche Fanpages können von den Nutzern des Netzwerkes mit dem berühmten Facebook-Daumen – also einem „Gefällt mir" – markiert werden. Sodann werden die Nutzer über sämtliche Aktivitäten, die das Unternehmen in dem Netzwerk der Öffentlichkeit zur Schau stellt, auf ihrer Facebook-Startseite informiert. Dies schafft eine enorme Bindung. Aber auch die an einem Unternehmen Interessierten rufen mittlerweile häufig zunächst die Facebook-Fanpage auf, um sich zu informieren, bevor sie die eigene Webseite des Unternehmens besuchen. Gemeinnützige Einrichtungen, Künstler und Prominente nutzen daher ebenfalls die Möglichkeit, sich auf Facebook mittels Fanpages zu präsentieren.
Diese Erkenntnisse haben sich mittlerweile bis in die Öffentlichkeitsabteilungen der Hochschulen herumgesprochen. Daher betreiben auch viele Hochschulen solche Fanpages, um interessierte Studierende und die sonstige Öffentlichkeit auf die eigenen Angebote aufmerksam zu machen.

Zugleich ergibt sich im Rahmen der Nutzung von Facebook aber eine Vielzahl bislang ungeklärter rechtlicher Fragestellungen, die insbesondere dem Datenschutzrecht entspringen. Viele Datenschützer kritisieren Facebook und behaupten, dass das Unternehmen das deutsche bzw. europäische Datenschutzrecht umgehe und datenschutzwidrige Nutzerprofile anlege, um nur einige der Streitpunkte zu benennen.

Eine besondere Rolle im Kampf der Datenschützer gegen Facebook kommt dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) zu, dessen Leiter zugleich der Landesbeauftragte für Datenschutz in Schleswig-Holstein ist. Das ULD ist bekennender Gegner von Facebook und betrieb mehrere Verfahren, die mit der Datenschutzkonformität von Facebook in Verbindung stehen. So ging das ULD auch gegen Facebook-Fanpages vor: Dabei war Facebook allerdings nicht direkter Klagegegner. Vielmehr verbot das ULD schleswig-holsteinischen Unternehmen den Betrieb der Fanpages, was diese im Gegenzug dazu aufrief, rechtliche Schritte gegen das Verbot einzuleiten.

II. Die Entscheidung des Gerichts

Das OVG Schleswig hält an der Rechtsauffassung des Verwaltungsgerichts (VG) Schleswig (s. dazu bereits Hinrichsen, „Quo vadis Datenschutz? – Keine Regulierung in Sicht!“, DFN-Infobrief Recht 1/2014) fest. Dies bedeutet, dass der Betreiber einer Facebook-Fanpage datenschutzrechtlich keine Verantwortung trägt und durch den Betrieb der Fanpage auch keinen Datenschutzverstoß begeht. Damit ist eine entsprechende Verbotsverfügung von datenschutzrechtlichen Aufsichtsbehörden rechtswidrig.

1. Sachverhalt

In dem konkreten Fall ging es um die Rechtmäßigkeit einer datenschutzrechtlichen Anordnung des ULD gegenüber einem Bildungsunternehmen, das u.a. für die Industrie- und Handelskammern des Landes Schleswig-Holstein tätig ist. Dieses Bildungsunternehmen unterhielt eine Facebook-Fanpage.

Das ULD ordnete in der Anordnung die Deaktivierung der Fanpage an. Im Wesentlichen stützte die Behörde ihre Rechtansicht darauf, dass die mit dem Aufruf der Fanpage entstehenden Nutzungsdaten für Werbezwecke erhoben würden, ohne dass das Bildungsunternehmen den Nutzern eine Möglichkeit zum Widerspruch gegeben hätte. Die Pflicht zur Einräumung einer solchen Widerspruchsmöglichkeit bestimmt § 15 Abs. 3 S. 1 Telemediengesetz (TMG). Die entsprechende Verpflichtung setzt allerdings eine datenschutzrechtlich verantwortliche Stelle im Sinne des § 12 Abs. 2 TMG i.V.m. § 3 Abs. 7 Bundesdatenschutzgesetz (BDSG) voraus. Das ULD trug weiterhin vor, Facebook lege pseudonyme Nutzerprofile an, was gegen § 15 Abs. 3 Satz 3 TMG verstoße: Dieser verbiete es, Nutzungsprofile mit Daten über die Träger des Pseudonyms zusammenzufassen.

Das Bildungsunternehmen legte Widerspruch gegen den Bescheid ein. Es bestritt, verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG zu sein. Auch handele es sich um keine Auftragsdatenverarbeitung durch Facebook, da kein Vertrag über die Erbringung einer Reichweitenanalyse bestehe.

2. Urteil

Das OVG Schleswig sprach dem Bildungsunternehmen auf ganzer Linie Recht zu und bewertete die Anordnung als rechtswidrig.

Verfahrensrechtliche Fehler

Zunächst bemängelte das OVG bereits das verfahrensrechtliche Vorgehen des ULD. Dieses hatte seine Anordnung zur Deaktivierung auf § 38 Abs. 5 BDSG gestützt. Diese Norm verlangt von der Datenschutzaufsichtsbehörde allerdings die Einhaltung eines sog. „abgestuften Verfahrens“. Hinter diesem juristischen Begriff verbirgt sich das Prinzip, dass die Behörde dem Adressat der Anordnung zunächst die Möglichkeit zur Beseitigung geben muss: Eine sofortige Untersagung des Datenverarbeitungsvorgangs – wie es das ULD angeordnet hatte – ist dagegen regelmäßig unwirksam, was selbst bei erheblichen Mängeln gilt. Zunächst muss die Möglichkeit zur Beseitigung gegeben werden. Zwar existieren auch anerkannte Ausnahmen von diesem Grundsatz, aber eine solche, so das OVG Schleswig, sei in dem vorliegenden Verfahren nicht ersichtlich.

Fanpage-Betreiber keine verantwortliche Stelle im Sinne des Datenschutzrechts

Ganz wesentlich ist die Bewertung des OVG Schleswig, dass es sich bei dem Betreiber einer Facebook-Fanpage um keine verantwortliche Stelle hinsichtlich der von Facebook erhobenen Daten handelt. Eine Verantwortlichkeit leite sich weder aus § 3 Abs. 7 BDSG noch aus Art. 2 lit. d der Datenschutzrichtlinie (RL 95/46/EG) ab. Die datenschutzrechtliche Anordnung könne sich allerdings nur gegen die verantwortliche Stelle richten.

Vielmehr sei der Betreiber einer Facebook-Fanpage ausschließlich ein Diensteanbieter im Sinne des TMG (§ 2 Nr. 1 TMG). Solche Diensteanbieter müssten jedoch nach den §§ 11 ff. TMG nur die eigene Erhebung und Verwendung von Daten verantworten. Eine entsprechende eigene Erhebung und Verarbeitung personenbezogener Daten der Fanpage-Besucher konnte das OVG aber nicht feststellen.

Auch eine Datenübermittlung durch den Fanpage-Betreiber finde nicht statt. Eine Übermittlung im Sinne des § 3 Abs. 4 Satz 2 Nr. 3 BDSG verlange die Bekanntgabe personen-

bezogener Daten an einen Dritten. Facebook sei jedoch nach diesem Verständnis kein Dritter, da die Fanpage eine originäre Facebook-Seite darstelle. Nicht der Betreiber der Fanpages erhalte Daten wie die IP-Adresse des Nutzers und hinterlege Cookies, sondern nur Facebook selbst. Auch die Datenschutzrichtlinie veranlasse keine entgegengesetzte Bewertung.
Das OVG Schleswig behandelt weiterhin die Frage, ob der Fanpage-Betreiber – wenn schon nicht allein verantwortlich – zumindest eine von mehreren für die Datenverarbeitung verantwortlichen Stellen darstellt/ist. Im Ergebnis verneint das Gericht jedoch auch dies. Über die dafür erforderliche Einflussnahmemöglichkeit verfüge der Fanpage-Betreiber nicht. Zwar sei die Einrichtung der Fanpage unerlässliche Voraussetzung der Datenerhebung, jedoch obliege die Entscheidung über „ob", „warum" und „wie" der Datenverarbeitung Facebook allein.

Daraufhin untersucht das Gericht, ob das Bildungsunternehmen als datenverarbeitende Stelle behandelt werden kann, da es Daten durch andere – in diesem Fall Facebook – verarbeiten lässt (sog. Auftragsdatenverarbeitung). Allerdings, so das OVG, verlange eine Auftragsdatenverarbeitung einen schriftlichen Auftrag, der den Anforderungen des § 11 Abs. 2 Satz 2 BDSG gerecht wird. Ob mit der Anmeldung der Fanpage durch den Betreiber ein solcher Auftrag vorliegt, lässt das OVG trotz der mangelnden Schriftlichkeit letztlich dahinstehen. Entscheidend sei vielmehr, dass der Vertrag in der Praxis auch gelebt werde: Entscheide der Auftragnehmer (= Facebook) allerdings in eigener Verantwortung und ohne Kontrolle des Auftraggebers (= Fanpage-Betreiber) über die Datenverarbeitung, handele es sich bei dem Auftragnehmer um die verantwortliche Stelle. Insofern bestehe wegen des fehlenden Einflusses auch keine Auftragsdatenverarbeitung.

Keine Anordnung aufgrund von Datenschutzverstößen gegen Dritte

Zuletzt erarbeitete das OVG, dass die Ermächtigungsnorm des § 38 Abs. 5 BDSG keine Anordnungen gegenüber Dritten erlaubt. § 38 Abs. 5 Satz 1 und 2 BDSG besagt:
„Zur Gewährleistung der Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz kann die Aufsichtsbehörde Maßnahmen zur Beseitigung festgestellter Verstöße (...) oder technischer oder organisatorischer Mängel anordnen. Bei schwerwiegenden Verstößen oder Mängeln (...) kann sie die Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren untersagen, wenn die Verstöße oder Mängel entgegen der Anordnungen nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden."
Hieraus leitet sich ab, dass immer nur die tatsächlich verantwortliche Stelle als Adressat einer datenschutzrechtlichen Anordnung in Betracht kommt. Als sog. „Eingriffsnorm" müsse § 38 Abs. 5 BDSG den rechtsstaatlichen Geboten von Bestimmtheit und Klarheit genügen. Da § 38 Abs. 5 BDSG jedoch immer nur auf die Datenverarbeitung als solche abstelle, bestünden keine Zweifel daran, dass nur die verantwortliche Stelle Adressat sein könne.

Auch eine Störerhaftung sei der Norm nicht zu entnehmen. Nach den Vorschriften des Telemediengesetzes (§§ 8 ff. TMG) können rechtliche Schritte unter gewissen Umständen auch gegen denjenigen, der eine rechtswidrige Handlung erst ermöglicht (Access-, Host- oder Contentprovider), eingeleitet werden. Zwar nimmt der Fanpage-Betreiber den obigen Erwägungen folgend eine solche Mittlerrolle in Bezug auf die Datenverarbeitung ein. Allerdings sei § 38 Abs. 5 BDSG eine Störerhaftung nicht zu entnehmen.

III. Fazit und Konsequenzen für die Hochschulpraxis

Das OVG Schleswig stellt mit seiner Entscheidung klar, dass nur die für die Datenverarbeitung verantwortliche Stelle als Adressat von Anordnungen der Datenschutzbehörde in Betracht kommt. Insofern kommt der Klärung darüber, wer „verantwortliche Stelle" im Sinne des Datenschutzrechts ist, gerade in diesem Kontext eine überragende Bedeutung zu.

In verfahrensrechtlicher Hinsicht ist weiterhin herauszustellen, dass die Aufsichtsbehörde bei Anordnungen wegen datenschutzrechtlicher Verstöße das abgestufte Verfahren berücksichtigen muss. Somit ist es unabhängig von der Schwere des Verstoßes unerlässlich, dass die Aufsichtsbehörde zunächst die Beseitigung des festgestellten Verstoßes anordnet. Erst wenn der Adressat dieser Beseitigungsanordnung nicht folgt, kann die Datenverarbeitung gänzlich untersagt werden. Zwar gibt es anerkannte Ausnahmen hiervon, dies ist aber im Einzelfall zu prüfen.

Interessant sind auch die Ausführungen des Gerichts zu den Aspekten der Auftragsdatenverarbeitung: Nur wenn der Vertrag über die Auftragsdatenverarbeitung (§ 11 BDSG)

tatsächlich „gelebt“ werde, wie es das OVG formuliert, könne auch eine Auftragsdatenverarbeitung angenommen werden. Wenn die datenverarbeitende Stelle allerdings unabhängig von Weisungs- und Einflussnahmemöglichkeiten eines Dritten agiert, kommt nur sie (im vorliegenden Fall Facebook) als „verantwortliche Stelle“ in Betracht.
Unabhängig von diesen spannenden rechtlichen Erwägungen kommt der Entscheidung auch eine hohe praktische Relevanz zu: Nach derzeitiger Rechtslage ist davon auszugehen, dass der Betrieb einer Facebook-Fanpage für den Betreiber unter datenschutzrechtlichen Gesichtspunkten unbedenklich ist. Diese Nachricht dürfte für ein tiefes Durchatmen in der Öffentlichkeitsabteilung und im Justiziariat jeder Hochschule sorgen, sofern Facebook-Fanpages betrieben werden. Für die Datenverarbeitung rechtlich verantwortlich ist ausschließlich Facebook selbst. Denkbare Anordnungen der Aufsichtsbehörden gegen universitäre Einrichtungen sind somit rechtlich angreifbar.

Ist die Hochschule als Fanpage-Betreiber aktiv, müssen jedoch auch die sonstigen rechtlichen Anforderungen eingehalten werden – insbesondere gilt in sozialen Netzwerken die Impressumspflicht. Die erforderlichen Informationspflichten können § 5 TMG entnommen werden. Um auf der rechtlich sicheren Seite zu stehen, sollte ferner § 55 Abs. 1 Rundfunkstaatsvertrag berücksichtigt werden.

Der Kampf des ULD gegen den Betrieb von Facebook-Fanpages ist mit der Entscheidung des OVG Schleswig freilich noch nicht beendet. So hat das OVG wegen der grundsätzlichen Bedeutung der Entscheidung die Revision zugelassen. Von dieser Möglichkeit machte das ULD auch Gebrauch: Es gibt sich nicht geschlagen und verspricht sich nicht weniger als eine rechtliche Neubewertung der aufgeworfenen Fragen – Fanpage-Betreiber und Facebook würden sich gegenseitig ergänzen und voneinander abhängen. Die nächste Runde in der Auseinandersetzung ist damit bereits eingeläutet und wird in absehbarer Zeit vor dem Bundesverwaltungsgericht ausgefochten werden.

Ausnahmen bestätigen die Regel!

LG Neuruppin verneint Abmahnfähigkeit eines fehlerhaften Impressums

von Alice Overbeck

Die Urteile zur Impressumspflicht auf Webseiten nehmen kein Ende. Das Landgericht (LG) Neuruppin (Beschluss vom 9.12.2014, Az.: 5 O 199/14) verneinte jüngst einen Wettbewerbsverstoß durch ein fehlerhaftes Impressum und wich damit von der ständigen Rechtsprechung zu Verstößen gegen die Impressumspflicht ab. Es handelt sich jedoch um eine Einzelfallentscheidung, die keine Abkehr von der bisherigen Rechtsprechung bedeutet. In dem Verfahren lagen zwei nichtwirtschaftliche Vereine im Streit, deren ideelle Zielsetzung die Richter bewog, ausnahmsweise eine Spürbarkeit des Wettbewerbsverstoßes und damit den Unterlassungsanspruch abzulehnen. Dass diese Ausnahme lediglich die Regel bestätigt, belegt ein weiteres aktuelles Urteil des LG Essen (Urteil vom 13.11.2014, Az.: 4 O 97/14), in dem das Gericht die Geltung der Impressumspflicht auch für vom Betreiber längst vergessene und inhaltlich veraltete Webseiten bekräftigte. Das Gericht bejahte den dadurch verwirklichten Wettbewerbsverstoß.

I. Abmahnfähigkeit von Verstößen gegen die Impressumspflicht

Das Internet ist das zentrale Informationsmedium unserer Zeit. Hochschulen und Wissenschaftseinrichtungen nutzen Webseiten, um ihre Lehre und Forschung vorzustellen und Projektpartner, Wissenschaftler und Studierende anzuwerben. Mit dem Betrieb von Webseiten geht eine Reihe von Informationspflichten einher, die wohl bekannteste ist dabei die Pflicht zur Angabe eines Impressums. Die Impressumspflicht für Webseiten ergibt sich aus § 5 Abs. 1 Telemediengesetz (TMG). Für journalistisch-redaktionelle Angebote muss gemäß § 55 Abs. 2 Rundfunkstaatsvertrag (RStV) zusätzlich zu den im TMG genannten Angaben ein Verantwortlicher im Sinne des Presserechts mit Name und Anschrift benannt werden. Schutzzweck der Impressumspflicht ist die Ermöglichung von Rechtsverfolgung. Der Konsument eines Angebots, der sich durch dessen Inhalte in seinen Rechten verletzt sieht, soll alle für eine Rechtsverfolgung nötigen Informationen leicht finden können. Daher findet sich im Gesetz auch die Vorgabe, dass das Impressum auf einer Webseite leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten ist. Am rechtssichersten können diese Vorgaben durchgesetzt werden, wenn ein Link zum Impressum auf Webseiten im Frame platziert und als „Impressum“ benannt wird. So ist die Erreichbarkeit von jeder Unterseite mittels eines Klicks gewährleistet. Die Rechtsprechung ist großzügiger und lässt eine Erreichbarkeit des Impressums mittels zwei Klicks ausreichen, allerdings ist vorheriges langes Scrollen unzulässig. Technisch ist eine ständige, das heißt 24-stündige Erreichbarkeit des Impressums gefordert. Inhaltlich muss das Impressum die in § 5 Abs. 1 TMG bzw. § 55 Abs. 2 RStV geforderten Angaben enthalten (siehe hierzu: Overbeck, „Ich bin dann mal weg und mein Name bitte auch!“, DFN-Infobrief Recht 07/2013, S. 2).

Verstöße gegen die Impressumspflicht durch nicht vorhandene Impressen oder aufgrund fehlender oder falscher Angaben sind grundsätzlich als Wettbewerbsverstoß nach dem Gesetz gegen den unlauteren Wettbewerb (UWG) abmahnfähig. Das TMG selbst enthält keine entsprechenden Abwehransprüche. Nach dem UWG kann jedoch nicht jeder beliebige Nutzer einer Webseite bei Verstößen gegen die Impressumspflicht gegen den Betreiber vorgehen. Berechtigt zur Geltendmachung von Unterlassungs- und Beseitigungsansprüchen, mithin zur Abmahnung, sind nur Mitbewerber, Unternehmerverbände, Industrie- und Handelskammern sowie qualifizierte Einrich-

tungen im Sinne des § 4 Unterlassungsklagengesetzes (UKlaG) und des Art. 4 der europäischen Richtlinie 98/27/EG über Unterlassungsklagen zum Schutz der Verbraucherinteressen. Die wohl bekanntesten Einrichtungen dieser Art sind die Verbraucherzentralen der 16 Bundesländer. Wenn die Berechtigung zur Rechtsverfolgung, die sogenannte Aktivlegitimation, gegeben ist, müssen die inhaltlichen Voraussetzungen des Unterlassungs- oder Beseitigungsanspruchs vorliegen. Erforderlich ist ein unlauteres Handeln, das geeignet ist, die Interessen von Mitbewerbern, Verbrauchern oder sonstigen Marktteilnehmern spürbar zu beeinträchtigen. Unlauteres Handeln liegt gemäß § 4 Nr. 11 UWG bereits dann vor, wenn gegen eine gesetzliche Vorschrift verstoßen wird, die im Interesse der Marktteilnehmer das Marktverhalten regelt. § 5 Abs. 1 TMG, der die Impressumspflicht vorschreibt, ist eine solche Markverhaltensregel. Denn die Norm sieht im Interesse der Verbraucher bestimmte Betreiberangaben vor. Verstöße gegen die Impressumspflicht begründen daher grundsätzlich Unterlassungs- und Beseitigungsansprüche. Die Normenkette für diese Ansprüche lautet: § 5 Abs. 1 TMG in Verbindung mit §§ 3, 8 Abs. 1, Abs. 3, 4 Nr. 11 UWG. Wenn Juristen das Wort „grundsätzlich“ benutzen, bedeutet das allerdings immer auch, dass es Ausnahmen gibt.

II. Die Ausnahme – dazu die Entscheidung des Landgerichts Neuruppin

Eine solche Ausnahme bejahte kürzlich das LG Neuruppin in einem Beschluss (LG Neuruppin, Beschluss vom 9.12.2014, Az.: 5 O 199/14).

Sachverhalt

Der Antragssteller, ein eingetragener gemeinnütziger Verein, nahm den Antragsgegner, ebenfalls ein eingetragener gemeinnütziger Verein, auf Unterlassung in Anspruch. Beide Vereine betrieben eine „Paintballanlage“ und jeweils eine Webseite, auf der sie das Angebot der Anlage vorstellten. Bereits vor Einleitung des gerichtlichen Verfahrens hatte der spätere Antragssteller den Antragsgegner abgemahnt und dazu aufgefordert, seine Webseite um ein Impressum zu ergänzen. Dem kam der Antragsgegner nach, indem er ein Impressum einfügte. Allerdings unterblieb die nach § 5 Abs. 1 Nr. 4 TMG verpflichtende Angabe zum Vereinsregister und der dazugehörigen Registernummer. Auch die ihm Abmahnschreiben geforderte strafbewehrte Unterlassungserklärung unterzeichnete der Antragsgegner nicht. Der Antragssteller verfolgte sein Unterlassungsbegehren aufgrund des Verstoßes gegen die Impressumspflicht daraufhin gerichtlich.

Beschluss

Das Gericht lehnte den Antrag ab. Dem Antragssteller stehe der Unterlassungsanspruch gemäß § 5 Abs. 1 Nr. 4 TMG in Verbindung mit §§ 3, 8 Abs. 1, Abs. 3 Nr. 1, 4 Nr. 11 UWG nicht zu. Zwar sei der Antragssteller als Mitbewerber aktivlegitimiert, den Anspruch geltend zu machen, da es sich bei beiden Parteien um Betreiber einer „Paintballanlage“ handle. Allerdings seien die materiellen, also die inhaltlichen, Voraussetzungen des Anspruchs nicht gegeben. Durch die fehlende Angabe von Vereinsregister und Registernummer werde gegen die Impressumspflicht gemäß § 5 Abs. 1 TMG verstoßen. Da es sich bei der Impressumspflicht um eine Marktverhaltensvorschrift handle, sei hierdurch auch ein Rechtsbruch im Sinne des § 4 Nr. 11 UWG begründet worden. Der Anspruch scheitere jedoch an anderer Stelle, nämlich an der Bagatellgrenze des § 3 Abs. 1 UWG. Danach muss die unlautere Handlung – hier der Verstoß gegen die Impressumspflicht – auch geeignet sein, die Interessen des Mitbewerbers „spürbar“ zu beeinträchtigen. Die Überschreitung dieser Spürbarkeitsschwelle lehnte das Gericht ab. Maßgeblich für die Ahndung eines Wettbewerbsverstoßes sei seine Eignung, die Fähigkeit des Verbrauchers zu beeinflussen, sich aufgrund von Informationen für einen Marktteilnehmer zu entscheiden und ihn damit zu einer geschäftlichen Handlung zu veranlassen, die er andernfalls nicht getätigt hätte. Die auf der Webseite des Antragsgegners fehlenden Angaben seien nicht geeignet, das schützenswerte Interesse von Verbrauchern, sich aufgrund von Informationen für das Angebot eines Wettbewerbers zu entscheiden, spürbar zu beeinträchtigen. Denn es widerspreche der allgemeinen Lebenserfahrung, dass das Vereinsregister und die Registernummer für Verbraucher bei der Entscheidung zur Kontaktaufnahme mit einem (Sport-) Verein relevant seien.

Während das Oberlandesgericht (OLG) Hamm in einem Urteil vom 2.4.2009 (Az.: 4 U 213/08) die Angabe des Handelsregisters und der Registernummer im Impressum noch als spürbaren Wettbewerbsverstoß eingestuft habe, da diese Angaben zur Identifizierung des Anbieters und als Nachweis seiner Existenz dienten, sei dies im vorliegenden Fall anders zu beurteilen. Es handle sich im Streitfall um nicht-wirtschaftliche Vereine, die gerade nicht auf Gewinnerzielung im marktwirtschaft-

lichen Wettbewerb, sondern auf die Verfolgung ideeller Zwecke ausgerichtet seien. Dabei sei eine untergeordnete wirtschaftliche Funktion (Nebenzweckprivileg) zwar zulässig, Hauptzweck des sogenannten Idealvereins müsse aber die nicht-wirtschaftliche Tätigkeit sein. Dann geschehe die Eintragung in das Vereinsregister aber nicht aus wirtschaftsrechtlichen, insbesondere haftungsrechtlichen Gesichtspunkten, sondern um gemäß § 21 BGB die Rechtsfähigkeit des Vereines als juristische Person zu begründen. Zwischen der Haftung von eingetragenen und nicht-eingetragenen Vereinen bestehe ohnehin kein nennenswerter Unterschied. Die unterbliebene Angabe des Vereinsregisters und der Registernummer sei daher für durchschnittliche Verbraucher irrelevant. Die wettbewerbsrechtliche Spürbarkeitsschwelle sei durch diesen Rechtsbruch nicht überschritten. Das Gericht zweifle im Übrigen daran, dass der Antragssteller überhaupt einen rechtlich anerkennenswerten Grund habe, das streitgegenständliche Verhalten wettbewerbsrechtlich zu untersagen. Als nicht-wirtschaftliche Vereine stünden die Parteien lediglich sportlich oder nach Maßgabe ihrer weiteren Attraktivität auch in einem weiteren Sinne gesellschaftlich in einem Konkurrenzverhältnis. Für ein wettbewerbsrechtlich relevantes wirtschaftliches Konkurrenzverhältnis bestehe bei nicht-wirtschaftlichen Vereinen jedoch kein Raum.

III. Die Regel – dazu die Entscheidung des LG Essen

Demgegenüber hat das LG Essen jüngst einen Wettbewerbsverstoß wegen eines fehlerhaften Impressums auf einer Webseite angenommen (Urteil vom 13.11.2014, Az.: 4 O 97/14).

Sachverhalt

Sowohl die Klägerin als auch die beiden Beklagten vermieteten bzw. vermittelten Ferienwohnungen auf Borkum. Einer der Beklagten warb auf verschiedenen Portalen für die Vermietung einer Ferienwohnung. Zeitweise wurde die Ferienwohnung im März 2014 über eine Webseite beworben, die die andere Beklagte im Jahr 2007 errichtet und ins Internet eingestellt hatte. Sie war auch die Domaininhaberin. Im März 2014 waren die Inhalte der Webseite veraltet und unvollständig. Die Preisliste etwa hatte den Stand des Jahres 2010, Texte waren teilweise unvollendet oder überhaupt nicht ausgeführt. Außerdem waren die Bilder der Ferienwohnung teilweise verdreht eingestellt worden. Als Anbieter war auf der Webseite lediglich „Familie XY“ angegeben. Wegen mangelnder Impressumsangaben ließ die Klägerin die Beklagten mit Anwaltsschreiben vom 19.3.2014 abmahnen und forderte sie zur Abgabe einer strafbewehrten Unterlassungserklärung sowie Erstattung der Abmahnkosten auf. Die Beklagten lehnten dies mit dem Hinweis ab, dass der Anwalt keine Vollmachtsurkunde nach § 174 BGB vorgelegt habe. Zum Zeitpunkt des Gerichtsverfahrens existierte die Webseite nicht mehr. Die Beklagte hatte ab Mai 2014 die Löschung der Domain veranlasst. Auf dem Klageweg verfolgt die Klägerin ihr Unterlassungsbegehren weiter und fordert außerdem Abmahnkosten in Höhe von 382,70 Euro. Die zwischenzeitliche Abschaltung der Webseite stünde dem Unterlassungsbegehren nicht entgegen, da die Beklagten jederzeit eine neue Webseite mit mangelhaften Impressumsangaben, insbesondere ohne Angabe der Vor- und Nachnamen der Anbieter und ohne Angabe der jeweiligen Anschrift, online stellen könnten. Die Beklagten beantragten die Klage abzuweisen. Sie trugen vor, dass der Webseite wegen der zahlreichen Defizite bzw. Unverständigkeiten kein Werbeeffekt zugekommen sei. Der eine Beklagte sei ferner nicht passivlegitimiert, das heißt nicht der richtige Anspruchsgegner für den Unterlassungsanspruch, da die Webseite 2007 ohne sein Wissen ins Internet eingestellt worden sei. Im Übrigen habe die Beklagte die Webseite nur versehentlich online gestellt und diese danach vergessen. Die Beklagten meinten daher, dass die etwaige Verletzung der Impressumspflicht gemäß § 5 Abs. 1 TMG nicht die Spürbarkeitsschwelle des § 3 Abs. 1, 2 UWG überschreite.

Urteil

Dieser Argumentation der Beklagten folgte das LG Essen nicht. Es gab der Klage statt und verurteilte die Beklagten zur Unterlassung und zur Zahlung der Abmahnkosten in Höhe von 382,70 Euro. Die Aktivlegitimation der Klägerin als Mitbewerberin gemäß § 8 Abs. 3 Nr. 1 UWG sei gegeben, da es sich bei beiden Parteien um Vermieter bzw. Vermittler von Ferienwohnungen auf Borkum handle. Rechtlich unerheblich sei die Behauptung, dass der Webseite aufgrund der zahlreichen Defizite und Unvollständigkeiten überhaupt kein Werbeeffekt zukomme. Der Webauftritt eröffne zumindest die Möglichkeit, Kunden zu interessieren und zu einer Kontaktaufnahme zu bewegen. Ein Verstoß gegen die Impressumspflicht gemäß § 5 Abs. 1 TMG liege vor. Sinn und Zweck der Vorschrift sei es, Verbrauchern die Geltendmachung von Rechten zu ermöglichen. Diese Möglichkeit sei bei fehlender Angabe von Vor- und Nachnamen sowie einer ladungsfähigen Anschrift der Webseitenanbieter jedoch nicht gegeben. Da es sich um eine Marktverhaltensvorschrift

handle, sei auch ein Verstoß gegen § 4 Nr. 11 UWG zu bejahen. Für diesen Rechtsverstoß müsse die Beklagte als Domaininhaberin einstehen. Der Beklagte müsse ebenfalls einstehen, nicht als Domaininhaber, aber als Mitstörer. Er habe die auf der Webseite dargestellte Ferienwohnung mitvermietet und habe, spätestens seit der vorgerichtlichen Abmahnung, gewusst, dass für die Ferienwohnung auch in seinem Namen geworben wurde. Unerheblich sei ferner der Bagatelleinwand der Beklagten. Es sei irrelevant, dass die Beklagte die Webseite nur versehentlich online gestellt und danach vergessen habe. Die Spürbarkeitsschwelle diene dazu, solche Verletzungshandlungen aus dem Verbotsbereich auszuschließen, die sich auf das Marktgeschehen praktisch nicht auswirkten. Dies sei bei dem hier einschlägigen Verstoß aber nicht der Fall. Auch der Einwand mangelnden Verschuldens gehe ins Leere. Die wettbewerbsrechtliche Unterlassungspflicht setze kein Verschulden voraus. Der Berechnung der Abmahnkosten lag ein Streitwert von 10.000 Euro zugrunde, den das Gericht im Hinblick auf die Rechtsprechung anderer Gerichte in ähnlich gelagerten Fällen für angemessen und sogar für im unteren Bereich angesiedelt hielt. Die Abmahnung sei wirksam gewesen. Die fehlende Vorlage einer Vollmachtsurkunde durch den Anwalt stehe dem nicht entgegen. Die Vorschrift des § 174 BGB, die sich auf einseitige Rechtsgeschäfte bezieht, sei nicht anwendbar, wenn der Abmahnung ein Angebot zum Abschluss eines zweiseitigen Unterwerfungsvertrages beiliege.

IV. Fazit und Folgen für die Hochschulpraxis

Den vorgestellten Urteilen ist gemein, dass in beiden Fällen unstreitig ein Verstoß gegen die Impressumspflicht gemäß § 5 Abs. 1 TMG vorliegt. Beide Gerichte haben daher einen Rechtsverstoß im Sinne des § 4 Nr. 11 UWG bejaht. Die jeweiligen Anspruchsgegner traten dem wettbewerbsrechtlichen Unterlassungsanspruch mit dem Einwand entgegen, dass der Rechtsverstoß nicht die Spürbarkeitsschwelle des § 3 Abs. 1, 2 UWG überschreite, wonach eine unlautere Handlung geeignet sein muss, die Interessen von Mitbewerbern, Verbrauchern oder sonstigen Marktteilnehmern spürbar zu beeinträchtigen. Das Eingreifen dieser Bagatellgrenze bejahte jedoch nur das LG Neuruppin. Die Begründung lässt sich hören. Entscheidend ist nach Ansicht des Gerichts, dass die fehlenden Angaben im Impressum – das Vereinsregister und die Registernummer – sich auf die Möglichkeit der Rechtsverfolgung des Webseitenanbieters durch Verbraucher nicht auswirken. Denn nicht in das Vereinsregister eingetragene Vereine sind haftungsrechtlich eingetragenen Vereinen gleichgestellt. Für Verbraucher macht es also keinen Unterschied, ob sie rechtlich gegen einen eingetragenen oder einen nicht-eingetragenen Verein vorgehen. Die fehlenden Angaben des Vereinsregisters und der Registernummer waren daher nicht geeignet, das Marktgeschehen spürbar zu beeinträchtigen. Anders lag dies im Fall vor dem LG Essen. Hier fehlten im Impressum die Angaben von Vor- und Nachnamen der Anbieter und die ladungsfähigen Anschriften. Verbrauchern ist daher eine Rechtsverfolgung unmöglich. Der Sinn und Zweck des § 5 Abs. 1 TMG wird nicht erfüllt. Die Entscheidungen sind daher überzeugend. Es wird aber auch deutlich, dass in aller Regel ein relevanter Verstoß gegen die Impressumspflicht und damit auch die Abmahnfähigkeit vorliegen wird. An der Impressumspflicht für die Hochschulen ändert sich durch das Urteil des LG Neuruppin daher nichts. Wichtig ist, dass im Impressum die Person aufgeführt wird, die für die Hochschule Rechtsfähigkeit nach außen besitzt. Das ist jedenfalls die Hochschule selbst als juristische Person, vertreten durch die/den RektorIn. Insbesondere für die Webseiten von Instituten ist es daher nicht ausreichend, wenn im Impressum das Institut vertreten durch die/den InstitutsleiterIn genannt wird. Im Falle fehlerhafter Angaben liegt ein abmahnfähiger Verstoß gegen die Impressumspflicht vor. Faktisch wird es wohl nicht dazu kommen, dass Hochschulen sich gegenseitig aufgrund von Impressumsverstößen abmahnen. Es besteht jedoch die Möglichkeit, dass eine Abmahnung durch die Verbraucherschutzzentralen oder andere qualifizierte Einrichtungen erfolgt. Außerdem ist eine Einhaltung der Impressumspflicht im Sinne der Vorbildfunktion der Hochschulen ratsam.

Kommerziell oder nicht kommerziell, das ist hier die Frage…

OLG Köln revidiert Urteil der Vorinstanz zur Nutzung von CC-Lizenzen

von Marten Hinrichsen

Die Lizenzierung von urheberrechtlich geschützten Werken unter den Bedingungen der Creative Commons-Lizenzen stellt in der Praxis längst keine Seltenheit mehr dar. Immer mehr Urheber leisten somit einen Beitrag zum freien Zugang zu Kulturgütern und steigern durch die Verbreitung der Werke gleichzeitig ihre Bekanntheit. Dabei können sich jedoch mitunter erhebliche rechtliche Probleme bei der Anwendung des Lizenztextes ergeben. Wie ein aktueller Streitfall über die Reichweite des Verbots der kommerziellen Nutzung zeigt, stellt die Klärung dieser Fragen auch die Gerichte immer wieder vor Schwierigkeiten. So entschied nun das Oberlandesgericht (OLG) Köln entgegen der Vorinstanz, dass Unklarheiten bei der Verwendung des Lizenztextes wie beispielsweise bei der Bewertung, ob eine Tätigkeit als kommerzielle Nutzung anzusehen ist, zu Lasten der Verwender und somit der Urheber gehen. Trotz dieses neuen Urteils bleiben jedoch weiterhin Fragen offen, die auch für die Hochschulen als mögliche Nutzer dieser Lizenzverträge von nicht zu unterschätzender Bedeutung sind.

Übertragbarkeit von Urheberrechten

Der eigene Internetauftritt ist heutzutage das Aushängeschild und Informationsportal für Unternehmen und sonstige Organisationen. Eine gelungene Webpräsenz lebt dabei nicht nur von den bereitgestellten Informationen, sondern vor allem auch von einer anschaulichen grafischen Umsetzung.

Fremde Bilder und Designvorlagen werden durch das Urheberrecht allerdings vor einer unbefugten Nutzung geschützt. In der Folge ist oftmals die kostenpflichtige Einholung von Nutzungsrechten erforderlich. Auch wenn das Urheberrecht im Gegensatz zu Patent- und Markenrechten ursprünglich weniger auf die wirtschaftliche Verwertung und mehr auf den persönlichkeitsrechtsähnlichen Schutz der Beziehung zwischen Urheber und Werk ausgerichtet war, fallen heutzutage mitunter erhebliche Kosten für urheberrechtliche Nutzungsrechte an. Viele Organisationen verfügen jedoch nicht über die Mittel, um entsprechende Leistungen in Anspruch zu nehmen, und müssen deshalb kostenlose oder gemeinfreie Alternativen ins Auge fassen.

Im Gegensatz zu anderen Rechtsordnungen kann der Schöpfer eines Werks nach dem deutschen Urheberrecht nicht auf seine Urheberschaft (als solche) verzichten oder diese an andere Personen übertragen. Zwar kann der Urheber einseitig auf die Durchsetzung seiner Rechte verzichten, dies stellt jedoch aus Nutzersicht im Regelfall keine rechtssichere Vorgehensweise dar. Im Ergebnis können Werke daher nicht ohne weiteres frei verfügbar gemacht werden.

Creative Commons-Lizenzen

Eine mögliche Alternative können unter anderem Werke, die unter den sogenannten Creative Commons-Lizenzen (CC-Lizenz) bereitgestellt werden, sein. Bei den CC-Lizenzen handelt es sich um vorformulierte Standardlizenzverträge, die eine schnelle und weitestgehend rechtssichere Einräumung von Nutzungsrechten an urheberrechtlich geschützten Werken ermöglichen sollen. Dabei bestehen bis heute mehrere unterschiedliche Standardvertragstexte, die auf die jeweiligen

Bedürfnisse zugeschnitten sind. Je nach seinen Vorstellungen kann der Urheber wählen, ob er lediglich eine Namensnennung (by – Attribution) einfordert, zusätzlich die kommerzielle Nutzung (nc – non Commercial) oder eine weitere Bearbeitung ausschließt (nd – non derivatives) oder sogar auf Basis der speziellen CC Zero-Lizenz überhaupt keine Anforderungen stellt (vgl. hierzu auch Thinius, Öffentlich-rechtlicher Rundfunk zu „unprivat"?, DFN-Infobrief Recht 5/2014).

Die Lizenzen werden dabei fortlaufend überarbeitet und weiterentwickelt. Gegenwärtig bestehen im Wesentlichen zwei Varianten der Lizenzen. So sind die Lizenzbedingungen zum einen in der Fassung 3.0 speziell auf die deutsche Rechtslage portiert und zum anderen in der neueren Fassung 4.0 zumindest in der deutschen Übersetzung verfügbar. Dabei wählt der Urheber die von ihm gewünschte Fassung und der Nutzer akzeptiert die Lizenzbedingungen durch die Nutzung des Werks. Diese Vorgehensweise ermöglicht somit die Einräumung von Nutzungsrechten, ohne dass dafür umfangreiche Gespräche oder Verhandlungen erforderlich wären. Als Hauptgrund für diese kostenfreie Bereitstellung von Werken wird immer wieder der Beitrag für den freien Zugang zu Kulturgütern genannt und somit das Allgemeinwohl in den Vordergrund gestellt. Daneben kann eine entsprechende Lizenzierung jedoch auch für den Urheber von Vorteil sein, da sich das Werk so frei verbreiten kann und in der Folge auch die Bekanntheit des Künstlers gesteigert wird.

Rechtliche Problemstellung

Der Vorteil des CC-Lizenzierungsmodells liegt darin, dass der Urheber auf der einen Seite die Nutzung des Werks für bestimmte Kreise ermöglichen kann und gleichzeitig den rechtlichen Schutz des Urheberrechts gegenüber Unberechtigten nicht verliert. So stellt die unberechtigte Nutzung eines entsprechend lizenzierten Werkes weiterhin eine Urheberrechtsverletzung dar, mit der Schadensersatz- und Unterlassungsansprüche einhergehen. Im Zusammenhang mit der Nutzung im Internet kann es dabei schnell zu einem Verstoß gegen das Recht auf öffentliche Zugänglichmachung gem. § 19a Urheberrechtsgesetz (UrhG) kommen.

Rechtliche Probleme können trotz des Lizenztextes dort auftreten, wo der Umfang der verwendeten Begrifflichkeiten nicht abschließend geklärt ist. Dies zeigt ein aktueller Fall, in dem das Deutschlandradio als öffentlich-rechtlicher Rundfunkanbieter von einem Fotografen auf Unterlassung und Schadensersatz in Anspruch genommen worden ist.
Der Radiosender hatte ein Bild, das von dem Kläger unter der Lizenzbedingung der Namensnennung und nicht kommerziellen Nutzung bereitgestellt worden war, genutzt, um einen Beitrag auf einer Webseite des Deutschlandradios zu untermalen. Mit dieser Nutzung war der Fotograf nicht einverstanden, weil es sich unter anderem um eine kommerzielle Nutzung handle. Der anschließende Rechtsstreit musste sich deshalb in erster Linie mit der Frage befassen, ob die Tätigkeit des Deutschlandradios noch als nicht kommerziell einzustufen ist.

Erstinstanzliches Urteil des LG Köln

In der ersten Instanz entschied das Landgericht (LG) Köln (vgl. dazu auch Thinius, Öffentlich-rechtlicher Rundfunk zu „unprivat"?, DFN-Infobrief Recht 5/2014), dass als eine nicht kommerzielle Nutzung nur die rein private Nutzung in Betracht komme.

Da der Begriff der kommerziellen Nutzung nach Ansicht des Gerichts in den Lizenzbedingungen selbst nicht definiert werde, greift es zur Klärung der Frage zunächst ergänzend auf die in § 16a Abs. 1 Rundfunkstaatsvertrag (RStV) für das Rundfunkrecht kodifizierte Definition zurück. Nach der Feststellung, dass das Angebot des Deutschlandradios weder kostenpflichtig sei noch durch Werbung oder Sponsoring finanziert werde und die Voraussetzungen des § 16a Abs. 1 RStV insoweit nicht erfüllt sind, stellt es sich allerdings auf den Standpunkt, dass es auf diese Definition nicht ankomme. Stattdessen müsse auf die urheberrechtliche Zweckübertragungslehre und die allgemeinen zivilrechtlichen Auslegungsregelungen der §§ 133, 157 Bürgerliches Gesetzbuch (BGB) und somit den objektiven Erklärungswert zurückgegriffen werden.

Nach Ansicht des Gerichts umfasse dieser objektive Erklärungswert einer nicht kommerziellen Nutzung lediglich die rein private Nutzung. So sei von dem Urheber keine Unterscheidung zwischen öffentlich-rechtlichen und privaten Sendern gewollt worden. Das Deutschlandradio müsse sich daher wie ein privater und somit auch kommerzieller Sender behandeln lassen.

An diesem Urteil wurde von verschiedenen Seiten teils erhebliche Kritik geübt. So irre das Gericht unter anderem darin, dass die Lizenzbedingungen keine Definition für die nicht

kommerzielle Nutzung enthielten. Darüber hinaus wurde auch angemerkt, dass das Gericht die Ziele, die mit CC-Lizenzen verfolgt werden, nicht ausreichend gewürdigt habe.

Urteil des OLG Köln

Als Berufungsinstanz hat sich nun das OLG Köln ebenfalls mit der Frage auseinandergesetzt, was unter einer nicht kommerziellen Nutzung im Rahmen der CC-Lizenzen zu verstehen ist (U. v. 31.10.2014 – 6 U 60/14). Das Gericht entschied zunächst, dass das Internetangebot des Deutschlandradios aufgrund der Gebührenfinanzierung nicht in einem engeren Sinne als unentgeltlich zu bezeichnen sei. Fraglich sei jedoch, ob das Angebot durch diesen Umstand im Gegenzug auch als kommerziell eingestuft werden muss.

Anders als die Vorinstanz greift das OLG Köln zur Beantwortung dieser Frage sowohl auf den konkreten Lizenzbedingungstext als auch auf eine Broschüre der Creative Commons Organisation zu diesem Thema zurück. Demnach sei eine kommerzielle Nutzung dann anzunehmen, wenn sie „hauptsächlich auf einen geschäftlichen Vorteil oder eine vertraglich geschuldete geldwerte Verfügung abzielt."

Allein anhand dieses Wortlauts lasse sich die Frage jedoch nicht abschließend beantworten. Erkennbar sei aber, dass es für die Bewertung auf die konkrete Nutzungsform und nicht auf das abstrakte Aufgabengebiet ankomme. Allein der Umstand, dass das Deutschlandradio einen öffentlich-rechtlichen Auftrag verfolge, bedeute nicht, dass alle vorgenommenen Handlungen auch als nicht kommerziell eingestuft werden müssen. Im Ergebnis sah sich das OLG dennoch auch unter Zugrundelegung der Lizenzbedingungen und unter ausdrücklicher Berücksichtigung der mit den CC-Lizenzen verfolgten Zwecke nicht in der Lage, eine abschließende Einordnung vorzunehmen.

Da die Lizenzbedingungen nach Ansicht des Gerichts jedoch als Allgemeine Geschäftsbedingungen (AGB) zu beurteilen sind, müsse letztlich auf die sogenannte Unklarheitenregelung des § 305c Abs. 2 BGB zurückgegriffen werden. Diese besagt, dass Zweifel an der Reichweite einer Formulierung zulasten des Verwenders gehen. Im Ergebnis müsse sich somit der Urheber, der sich für die Lizenzierung nach CC-Bedingungen entschieden hat, die Unklarheiten in diesem Einzelfall zurechnen lassen.

Fazit und Auswirkungen auf die Hochschulpraxis

Mit dem Urteil des OLG hat nun auch eine weitere Entscheidung des LG Köln zu urheber- und internetrechtlichen Fragestellungen einer weiteren Überprüfung nicht Stand gehalten. Anders als die Vorinstanz zieht das OLG auch direkt den Lizenztext zur Auslegung der offenen Formulierung zu Rate. Vor allem unter Zugrundelegung der Zwecke, die mitunter durch die CC-Lizenzierung verfolgt werden, erscheint die Beschränkung auf die rein private Nutzung als zu restriktiv. So besteht insbesondere bei vielen gemeinnützigen Organisationen oder Verbänden ein großes Bedürfnis für die Nutzung solcher Werke.
Gleichzeitig zeigt das vorliegende Verfahren aber auch deutlich, wie problematisch die Grenzziehung in einem solchen Fall sein kann. Zwischen der rein privaten Nutzung und der klar als kommerziell zu klassifizierenden Nutzung besteht ein Graubereich mit vielen Schattierungen, der eine rechtliche Einordnung schwierig macht und letztlich wohl nur über eine Einzelfallabwägung zu erfassen sein wird.

Zusammenfassend lässt sich jedoch sagen, dass das Urteil des OLG aus Hochschulsicht aufgrund der Abkehr von der Beschränkung auf rein private Tätigkeiten zu begrüßen ist. So handelt es sich bei den meisten Hochschulen und Universitäten um Körperschaften des öffentlichen Rechts, welche keiner direkten gewerblichen Tätigkeit nachgehen. So kann sich bei der Nutzung entsprechend lizenzierter Texte durch eine Hochschule ebenfalls die Frage stellen, ob eine kommerzielle Tätigkeit vorliegt. Während nach dem Urteil der Vorinstanz nur die rein private Nutzung als nicht kommerzielle Tätigkeit anzusehen ist und deshalb wohl auch bei Hochschulen regelmäßig eine kommerzielle Nutzung vorgelegen hätte, haben sich die Vorzeichen nach dem Urteil des OLG Köln leicht zugunsten der Hochschulen verschoben.

Auch wenn das OLG Köln keine ausdrückliche Definition für den Begriff der nicht kommerziellen Nutzung liefert, so folgt es nicht der Beschränkung auf die rein private Tätigkeit, die das LG vorgenommen hatte. In der Folge ist der Umfang der nicht kommerziellen Nutzung nicht nur auf die rein private Tätigkeit beschränkt und auch Hochschulen sind nicht von vornherein von einer entsprechend Nutzung ausgeschlossen. Dennoch bleibt festzuhalten, dass gegenwärtig keine definitiven Aussagen über die Reichweite gemacht werden können,

da das OLG lediglich auf eine Unklarheitenregelung aus dem AGB-Recht zurückgreift. Aus diesem Grund sollten die Hochschulen auch in der Zukunft Vorsicht bei der Nutzung von CC-lizenzierten Werken unter der Bedingung der nicht kommerziellen Nutzung walten lassen. In diesem Punkt kann daher keine Entwarnung gegeben werden. Da es bei der Einordnung nach Ansicht des Gerichts auf die konkrete Nutzung und nicht bloß die allgemeine Ausrichtung der Tätigkeit ankommt, sind abschließende Einordnungen hier nicht möglich. Es empfiehlt sich daher auf Werke, die auch zur kommerziellen Nutzung freigegeben sind, zurückzugreifen.

Bis auf weiteres muss abgewartet werden, ob obergerichtliche Entscheidungen hier für mehr Klarheit sorgen werden. Aus diesem Grund gilt es, die Rechtsprechung in diesem Bereich auch in der Zukunft näher im Auge zu behalten.

UniRep, Seminare, Kurse & Co. … aber vergesst mir das Urheberrecht nicht!

Seminar- und Kursunterlagen können urheberrechtlichen Schutz genießen

von Kevin Kuta

Das Oberlandesgericht (OLG) Frankfurt a.M. hat mit seinem Urteil vom 04.11.2014 (Az. 11 U 106/13) über die Anforderungen an die Schutzfähigkeit von Seminarunterlagen entschieden. Nach Ansicht des Gerichts können Seminar- und Kursunterlagen als Sammelwerk urheberrechtlichen Schutz nach § 4 Urheberrechtsgesetz (UrhG) genießen. Dafür müssen aber beispielsweise die Auswahl der Einzelwerke und ihre konkrete Anordnung innerhalb der Unterlagen einen geistigen Gehalt aufweisen, der die bloße Summe der Inhalte der einzelnen Elemente überschreitet.

I. Hintergrund

Das Angebot sowie die Anzahl der Anbieter von Seminaren und Kursen steigen fortlaufend an. Für eine Vielzahl der potentiellen Teilnehmer ist neben Inhalten und Dozenten vor allem auch das angebotene Seminar- und Kursmaterial von großer Bedeutung und maßgeblich bei der Entscheidung für oder gegen einen bestimmten Anbieter. Dementsprechend möchten Anbieter von Kursen und Seminaren qualitativ hochwertige Unterlagen anbieten, um die Teilnehmer für sich zu gewinnen. Dies erfordert einen hohen Zeit- und Kostenaufwand, da die mit der Erstellung solcher Unterlagen betrauten Personen häufig über einen längeren Zeitraum ausschließlich damit beschäftigt sind. Auch Hochschulen treten dabei immer mehr in Konkurrenz mit privatwirtschaftlichen Anbietern, wie etwa im Bereich der juristischen oder medizinischen Repetitorien. Hinter privaten Anbietern stehen häufig große Verlage, die auf entsprechendes Personal und eine besondere Expertise zurückgreifen können. Auf Seiten der Hochschulen übernehmen diese Aufgabe meist die jeweiligen Lehrstühle oder Institute.

Durch die Investitionen in Form von Zeit und Personalkosten haben die Anbieter, egal ob auf Seiten der Privatwirtschaft oder der Hochschulen, ein Interesse daran, dass sich der Aufwand längerfristig bezahlt macht und damit amortisiert. Findige Anbieter könnten natürlich auf die Idee kommen, die jeweiligen Seminar- und Kursunterlagen eines Konkurrenten eins-zu-eins zu übernehmen oder zumindest als Grundlage für die eigenen Materialien zu verwenden. Dementsprechend stellt sich die Frage, ob derartige Seminar- und Kursunterlagen urheberrechtlichen Schutz genießen, sodass die Rechteinhaber erfolgreich gegen eine unrechtmäßige Vervielfältigung und Verbreitung vorgehen können.

II. Das Urteil des OLG Frankfurt a.M.

Nach Auffassung des OLG Frankfurt a.M. können Seminar- und Kursunterlagen als Sammelwerk urheberrechtlichen Schutz nach § 4 UrhG genießen. Für einen solchen Schutz sei es aber erforderlich, dass beispielsweise die Auswahl der Einzelwerke und ihre konkrete Anordnung innerhalb der Unterlagen einen über die bloße Summe der Inhalte der einzelnen Elemente hinausgehenden geistigen Gehalt aufweisen. Der zweite Kernpunkt der Entscheidung war die Festlegung der Anforderungen an eine Abmahnung. Nach Ansicht des Gerichts müsse das vorgeworfene rechtswidrige Verhalten in der Abmahnung so bezeichnet werden, dass die Identifizierung der gerügten Rechtsverletzung sowie das betreffende Werk in angemessener Weise möglich sei. Werde der gegnerischen Partei die unberechtigte Verbreitung urheberrechtlich geschützter Unterlagen vorgeworfen, müsse dargestellt werden, worin die Verbreitungshandlung bestehe. Für die folgende Auseinandersetzung wird aus Gründen der Übersichtlichkeit auf diesen

zweiten Kernpunkt der Entscheidung nicht weiter eingegangen.

Sachverhalt

Im zugrundeliegenden Fall streiten die Parteien um vorgerichtliche Rechtsverfolgungskosten für ein urheberrechtliches Abmahnschreiben sowie die Kosten des Rechtsstreits erster Instanz wegen einer angeblichen Urheberrechtsverletzung. Das Gericht hat im Rahmen dieser Kostenstreitigkeiten über die urheberrechtliche Schutzfähigkeit von Seminar- und Kursunterlagen Stellung bezogen. Die Beklagte bietet geschäftsmäßig Seminare an. Die beiden Kläger führten in der Vergangenheit für die Beklagte Schulungen durch, bei denen sie das streitbefangene Lehrmaterial verwendet haben. Die Beklagte hat nach dem Ausscheiden der Kläger diese Unterlagen (handelnd durch ihren Geschäftsführer) an ihren neuen Dozenten weitergegeben. Die Kläger haben die Beklagte wegen angeblicher Urheberrechtsverletzung abgemahnt und forderten sie gleichzeitig erfolglos zur Abgabe einer Unterlassungserklärung, Auskunftserteilung sowie Schadensersatz auf. Nach Ansicht der Kläger seien die Unterlagen nämlich urheberrechtlich schutzfähig und sie seien als Miturheber anteilsberechtigt (nach § 8 Abs. 1 Urheberrechtsgesetz (UrhG) liegt eine Miturheberschaft an einem Werk vor, wenn mehrere ein Werk gemeinsam geschaffen haben, ohne dass sich ihre Anteile gesondert verwerten lassen, nach § 8 Abs. 2 S. 1 Hs. 1 UrhG steht das Recht zur Veröffentlichung und zur Verwertung des Werkes den Miturhebern zur gesamten Hand zu, wobei gemäß § 8 Abs. 2 S. 3 UrhG jeder Miturheber berechtigt ist, Ansprüche aus Verletzungen des gemeinsamen Urheberrechts geltend zu machen, er jedoch nur Leistung an alle Miturheber verlangen kann).

Das Landgericht (LG) Frankfurt a.M. hat die erstinstanzliche Klage letztlich abgewiesen und die Kosten insgesamt den Klägern auferlegt. Neben den Ausführungen zu den Anforderungen an das Abmahnschreiben (in diesem Beitrag erfolgt diesbezüglich keine nähere Erörterung) ließ das LG Frankfurt a.M. verlautbaren, dass durch die Kläger eine Aktivlegitimation zur Untersagung der Kursunterlagen insgesamt nicht dargelegt sei. Eine Miturheberschaft an diesem Lehrmaterial komme nicht in Betracht, da diese unterschiedliche Werkarten enthielten. Es handele sich somit nicht um ein einheitliches Werk, an dem eine Miturheberschaft bestehen könne. Aus diesem Grund sei eine Berufung auf die Vermutung der Urheberschaft nach § 10 UrhG nicht möglich. Das Gericht könne aufgrund der Geltendmachung als Miturheber auch nicht davon ausgehen, dass die Kläger die ihnen möglicherweise an den Einzelwerken zustehenden Einzelrechte geltend machten. Letztlich sei auch nicht ausreichend dargelegt worden, dass es sich bei dem Text der Unterlagen um ein schutzfähiges Sprachwerk im Sinne von § 2 Abs. 1 Nr. 1 UrhG handele. Es handele sich bei dem Text um ein Sprachwerk zu Gebrauchszwecken, sodass erhöhte Anforderungen an die urheberrechtliche Schutzfähigkeit zu stellen seien. Diese erhöhten Anforderungen seien jedoch nicht dargelegt worden. Im Hinblick auf die in den Unterlagen enthaltenen Zeichnungen, Skizzen etc. fehle eine Darstellung, aufgrund welcher Gestaltungen diese urheberrechtlichen Schutz beanspruchen könnten. Gegen dieses Urteil haben die Kläger Berufung beim OLG Frankfurt a.M. eingelegt.

Urheberrechts- und Leistungsschutz an den Unterlagen

Nach Ansicht des OLG Frankfurt a.M. standen den Klägern bis zur übereinstimmenden Erledigungserklärung (da dieses Ereignis für die Ausführungen zum urheberrechtlichen Schutz der Unterlagen nicht von Bedeutung ist, wurde auf eine dahingehende Erörterung im Sachverhalt verzichtet) gegenüber der Beklagten sowie ihrem Geschäftsführer die geltend gemachten Ansprüche auf Unterlassung, Auskunft und Schadensersatz im Hinblick auf das erstellte Lehrmaterial insgesamt nach § 97 Abs. 1, 2 UrhG zu. An den Seminarunterlagen insgesamt bestehe nämlich Urheberrechts- und Leistungsschutz. Die Kursunterlagen umfassen verschiedene Werkarten, wie etwa Sprachwerke in Gestalt der Texte gemäß § 2 Abs. 1 Nr. 1 UrhG, Zeichnungen, Pläne, Karten, Skizzen und Tabellen gemäß § 2 Abs. 1 Nr. 7 UrhG sowie Fotografien gemäß § 2 Abs. 1 Nr. 5 UrhG bzw. § 72 UrhG. Dementsprechend scheide eine einheitliche auf Beiträgen beider Kläger beruhende Werkschöpfung aus.

Eine Schutzfähigkeit der Kursunterlagen bestehe jedoch als Sammelwerk nach § 4 UrhG. Derartigen Sammelwerken stehe urheberrechtlicher Schutz zu, sofern die Auswahl und/oder die Anordnung der einzelnen darin aufgenommenen Elemente eine persönliche geistige Schöpfung im Sinne von § 2 Abs. 2 UrhG darstellten. Es müsse sich in den Elementen ein geistiger Gehalt manifestieren, der über die bloße Summe der Inhalte der einzelnen Elemente des Sammelwerkes hinausgehe. Bei dieser Betrachtung ist nach Ansicht des Bundesgerichtshofs (BGH) der Gesamteindruck entscheidend. Das OLG

Frankfurt a.M. ist der Auffassung, dass dieser geistige Gehalte hinsichtlich der Auswahl der Einzelwerke und ihrer konkreten Anordnung innerhalb der streitbefangenen Kursunterlagen zu bejahen sei. Der Inhalt der Seminarveranstaltung, zu deren Durchführung die Unterlagen angefertigt wurden, beeinflusse die Auswahl der jeweiligen aufzunehmenden Texte, der zu verwendenden Fotografien und Darstellungen wissenschaftlicher und technischer Art nur in geringem Umfang. Dementsprechend stehe dem Gericht ein weiter Entscheidungsspielraum zu. Zum einen spreche für einen geistigen Gehalt der Umstand, dass die Unterlagen der Kläger und damit die ausgewählten Einzelwerke nur im Hinblick auf eine Fotografie mit den Unterlagen übereinstimmten, die nunmehr der neue Dozent innerhalb des Seminares verwende. Zum anderen gehe auch die Anordnung der Einzelwerke zueinander über die Summe der bloßen Inhalte hinaus. Diesbezüglich dienten die jeweils in die textliche Darstellung eingefügten Fotografien sowie die Zeichnungen, Pläne, Karten, Skizzen und Tabellen didaktischen Zwecken, wie der Erläuterung und Veranschaulichung der textlichen Inhalte. Durch die Gegenüberstellung der Unterlagen des neuen Dozenten, die vom Inhalt und der Anordnung wesentlich von den klägerischen Unterlagen abweichend seien, mit den Unterlagen der Kläger werde die eigenschöpferische Leistung durch die Auswahl der Einzelwerke und ihre Anordnung bestätigt.

Aktivlegitimation

Nach Ansicht des Gerichts seien die Kläger auch aktiv legitimiert gewesen, die Ansprüche auf Unterlassung, Auskunft und Schadensersatz geltend zu machen. Die Miturheberschaft (§ 8 UrhG) an dem Sammelwerk sei nach § 10 UrhG zu Gunsten der Kläger zu vermuten. Die Urheberbezeichnung bei einem Sammelwerk nach § 4 UrhG zeigt auf, dass der oder die Urheber die Auswahl und/oder die Anordnung der Einzelwerke getätigt haben. Eine Miturheberschaft der Beteiligten sei bei einer gemeinsamen Auswahl und Anordnung der Beiträge anzunehmen. Da auf den Kursunterlagen mehrfach die Namen beider Kläger zu finden seien, bestehe eine Vermutung hinsichtlich der Miturheberschaft der Kläger. Die Beklagte habe keine Beweise vorgebracht, die die Urheberrechtsvermutung der Kläger widerlegen könnten.

Verletzung und Wiederholungsgefahr

Durch die Verbreitung der Unterlagen in den Seminaren durch die Beklagte habe diese auch das Urheberrecht der Kläger verletzt (§§ 15 Abs. 1 Nr. 2, 17 UrhG). Die Beklagte hat die Unterlagen an den neuen Dozenten weitergegeben, sodass sie diese dadurch in Verkehr gebracht und somit verbreitet hat (§§ 15 Abs. 1 Nr. 2, 17 Abs. 1 UrhG). Nach höchstrichterlicher Rechtsprechung wird ein Werkstück nämlich dann in Verkehr gebracht, wenn mindestens ein Original oder Vervielfältigungsstück aus einer internen Betriebssphäre durch Eigentumsübertragung der Öffentlichkeit zugeführt wird. In der Übergabe eines Unterlagenexemplars an den neuen Dozenten durch die Beklagte sei eine endgültige Zurverfügungstellung zu sehen. In dieser Überlassung sei nach dem objektiven Empfängerhorizont eine Übereignung des Unterlagenexemplars an denen neuen Dozenten zu sehen (§ 929 S. 1 Bürgerliches Gesetzbuch (BGB)). Bei dem neuen Dozenten handele es sich mangels einer persönlichen Verbindung zum Beklagten auch um die nach §§ 17 Abs. 1, 15 Abs. 3 S. 2 UrhG erforderliche „Öffentlichkeit". Da die Beklagte weder dargelegt noch bewiesen habe, dass eine Zustimmung der Kläger vorliege, erfolgte die Verbreitung der Unterlagen widerrechtlich.

Die Widerrechtlichkeit entfalle auch nicht, wenn sich die Beklagte darauf beriefe, die Kläger hätten die Unterlagen im Auftrag der Beklagten erstellt und der Beklagten dadurch die Unterlagen zur Verfügung gestellt und die Zustimmung zur Nutzung und Weiterverbreitung erteilt. Selbst bei einer Erstellung der Unterlagen für die Beklagte sei für die Übertragung oder Einräumung von Nutzungsrechten an die Beklagte nach §§ 34, 35 UrhG die Zustimmung der Urheber (also der Kläger) erforderlich, was aber von der Beklagten nicht dargelegt wurde. Gleiches gelte für eine Absprache zwischen der Beklagten und den Klägern, dass die Unterlagen neben Kursteilnehmern auch an interessierte Nicht-Kursteilnehmer gegen Zahlung eines Entgeltes weitergegeben werden dürften. Eine derartige Zustimmung der Kläger unterscheide sich jedoch von einer Zustimmung zur Weitergabe der Unterlagen an den neuen Dozenten, da dieser die Unterlagen nicht gegen Entgeltzahlung als Interessent des Seminars erhalte. Letztlich ergebe sich auch nichts anderes aus dem Vorbringen der Beklagten, die Erstellung der Unterlagen sei Bestandteil des an die Kläger gezahlten Honorars gewesen, wodurch der Beklagten die Unterlagen ohne Einschränkung zur beliebigen Verwendung und Weiterverbreitung überlassen worden seien.

Nach Ansicht des Gerichts handele es sich dabei um einen pauschalen Vortrag. Ihm sei nicht zu entnehmen, wann die Kläger der Beklagten derart weitgehende Befugnisse eingeräumt hätten. Vielmehr spreche § 44 Abs. 1 UrhG für die Kläger, wonach bei der Veräußerung des Originalwerkes durch den Urheber dieser dem Erwerber im Zweifel kein Nutzungsrecht einräume.

III. Fazit und Auswirkungen für die Hochschulen

Das Urteil des OLG Frankfurt a.M. macht deutlich, dass bei einem entsprechenden geistigen Gehalt von Seminar- und Kursunterlagen diese als Sammelwerk (§ 4 UrhG) urheberrechtlichen Schutz genießen können. Seminar- und Kursveranstaltungen gehören zum Alltag an deutschen Hochschulen. Daneben sprießen in bestimmten Fachbereichen auch neue universitäre Veranstaltungen aus dem Boden, wie etwa Repetitorien in den Bereichen Rechtswissenschaft und Medizin (sog. „UniRep“), welche mit privat-wirtschaftlichen Anbietern in Konkurrenz stehen. Die Qualität der im Zuge der Veranstaltung verteilten Unterlagen ist für eine Vielzahl der Teilnehmer ein wichtiges Auswahlkriterium. Dementsprechend qualitativ hochwertig müssen die eigens für die Veranstaltung angefertigten Unterlagen sein, um die Teilnehmer für sich zu gewinnen. Dabei stellt sich natürlich sowohl an Hochschulen, als auch bei den Anbietern aus der Privatwirtschaft die Frage, wem die Rechte an den erstellten Unterlagen zustehen. Das besprochene Urteil macht deutlich, dass man diese Frage im Idealfall im Vorfeld schriftlich regeln sollte, damit keine Probleme beim Wechsel der Dozenten sowie der Ersteller der Kursmaterialien aufkommen. Insbesondere die Einräumung von Nutzungsrechten erscheint unumgänglich, damit der Anbieter rechtssicher agieren kann.

Gerade bei universitären Seminaren oder Repetitorien obliegt die Unterlagenerstellung meist dem Professor, der das Seminar oder die Vorlesung abhält. Dieser betraut mit der Erstellung nicht selten einen oder mehrere Mitarbeiter. Je nach Themengebiet können auf diese Weise Skripte in Form ganzer Lehrbücher entstehen, die eine erhebliche Arbeitsleistung und -zeit in Anspruch genommen haben. Trotz des gebotenen Aufwands wird man in diesem Fall weiterhin den Professor als Urheber ansehen müssen, sodass diesem keine Nutzungsrechte seiner Mitarbeiter eingeräumt werden müssen. Die Erstellung der Unterlagen wird nämlich regelmäßig zu ihren Aufgaben gehören, die ihnen im Detail von ihrem Vorgesetzten vorgegeben und auf dieser Grundlage erstellt werden. Auch werden die Mitarbeiter kein darüber hinausgehendes Honorar verlangen können. Vielmehr wird die Erstellung durch den üblichen Arbeitslohn beglichen sein. Anders kann es natürlich aussehen, wenn externe Personen auf Werkvertragsbasis mit der Erstellung von Unterlagen betraut werden. In einem solchen Fall wird die externe Person – und gerade nicht der Professor – als Urheber der Unterlagen anzusehen sein. Dementsprechend sollte man in dieser Konstellation insbesondere auf die Einräumung entsprechender Nutzungsrechte achten, um die Gefahr rechtlicher Auseinandersetzungen schon im Vorfeld einzudämmen.

Das haben wir auf Band

Zu den persönlichkeitsrechtlichen Problemen bei der audiovisuellen Aufzeichnung von Personen

von Florian Klein

Jeder Person steht ein Recht am eigenen Wort und am eigenen Bild zu. Dieses wird berührt, sobald Foto-, Ton- oder gar Videoaufnahmen von ihr getätigt werden. Da auch im Hochschulbereich zunehmend mit solchen Mitteln gearbeitet wird, um Studierenden größtmögliche Flexibilität beim Zugang zu Lehrveranstaltungen zu bieten, kommt immer häufiger die Frage auf, was bei der Anfertigung und Veröffentlichung solcher Aufnahmen im Hinblick auf die Persönlichkeitsrechte von Lehrenden und Studierenden beachtet werden muss.

I. Hintergrund

Im Bereich der Lehre wird es an Hochschulen zunehmend populärer, Vorlesungen und andere studienbegleitende Veranstaltungen aufzuzeichnen, um diese anschließend im Internet oder zumindest im Intranet für Studierende und andere Interessierte zugänglich zu machen. Dadurch soll es den Studierenden ermöglicht werden, ihren Tagesablauf ungehindert von den Zwängen fester Vorlesungszeiten flexibler und individueller zu gestalten und trotz sonstiger Termine oder der Ausübung einer Nebentätigkeit zur Finanzierung des Studiums nicht auf die Darbietung der Lehrinhalte verzichten zu müssen. Technische Schwierigkeiten stehen einem solchen Angebot der jeweiligen Hochschulen heutzutage nur noch selten entgegen. Zwar ist es für den jeweiligen Dozenten und auch für die Interaktion zwischen Lehrenden und Lernenden durchaus erstrebenswert, auch weiterhin eine größtmögliche physische Anwesenheit der Studierenden in den Lehrveranstaltungen zu erreichen, allerdings gibt es zahlreiche Gründe, warum dies nicht immer umsetzbar ist. So komfortabel und förderlich für die Vor- und Nachbereitung des Lernstoffes ein solcher Service auch sein mag, gilt es dennoch, einige rechtliche Aspekte zu berücksichtigen. Neben urheberrechtlichen und datenschutzrechtlichen Problemen können dabei insbesondere persönlichkeitsrechtliche Friktionen entstehen, sobald Personen auf den Aufzeichnungen zu hören oder zu sehen sind. Was im Hinblick auf das Recht am eigenen Bild und das Recht am eigenen Wort bei Vorlesungsaufzeichnungen zu berücksichtigen ist, soll daher in diesem Beitrag dargestellt werden.

II. Rechtliche Betrachtung

Den aufgenommenen Personen stehen die Rechte am eigenen Bild und am eigenen (gesprochenen) Wort zu, welche aus dem allgemeinen Persönlichkeitsrecht nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz (GG) hergeleitet werden. Insofern ist nicht zuletzt wegen der unterschiedlichen gesetzlichen Regelungen zwischen dem visuellen und dem auditiven Teil einer Aufnahme zu differenzieren.

1. Recht am eigenen Bild

Das Recht am eigenen Bild findet neben seiner verfassungsrechtlichen Herleitung auch einen spezialgesetzlichen Niederschlag im Kunsturhebergesetz (KUG). Gemäß § 22 S. 1 KUG dürfen Bildnisse nur mit Einwilligung der Betroffenen verbreitet und öffentlich zur Schau gestellt werden. Ein Bildnis im Sinne des KUG ist die Wiedergabe des äußeren Erscheinungsbildes einer Person in einer für Dritte erkennbaren Weise, sodass auch Videoaufnahmen als geschütztes Bildnis einzuordnen sind, wenn Personen darauf in erkennbarer Weise abgebildet sind. Das Recht am eigenen Bild ist also berührt, sofern es um Bild- oder Videoaufnahmen geht, auf denen der Dozent oder andere Veranstaltungsteilnehmer zu erkennen sind. Zu beachten ist allerdings, dass das Recht am

eigenen Bild im Sinne des KUG noch nicht die Herstellung der Videoaufnahmen verbietet, sondern nur deren Verbreitung und öffentliche Zurschaustellung. Insofern steht zumindest das KUG der bloßen visuellen Aufzeichnung einer Lehrveranstaltung nicht im Wege. Allerdings ist anerkannt, dass darüber hinausgehend das allgemeine Persönlichkeitsrecht im Einzelfall auch schon der bloßen Aufnahme entgegenstehen kann. Das generelle Einwilligungserfordernis des KUG gilt also erst, wenn entsprechende Videoaufnahmen veröffentlicht oder an Dritte weitergegeben werden sollen. Dies gilt nicht nur für Veröffentlichungen der fertigen Dateien im Inter-/Intranet, sondern auch für das Angebot von Live-Streams der jeweiligen Veranstaltungen.

Es gibt allerdings auch Ausnahmen von diesem generellen Einwilligungserfordernis, die insbesondere der Wahrung der Pressefreiheit und der Befriedigung des Informationsinteresses der Allgemeinheit dienen. Diese finden sich in § 23 Abs. 1 Nr. 1-4 KUG. Liegt eine der dort benannten Ausnahmekonstellationen vor, dürfen Bildnisse auch ohne Einwilligung der abgebildeten Personen veröffentlicht werden, sofern nicht berechtigte Interessen der Betroffenen dadurch verletzt werden.

Von besonderer praktischer Relevanz sind dabei die Ausnahmen für Bildnisse aus dem Bereich der Zeitgeschichte (Nr. 1), für Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen (Nr. 2) oder für Bilder von Versammlungen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben (Nr. 3). Bei den letzten beiden Varianten (Aufnahmen von Landschaften/Versammlungen) ist jedoch zu beachten, dass die Abbildung einer bestimmten Person gerade nicht im Vordergrund stehen darf, sondern es primär um die Darstellung der Landschaft beziehungsweise der Versammlung als solcher gehen muss. Entscheidend ist dabei der Gesamteindruck, den das jeweilige Bild dem Betrachter vermittelt. Zu berücksichtigen ist außerdem, dass die Ausnahme für Abbildungen von Versammlungen und ähnlichen Vorgängen nur für Vorgänge gilt, die in der Öffentlichkeit stattfinden. Im Rahmen von Aufzeichnungen von Lehrveranstaltungen kommt es deshalb darauf an, inwieweit diese für die Öffentlichkeit zugänglich sind. In Nordrhein-Westfalen beispielsweise regelt § 59 Abs. 1 Hochschulgesetz NRW (HG NRW), dass das Recht zum Besuch von Lehrveranstaltungen außerhalb des gewählten Studienganges durch den Fachbereich beschränkt werden kann, wenn ohne die Beschränkung eine ordnungsgemäße Ausbildung der für einen Studiengang eingeschriebenen Studierenden nicht gewährleistet werden kann. Deshalb wird man hier nicht generell von einer Öffentlichkeit der Vorlesungen ausgehen können. Entscheidend sind also die jeweilige landesgesetzliche Regelung und etwaige Zugangsregelungen der betreffenden Hochschule.
Bei den Bildnissen aus dem Bereich der Zeitgeschichte kommt es hauptsächlich darauf an, ob die Abbildung der betroffenen Person dem Informationsinteresse der Öffentlichkeit dient, wobei dies weit zu verstehen ist und alle Fragen von allgemeinem gesellschaftlichen Interesse umfasst. Klassische Anwendungsbeispiele dieser Ausnahme sind Veröffentlichungen von Fotos von Prominenten, Politikern und anderen Personen, die im Fokus der Öffentlichkeit stehen. Dennoch geht sie auch darüber hinaus und kann Abbildungen von Personen erfassen, die nur (vorübergehend) aufgrund besonderer Ereignisse in der Öffentlichkeit Beachtung finden. Sofern davon jedoch normale Privatpersonen betroffen sind, kommt dem Schutz ihres Privatlebens eine größere Bedeutung zu als bei Personen des öffentlichen Lebens, was bei der Abwägung der betroffenen Interessen zu berücksichtigen ist.

Ob diese Ausnahmen bei einer Bildaufnahme von Zuhörern einer Lehrveranstaltung einschlägig sind, entzieht sich einer abstrakten Beurteilung, sondern muss im Einzelfall unter Betrachtung der Art der Veranstaltung sowie der konkreten Abbildung beurteilt werden.

Da diese Ausnahmetatbestände jedoch allesamt unter dem Vorbehalt stehen, dass durch die Verbreitung oder öffentliche Zurschaustellung keine berechtigten Interessen der Betroffenen verletzt werden, ist stets eine Interessenabwägung vorzunehmen, in der ermittelt wird, ob eine Veröffentlichung nicht zu unterbleiben hat, wie dies zum Beispiel meist bei Aufnahmen der Fall ist, die intime oder sehr private Situationen abbilden.

Erteilung einer Einwilligung

Kann man sich für die konkrete Abbildung nicht auf die Ausnahmetatbestände des § 23 KUG berufen, bleibt es bei dem Grundsatz, dass eine Verbreitung und öffentliche Zurschaustellung nur mit Einwilligung des Abgebildeten zulässig ist. Dies gilt also für jegliche Bereitstellung solcher Aufnahmen im Intranet/Internet. Die für eine Online-Veröffentlichung von Aufzeichnungen erforderliche Einwilligung der abgebildeten Personen kann allerdings nur dann wirksam sein, wenn sie sich auch explizit auf diese Form der Veröffentlichung bezieht.

Das KUG stellt keine speziellen formellen Anforderungen an die Einwilligung. Nur in § 22 Abs. 2 KUG findet sich eine Regelung zur Einwilligung, wonach diese im Zweifel als erteilt gilt, wenn der Abgebildete für die Abbildung eine Entlohnung erhielt. Es entspricht der herrschenden Meinung, dass die Einwilligung deshalb formfrei möglich ist, sodass die Erteilung der Einwilligung im Hinblick auf das Recht am eigenen Bild mündlich oder sogar nur konkludent, d. h. stillschweigend durch entsprechendes Verhalten, erfolgen kann. Eine konkludente Einwilligung kann regelmäßig bejaht werden, wenn aus Sicht des Einwilligungsempfängers unter Berücksichtigung der Gesamtumstände davon ausgegangen werden kann, dass der Abgebildete die Anfertigung der Aufnahme in Kenntnis ihres Zweckes gebilligt hat. Dabei ist zu beachten, dass die Einwilligung so konkret wie möglich auf die geplanten Verwendungen und deren Ausgestaltungen abzielen sollte. Denn im Zweifel wird angenommen, dass der Abgebildete die Einwilligung nur in dem Umfang erteilt hat, wie dies zur Erfüllung des Aufnahmezwecks erforderlich war. Eine lediglich allgemein formulierte Einwilligung wird dementsprechend nicht ausreichend sein. Vielmehr muss dem Betroffenen bei Erteilung der Einwilligung Art, Umfang und Zweck der Verwendung seines Bildnisses bekannt sein. Eine ausführliche Aufklärung über den Zweck der Aufnahme verhindert zudem, dass die Einwilligung im Nachhinein willkürlich widerrufen werden kann. Die Beweislast für den Umfang der Einwilligung trägt derjenige, der das Bildnis nutzt. Außerdem ist eine Einwilligung nur dann wirksam, wenn sie freiwillig erteilt wird. Deshalb muss bei Bild- oder Videoaufnahmen von Vorlesungen, in denen in aller Regel zumindest der Dozent zu sehen sein wird, dessen Einwilligung eingeholt werden, sofern er überhaupt mit einer Aufnahme einverstanden ist. Gegen seinen Willen wird sich eine Aufzeichnung nicht realisieren lassen.

Im Übrigen sollte darauf geachtet werden, dass möglichst keine Zuhörer mit erfasst werden, um die Anzahl der erforderlichen Einwilligungen weitestgehend zu minimieren. Bei einem Schwenk über die Zuhörerschaft in einem Hörsaal könnte im Einzelfall zwar die Ausnahme des KUG für Versammlungen einschlägig sein, sofern die Veranstaltung öffentlich zugänglich ist, allerdings ist dies rechtlich nicht risikolos im Hinblick auf potentielle Verletzungen des Rechts am eigenen Bild, falls die Voraussetzungen dieser Ausnahme nicht erfüllt sind.

Hält man eine Einbeziehung der Zuhörerschaft für unabdingbar, empfiehlt es sich, im Saal einen Bereich speziell zu kennzeichnen, welcher von der Aufzeichnung betroffen ist, und gleichzeitig auch einen Bereich frei zu lassen, in dem die Zuhörer unbehelligt bleiben können. Im Aufzeichnungsbereich sollte dann im Vorhinein ein deutlicher Hinweis angebracht werden, dass dort die Wahl eines Sitzplatzes eine Einwilligung in eine entsprechende Aufzeichnung und spätere Veröffentlichung darstellt. Dabei ist es in jedem Fall erforderlich, dass klar kommuniziert wird, in welcher Art und Weise die Veröffentlichung erfolgen soll. Allgemeine Ausführungen reichen in aller Regel nicht aus. Gerade bei einer Veröffentlichung im Internet, die zu einer Zugänglichkeit der Aufnahmen für eine unbeschränkte, weltweite Öffentlichkeit führt, ist eine explizite Aufklärung zu fordern. Bei Erfüllung dieser Voraussetzungen lässt sich die Wahl eines Sitzplatzes im Aufzeichnungsbereich jedoch als konkludente Einwilligung deuten.

Aus rechtlicher Sicht sind schriftliche und mündliche oder gar konkludente Einwilligungen im Hinblick auf das Recht am eigenen Bild/Wort grundsätzlich gleichwertig. Rein praktisch ergibt sich jedoch insofern ein Unterschied, als derjenige, der die Veröffentlichung der Aufzeichnungen vornimmt, beweispflichtig für das Vorliegen der Einwilligung und deren Umfang ist. Aus diesem Grund ist stets die Einholung einer schriftlichen Einwilligung anzuraten, in der möglichst klar die Verwendungszwecke beschrieben werden. Der durch eine schriftliche Einwilligung mögliche Urkundenbeweis ist deutlich verlässlicher als der Zeugenbeweis und räumt einem Gericht im Streitfall tendenziell weniger Auslegungsspielraum hinsichtlich der Reichweite einer konkreten Einwilligung ein. Gerade die Einwilligung der Dozenten, die bei solchen Veranstaltungen im absoluten Fokus stehen, sollte deshalb unbedingt vorab schriftlich eingeholt werden. Aber auch bei Einbeziehung der Zuhörerschaft in einem speziell gekennzeichneten Aufzeichnungsbereich ist man mit der Einholung einer vorherigen schriftlichen Einwilligung gut beraten.

Widerruf der Einwilligung

Ist man mit einer Einwilligung des Betroffenen zunächst auf der sicheren Seite, stellt sich die Frage, wie zu verfahren ist, wenn Aufnahmen bereits veröffentlicht sind und die abgebildete Person nun den Widerruf ihrer Einwilligung erklärt, weil sie sich im Nachhinein überlegt hat, dass sie doch nicht (mehr) in der veröffentlichten Aufzeichnung abgebildet sein möchte.

Die mittlerweile herrschende Meinung ordnet die Einwilligung als empfangsbedürftige rechtsgeschäftliche (oder zumindest rechtsgeschäftsähnliche) Willenserklärung ein, die grundsätzlich bindend und darum nicht frei widerruflich ist. Welche Konsequenzen dies jedoch für die Widerrufsmöglichkeit im persönlichkeitsrechtlichen Bereich hat, ist in der Rechtswissenschaft umstritten.

Einige Stimmen halten die Einwilligung jedenfalls im Hinblick auf spätere Veröffentlichungen für frei widerruflich. Andere hingegen verlangen, dass der Betroffene durch die Publikation in seiner Persönlichkeit empfindlich beeinträchtigt wird.

In der Rechtsprechung wiederum hat sich eine weitgehend einheitliche Herangehensweise herausgebildet. Ein großer Teil der Rechtsprechung erkennt aufgrund der besonderen persönlichkeitsrechtlichen Bedeutung einer solchen Einwilligung eine Widerrufsmöglichkeit grundsätzlich an, fordert dafür aber das Vorliegen eines wichtigen Grundes. Dies gilt insbesondere für eine vertraglich erteilte Einwilligung, die mit einer Gegenleistung vergolten wird und damit kommerzialisiert ist (z. B. für Werbefotos etc.).

Dass eine besondere Widerrufsmöglichkeit überhaupt diskutiert wird, beruht auf dem Gedanken, dass sich die Persönlichkeit stets fortentwickelt und entfaltet und in diesem Rahmen auch Veränderungen fundamentaler Überzeugungen eintreten können. Ein solcher Überzeugungswandel muss allerdings nachhaltig, dauerhaft und erkennbar sein, um ausnahmsweise einen Widerruf legitimieren zu können. Wann dies der Fall ist, lässt sich nicht pauschal beurteilen, sondern erfordert eine Betrachtung der genauen Umstände des Einzelfalls. Aber auch andere Umstände können im Einzelfall einen wichtigen Grund darstellen, der zum Widerruf berechtigt. Zu Illustrationszwecken sollen im Folgenden einige Beispiele aus der Rechtsprechung genannt werden, bei denen das Vorliegen eines wichtigen Grundes thematisiert wurde:

- Wird in Überrumpelungsfällen vorschnell eine Einwilligung erteilt, z. B. wenn ein Fernsehteam plötzlich vor der Haustür steht, wird dies in der Regel als wichtiger Grund eingeordnet.
- Wenn die Weiterverwertung von Filmaufnahmen in Folge einer Wandlung der Persönlichkeit verletzend wäre, insbesondere weil die Ausstrahlung der Sendung zu erheblichen physischen oder psychischen Belastungen führen würde, liegt ebenfalls ein wichtiger Grund vor, der den Widerruf der vorher erteilten Einwilligung ermöglicht.
- Kein wichtiger Grund liegt vor, wenn jemand mit einem von ihm gegebenen Interview in seiner Gesamtheit schlicht unzufrieden ist oder wenn andere Fragen gestellt werden als ursprünglich besprochen. Hiervor bietet allenfalls ein zuvor vereinbarter Autorisierungsvorbehalt Schutz oder eine unmittelbar nach Beendigung des Interviews erfolgende Rücknahme der Einwilligung.

Somit ist festzuhalten, dass bei Vorliegen eines wichtigen Grundes eine Widerrufsmöglichkeit stets gegeben ist. Wird ein Widerruf dagegen vollkommen willkürlich erklärt, sollte es in Anbetracht der bisherigen Rechtsprechung gut vertretbar sein, sich einem Löschungsersuchen zu widersetzen. Hier muss sich der Abgebildete an seiner vormals erteilten Einwilligung festhalten lassen. Als Maßstab für die Bestimmung des „wichtigen Grundes“ sollte man dabei denjenigen wählen, der generell bei der Beurteilung von Persönlichkeitsrechtsverletzungen angewendet wird, und die Widerrufsmöglichkeit deshalb an das Ergebnis einer umfassenden Interessenabwägung knüpfen. Überwiegt das persönlichkeitsrechtliche Interesse des Abgebildeten die Interessen der Hochschule an der Beibehaltung der Aufzeichnung im Internet oder an anderem Ort, sollte eine Widerrufsmöglichkeit bejaht und die Aufzeichnung gelöscht werden. Bei dieser Abwägung kann auch mit einbezogen werden, wie ausführlich der Abgebildete vor Erteilung der Einwilligung aufgeklärt und informiert wurde. Im Zweifel sollte aufgrund des besonderen Gewichts des Persönlichkeitsrechts dem Widerruf der Vorzug gegeben werden.

Konsequenz eines wirksamen Widerrufs der Einwilligung ist, dass es für eine (weitere) Veröffentlichung der Aufnahmen keinen rechtfertigenden Grund mehr gibt, sodass zukünftige Veröffentlichungen/Verbreitungen zu unterlassen und bereits vorgenommene – soweit möglich – rückgängig zu machen bzw. zu löschen sind.

Im Übrigen ist noch anzumerken, dass Verstöße gegen die Vorschriften des KUG zum Recht am eigenen Bild gem. § 33 KUG strafbar sind und mit Geldstrafe oder mit Freiheitsstrafe bis zu einem Jahr geahndet werden können, wobei die Strafverfolgung davon abhängt, dass der Betroffene einen Strafantrag bei den Strafverfolgungsbehörden stellt.

2. Recht am eigenen Wort

Im Hinblick auf das Recht am eigenen Wort gelten weitgehend ähnliche Maßstäbe wie für das Recht am eigenen Bild. Das Recht am eigenen gesprochenen Wort gibt dem Einzelnen das Recht, selbst zu bestimmen, inwiefern Kommunikationsinhalte Dritten zugänglich sein sollen. In diesem Zusammenhang kommt es darauf an, ob es sich um ein öffentlich oder ein nichtöffentlich gesprochenes Wort handelt. Nach wohl einhelliger Meinung ist nur das nichtöffentliche Wort vom Schutzumfang erfasst. Betrifft die Tonaufzeichnung also öffentlich getroffene Äußerungen, ist keine Einwilligung des Aufgezeichneten erforderlich. Insofern liegen beispielsweise Wortbeiträge, die während einer öffentlichen Veranstaltung wie z. B. einer öffentlichen Podiumsdiskussion getätigt werden, bereits von vornherein außerhalb des Schutzbereiches.

Wenn die Äußerungen jedoch in nichtöffentlichem Rahmen getätigt werden, ist für die Zulässigkeit sowohl der Aufnahme als auch der späteren Veröffentlichung eine Einwilligung des Betroffenen unumgänglich. Nichtöffentlich ist der Rahmen, wenn die Äußerung nicht für einen größeren, nach Zahl und Individualität unbestimmten oder nicht durch persönliche oder sachliche Beziehungen miteinander verbundenen Personenkreis bestimmt oder unmittelbar verstehbar ist (Lenckner/Eisele, in: Schönke/Schröder, StGB, München, 29. Aufl. 2014, § 201 Rn. 6). Sind mehrere Personen an einem Gespräch beteiligt, liegt Nichtöffentlichkeit nur dann vor, wenn der Teilnehmer-/Zuhörerkreis eingeschränkt und nicht für beliebige Dritte offen ist. Fehlt die erforderliche Einwilligung, besteht bei Eingriffen in das Recht am eigenen Wort nicht nur eine zivilrechtliche Verantwortlichkeit, sondern der Aufnehmende macht sich auch strafbar gem. § 201 Strafgesetzbuch (StGB; Strafrahmen: Freiheitsstrafe bis zu 3 Jahren oder Geldstrafe).

Ist in einer Hochschulveranstaltung, die nicht öffentlich ist, im Vorhinein deutlich kommuniziert worden, dass eine Aufzeichnung stattfindet, wird man bei Wortmeldungen der Teilnehmer, die in Kenntnis der Aufnahme erfolgen, meist von einer konkludenten Einwilligung zumindest in die Aufnahme ausgehen können. Problematisch ist dies jedoch, wenn es sich um eine Veranstaltung handelt, in der die mündliche Beteiligung Teil einer Prüfungsleistung ist und Eingang in die Leistungsbewertung findet. Hier kann mangels Freiwilligkeit nicht ohne Weiteres von einer konkludenten Einwilligung durch Meldung ausgegangen werden.

Um den Audio-Teil der Aufnahme später auch veröffentlichen zu können, ohne auf eine Einwilligung des Betroffenen angewiesen zu sein, empfiehlt es sich, von Seiten des Dozenten die Frage/Aussage des Teilnehmers noch einmal zusammenzufassen. Dies hat den Vorteil, dass die Wortmeldung des Teilnehmers vor der Veröffentlichung einfach herausgeschnitten werden kann, ohne dass dadurch inhaltliche Lücken entstehen, die zu einer Unverständlichkeit der Aufnahme führen würden. Gleichzeitig ist dies auch für die anderen Teilnehmer hilfreich, da es oft schwierig ist, in größeren Hörsälen die Aussagen der Kommilitonen, die ohne Mikrofon sprechen, akustisch zu verstehen.

Im Übrigen kann hinsichtlich der Anforderungen an die Einwilligung auf die Erläuterungen im Rahmen des Rechts am eigenen Bild verwiesen werden, da die dortigen Voraussetzungen hier in gleicher Weise gelten.

Der Bestand einer Widerrufsmöglichkeit im Hinblick auf das Recht am eigenen Wort ist allerdings in der Rechtsprechung noch nicht eindeutig geklärt und wird vor den Gerichten meistens nur in einem presserechtlichen Kontext relevant. Deshalb gibt es auch kaum Urteile, die generell den Widerruf einer Einwilligung in die Aufzeichnung und Veröffentlichung des nichtöffentlich gesprochenen Wortes ausdrücklich vom Vorliegen eines wichtigen Grundes abhängig machen, wie dies vielfach im Hinblick auf das Recht am eigenen Bild vertreten wird. Eine Ausnahme bildet ein Urteil des Landgerichts (LG) Köln, welches im Jahr 1989 entschieden hat, dass der Widerruf des Einverständnisses in die Ausstrahlung eines gegebenen Interviews entsprechend den Grundsätzen, wie sie beim Widerruf der Einwilligung gemäß § 22 KUG entwickelt worden sind, allenfalls dann in Betracht kommen kann, wenn veränderte Umstände, die sich nach einer zunächst gegebenen Einwilligung ergeben haben, dazu führen würden, dass die Ausstrahlung des Interviews zu einer Verletzung des Persönlichkeitsrechts des Betroffen führen würde (LG Köln, Urteil vom 29.3.1989 - 28 O 134/89). Auch andere Urteile, die sich mit der Frage der Zulässigkeit der Veröffentlichung von Interviews befassen, deuten zumindest mittelbar in diese Richtung.

Aus systematischer Sicht ist hier ein Gleichlauf mit dem Recht am eigenen Bild sinnvoll. Man kann sich also gut auf den Standpunkt stellen, den Widerruf einer Einwilligung in Bild- und Tonaufnahmen nur bei Vorliegen eines wichtigen Grundes

bzw. einer nicht unerheblichen Änderung der Umstände anzuerkennen. Dabei sollte man sich abermals an dem Ergebnis einer umfassenden Interessenabwägung orientieren und im Zweifel dem Persönlichkeitsrecht den Vorrang einräumen, indem man einen Widerruf für zulässig hält. Droht durch die Veröffentlichung einer Äußerung aufgrund veränderter Umstände eine Persönlichkeitsrechtsverletzung des Betroffenen, muss ein Widerruf zulässig sein.

3. Problematik bei Ton- und Videoaufzeichnungen von mehreren Betroffenen

Eine besondere Konfliktlage entsteht, wenn auf einer Aufzeichnung die Abbildungen oder Äußerungen mehrerer Personen enthalten sind. Liegt dann nicht für alle Betroffenen eine Rechtfertigung für die Aufnahme und spätere Veröffentlichung vor, ist fraglich, ob die gesamte Aufnahme zu löschen ist oder nur Teile davon. Eine solche Konstellation kann insbesondere dann eintreten, wenn zuvor ordnungsgemäß Einwilligungen von allen Betroffenen eingeholt wurden und im Nachhinein eine oder mehrere davon ihre Einwilligungen wirksam widerrufen.

Bei der Beurteilung solcher Situationen ist zu differenzieren: Einzelnen Stimmen der Rechtsprechung lässt sich entnehmen, dass es ausreichend ist, diejenige Person unkenntlich zu machen, die ihre Einwilligung widerrufen hat. Hier muss also nicht die gesamte Aufnahme gelöscht werden, sondern kann im Übrigen erhalten bleiben. Ist dies visuell durch Verpixelung oder ähnliche Methoden meist gut zu bewerkstelligen, sollte im Hinblick auf Wortbeiträge in der Regel eine vollständige Löschung stattfinden, an deren Stelle allenfalls eine nachgesprochene inhaltliche (nicht wortgetreue) Wiedergabe der Äußerung treten kann.

Selbst diese Behelfslösung kann jedoch bei Wortbeiträgen unzulässig sein, wenn schon die Aufnahme als solche unbefugt erfolgte, da in diesem Fall der Straftatbestand des § 201 Abs. 2 Nr. 2 StGB einschlägig sein kann. Allerdings steht diese Strafbarkeit der öffentlichen Mitteilung des wesentlichen Inhalts einer unbefugt erstellten Tonaufnahme unter dem Vorbehalt einer Bagatellklausel. Demzufolge erfordert die Strafbarkeit zusätzlich, dass die öffentliche Mitteilung geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen. Hierdurch sollen Gespräche über Belanglosigkeiten wie beispielsweise das Wetter vom strafrechtlichen Schutz ausgenommen werden. Liegt die erforderliche Eignung zur Beeinträchtigung fremder Interessen vor, wird man um eine vollständige Löschung selbst dann nicht umhin kommen, wenn dadurch der Sinnzusammenhang der jeweiligen Aufnahme erheblich beeinträchtigt wird. Eine Rückausnahme gilt nur dann, wenn die öffentliche Mitteilung der wesentlichen Aussageinhalte wiederum zur Wahrnehmung überragender öffentlicher Interessen gemacht wird, was zum Beispiel bei der Aufdeckung schwerwiegender Straftaten der Fall sein kann. Da diese Rückausnahme relativ hohe Anforderungen stellt, wird sie für den Hochschulbereich eher von theoretischem Interesse sein. Deshalb sollten für eine Veröffentlichung generell nur Tonaufnahmen verwendet werden, deren Herstellung in rechtmäßiger Weise erfolgt ist und deren Veröffentlichung auch im Übrigen von einer Einwilligung des Sprechers gedeckt ist.

Zusammenfassend lässt sich festhalten, dass eine solche partielle Unkenntlichmachung einer Aufnahme mehrerer Personen als milderes Mittel im Vergleich zur kompletten Löschung eingeordnet werden kann, welche auch den Interessen der anderen aufgezeichneten Personen bzw. denen des Aufzeichnenden gerecht wird. Dennoch ist darauf hinzuweisen, dass es an gefestigter Rechtsprechung dazu mangelt.

III. Fazit

Ton- und Bildaufnahmen von Personen tangieren regelmäßig das Recht am eigenen Bild sowie das Recht am eigenen Wort und unterliegen damit persönlichkeitsrechtlichen Einschränkungen. Im Hochschulkontext werden entsprechende Aufnahmen nur selten von gesetzlichen Erlaubnistatbeständen gedeckt sein, sodass eine Einwilligung der betroffenen Personen einzuholen ist. Die Einwilligung in Ton- und Bildaufnahmen ist nach herrschender Meinung in der Rechtsprechung formfrei möglich, kann also auch mündlich oder gar konkludent erklärt werden. So kann beispielsweise die freiwillige und bewusste Wahl eines Sitzplatzes in einem deutlich gekennzeichneten Aufzeichnungsbereich im Einzelfall dafür ausreichen, allerdings ist sorgfältig zu prüfen, wie weit eine solche konkludente Einwilligung reicht. Um eine Internetveröffentlichung der gemachten Aufnahmen legitimieren zu können, muss gewährleistet sein, dass dem Betroffenen vorher klar kommuniziert wurde, dass eine solche Veröffentlichung geplant ist. In welcher Form die Einwilligung erteilt wurde, ist nur insofern von Bedeutung, als derjenige, der die Veröffentli-

chung der Aufzeichnungen vornimmt, beweispflichtig für das Vorliegen der Einwilligung und deren Umfang ist. Praktisch ist daher stets die Einholung einer schriftlichen Einwilligung anzuraten.

Ein Widerruf der Einwilligung ist jedenfalls dann möglich, wenn ein wichtiger Grund dafür vorliegt. Ein solcher Grund kann beispielsweise ein Wandel der fundamentalen Überzeugungen des Betroffenen sein. Im konkreten Fall kann über das Vorliegen eines wichtigen Grundes und damit über die Möglichkeit eines Widerrufs der Einwilligung nur nach einer umfassenden Abwägung der betroffenen Interessen abschließend entschieden werden. Überwiegen die persönlichkeitsrechtlichen Interessen des Betroffenen die Interessen der aufnehmenden Hochschule an der Aufrechterhaltung der Veröffentlichung der Aufzeichnung, muss ein Widerruf der Einwilligung möglich sein. Im Zweifel ist hier dem Persönlichkeitsrecht der Vorzug zu gewähren und ein Widerruf zuzulassen. Ist ein Widerruf wirksam erklärt worden, hat der Betroffene unmittelbar einen Anspruch auf Löschung der Aufzeichnungen aus dem Internet sowie auf Unterlassung zukünftiger Veröffentlichungen.

Geht man jedoch mit einem gewissen Augenmaß an diese Problematik heran und informiert potentielle Betroffene einer Aufzeichnung vorab in hinreichendem Umfang, sollte es in der Praxis möglich bleiben, durch verstärkten Einsatz von Videotechnik die Möglichkeiten der Teilhabe an diversen Hochschulveranstaltungen auszuweiten. Dennoch sind auch die Wünsche derjenigen Lehrenden oder Studierenden zu respektieren, die sich mit einer Aufnahme nicht anfreunden können.

Anmerkungen

Siehe hierzu auch:
Franck, „Veröffentlichung von Arbeitnehmerdaten im Internet – Rechtliche Rahmenbedingungen der Verbreitung von Mitarbeiterdaten durch Arbeitgeber“, in: DFN-Infobrief Recht 11/2010
Fischer, „Homepagepflege bei Arbeitnehmerfotos – Landesarbeitsgericht Frankfurt a. M.: Anspruch auf Löschung nach Beendigung des Beschäftigungsverhältnisses“, in: DFN-Infobrief Recht 6/2012

Gut gemeint ist leider doch nicht immer gut genug

Entwicklungen im Zusammenhang mit dem Gesetz gegen unseriöse Geschäftspraktiken und den Redtube-Massenabmahnungen

von Susanne Thinius

Im Dezember 2013 wurde das Gesetz gegen unseriöse Geschäftspraktiken bereits vorgestellt (Thinius, „Gut gemeint – aber auch gut genug?“, Infobrief Recht 12/2013). Über dessen Auswirkungen konnte seinerzeit lediglich gemutmaßt werden. Nach einem guten Jahr kann man eine vorsichtige Bilanz ziehen: demnach bestätigen sich die Mutmaßungen. Denn an der massenhaften anwaltlichen Abmahnpraxis hat sich nicht viel geändert – abgesehen von einigen Ausnahmen.

Hintergrund des Gesetzes und der Massenabmahnungen

Das Gesetz gegen unseriöse Geschäftspraktiken, welches im Oktober 2013 in Kraft trat, sollte all denjenigen dienen, die massenhaft und teilweise zu Unrecht und in völlig überdrehter Höhe abgemahnt wurden, wie im Falle des angeblichen Massen-Streamings über das Portal Redtube, welches erotische und pornographische Inhalte anbietet. Die Regensburger Anwälte Urmann und Kollegen hatten 2013 massenhaft Abmahnungen versandt, wegen angeblicher Urheberrechtsverletzungen durch das Anschauen erotischer Filme über besagtes Portal. Die Betroffenen sollten mitunter 250 € „Strafgebühr“ zahlen (zusammengesetzt aus Rechtsanwaltsgebühren, Telekommunikationspauschale, Schadensersatz und Ermittlungsgebühren) und eine Unterlassungserklärung abgeben. Bei mehreren tausend Betroffenen war das ein gutes Geschäft für die Anwälte, die im Auftrag der Schweizer Archiv AG handelten.

Mit dem Gesetz gegen unseriöse Geschäftspraktiken sollte solch ein Vorgehen unterbunden werden. Denn danach müssen die Abmahngebühren fortan auf 155€ gedeckelt (§ 97a Abs. 3 Urheberrechtsgesetz, UrhG), die Abmahnungen selbst transparenter gestaltet (§ 97a Abs. 2 UrhG) und der fliegende Gerichtsstand abgeschafft werden (§ 104a UrhG). Schadenersatz konnte hingegen weiterhin in voller Höhe verlangt werden – zumindest schwieg das Gesetz dazu.

Rechtssicherheit rund ums Streaming

Die Abmahnwelle entfachte einen bundesweiten Streit darüber, ob Streaming rechtlich wie das illegale Downloaden zu behandeln sei (siehe vertiefend Thinius, „Stream dich ins Unglück“, Infobrief Recht 2/2014). In diesem Zusammenhang gewann die Unterscheidung zwischen Tauschbörse und Streaming-Portal an Relevanz sowie das damit einhergehende Problem, ob eine Zwischenspeicherung der Inhalte im Arbeitsspeicher des Nutzer-Rechners vorgenommen wird oder nicht. Nach wie vor ist rechtlich ungeklärt, wie das Streaming urheberrechtlich geschützter Inhalte zu bewerten ist. Es gibt bislang keine deutschen Urteile, die Streaming als illegal und somit rechtswidrig bewerten. Bislang musste man sich mit den bestehenden Vorschriften der §§ 44a (erlaubt vorübergehende Vervielfältigungshandlungen) und 53 UrhG (Vervielfältigungen zum privaten und sonstigen eigenen Gebrauch) behelfen.

Seit Sommer 2014 gibt es jedoch ein Urteil des Europäischen Gerichtshofes (EuGH, C 360/13), in dem die Richter feststellten, dass das reine Betrachten (inklusive Streaming, RAM-Speiche-

rung, Caching) urheberrechtlich geschützter Werke (also auch Filme) im Web nicht gegen das Urheberrecht verstößt, sofern die Werke weder ausgedruckt noch heruntergeladen werden. Grund hierfür ist die Tatsache, dass die Inhalte lediglich im Browser-Cache zwischengespeichert werden. Konkret heißt es dort, „Art. 5 der Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft ist dahin auszulegen, dass die von einem Endnutzer bei der Betrachtung einer Internetseite erstellten Kopien auf dem Bildschirm seines Computers und im „Cache" der Festplatte dieses Computers den Voraussetzungen, wonach diese Kopien vorübergehend, flüchtig oder begleitend und ein integraler und wesentlicher Teil eines technischen Verfahrens sein müssen, sowie den Voraussetzungen des Art. 5 Abs. 5 dieser Richtlinie genügen und daher ohne die Zustimmung der Urheberrechtsinhaber erstellt werden können".

Dieses Urteil hat Signalwirkung für das deutsche Recht. Es bleibt abzuwarten, wie deutsche Gerichte in Zukunft mit dem Phänomen Streaming umgehen. Zu hoffen bleibt, dass sich hier eine Einheitlichkeit in der deutschen Rechtsprechung zeigt oder klare gesetzliche Regelungen geschaffen werden.

Hat das Gesetz gegen unseriöse Geschäftspraktiken Wirkung gezeigt?

Teils teils, muss hier die Antwort lauten. In der „Porno-Branche" hatten die Massenabmahnungen offensichtlich abschreckende Wirkung. Im Allgemeinen mahnen weniger Anwälte ab, diese wenigen dafür umso häufiger. Jedoch nicht nur wegen Streaming-Vorfällen, sondern vor allem wegen illegalen Downloads. Insbesondere die Münchner Anwaltskanzlei Waldorf Frommer mahnt immer noch regelmäßig ab.

Ferner ist zu beobachten, dass Kanzleien seit Inkrafttreten des Gesetzes gegen unseriöse Geschäftspraktiken überhöhten Schadensersatzforderungen geltend machen, anstatt erhöhte Anwaltskosten, so wie es Kritiker vor Inkrafttreten bereits vermuteten. Es läuft also letztendlich für die Verbraucher auf das Gleiche hinaus. Das Gesetz, welches Verbraucher vor dubiosen Geschäftspraktiken schützen sollte, verfehlt hinsichtlich der Deckelung der Kosten für Abgemahnte seine Wirkung. Auch Schuld sind hieran die Gerichte, da es ihrerseits keine einheitlichen Schadensberechnungen gibt, sondern die Summen meist geschätzt werden und sich daher ein großes Gefälle auftut.

Auch im Hinblick auf die gesetzlichen Ausnahmen von der Deckelung der Abmahnkosten („es sei denn, der Wert ist nach besonderen Umständen unbillig", § 97a Abs. 3 Satz 3 UrhG) besteht weiterhin Rechtsunsicherheit für die Verbraucher. Das zeigt einmal mehr, dass manche Gesetzesinitiativen gut gemeint sind, aber mangels Durchsetzbarkeit und aufgrund von Schlupflöchern im System durchaus ihre Wirkung verfehlen können. Als Lösung wird hier von einigen Seiten ein aktives Tun der Unterhaltungsindustrie gefordert, nämlich durch das vermehrte legale Bereithalten von Inhalten gegen ein geringes Entgelt – wie das beispielsweise bei Netflix oder Spotify der Fall ist.

Bei aller Kritik muss allerdings auch die positive Wirkung des Gesetzes erwähnt werden, und zwar bezüglich der Abschaffung des fliegenden Gerichtsstandes (§ 104a UrhG): hinter dem Begriff verbirgt sich die freie Wahl des Gerichtsortes durch den Kläger– im Zweifel immer dort, wo die Richter zu ihren Gunsten entscheiden. Seit 2013 müssen die Kläger jedoch zum Wohnort der Beklagten fahren. Dies lohnt sich für sie nur dann finanziell, wenn sie bezüglich des Ausgangs der Fälle sicher sind. Zudem garantiert die neue Regelung eine halbwegs ausgeglichene Rechtsprechungspraxis, da die Entscheidungsfindung auf zahlreiche und nicht nur ausgewählte Gerichte verteilt ist. Das beste Beispiel hierfür ist ein Urteil des Amtsgerichts (AG) Köln vom 10.3.2014 (Az. 125 C 495/13), bei welchem die Richter dem Kläger lediglich 10 € Schadensersatz pro verbreitetem Musiktitel unter Bezugnahme auf das Gesetz gegen unseriöse Geschäftspraktiken zusprachen und sich explizit gegen höhere Schadenssummen aussprachen. Es fragt sich an dieser Stelle jedoch, ob das Urteil eines einzigen Gerichts repräsentativ für die Zukunft ist und sich andere Gerichte dem anschließen. Dies bleibt abzuwarten. Eine Evaluierung des Gesetzes durch die Bundesregierung soll noch in diesem Jahr erfolgen.

Freies Wissen für alle?

Das neu eingeführte Zweitveröffentlichungsrecht für Urheber wissenschaftlicher Beiträge

von Philipp Roos

Die Diskussionen über eine Anpassung des Urheberrechts an das digitale Zeitalter sind weiterhin in vollem Gange. Zu den wesentlichen Herausforderungen zählt es dabei auch, die infolge des digitalen Wandels entstandenen Bedürfnisse der Wissenschaft im geltenden Urheberrecht zu berücksichtigen. Hier prallen die Interessen der Universitäten und Länder mit den Interessen der wissenschaftlichen Verlage aufeinander. Dem Gesetzgeber kommt insofern die Aufgabe zu, die gegensätzlichen Positionen in einen Ausgleich zu bringen. Nunmehr existiert seit dem 1.1.2014 ein sog. Zweitveröffentlichungsrecht im Urheberrechtsgesetz, das für Urheber wissenschaftlicher Publikationen gilt. Dieses soll den Weg für „Open Access" – frei verfügbares Wissen im Internet – freimachen.

I. Hintergründe und Zielsetzung

Die Wissenschaftsvertreter klagen seit jeher über die Beschränkungen, die das Urheberrecht der Lehre und Forschung auferlegt. Dass es in Anbetracht der Digitalisierung tatsächlich Anpassungen und Überarbeitungen des Urheberrechts bedarf, hat auch der Gesetzgeber wahrgenommen. Insbesondere das „Zweite Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft" (sog. Zweiter Korb), dessen Regelungen zum 1. Januar 2008 in Kraft traten, enthielt einige bemerkenswerte Neuregelungen mit Bedeutung für Wissenschaft und Forschung. Damit setzte die Bundesrepublik Deutschland die EG-Richtlinie zur „Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft" (sog. InfoSoc-Richtlinie) um. Wie die entsprechenden Normen auszulegen sind, beschäftigte die Gerichte in letzter Zeit besonders intensiv.

So gab es im September 2014 erfreuliche Nachrichten für die Wissenschaftsvertreter, als der Gerichtshof der Europäischen Union (EuGH) den Weg für digitale Leseplätze in Hochschulbibliotheken weitgehend ebnete (s. dazu Roos, Weniger Papier ist mehr! – Europäischer Gerichtshof macht den Weg für digitale Leseplätze frei, DFN-Infobrief Recht 11/2014; Roos, Bibliothek 2.0: Alles digital, oder was? – Schlussanträge des Generalanwalts des Europäischen Gerichtshofs zur Auslegung der Bibliotheksschranke, DFN-Infobrief Recht 8/2014). In absehbarer Zeit wird der Bundesgerichtshof (BGH) wieder zu digitalen Leseplätzen entscheiden und die Vorgaben des obersten europäischen Gerichts umsetzen müssen. Konkret geht es um die Auslegung der Norm des § 52b Urheberrechtsgesetz (UrhG), der sog. Bibliotheksschranke.

Eine andere vielbeachtete Entscheidung erging hinsichtlich § 52a UrhG, der sog. Bildungsschranke. Die Bildungsschranke trifft Bestimmungen über den Umgang mit urheberrechtlich geschützten Werken, die Dozenten im Rahmen ihres Unterrichts im Internet hochladen möchten. Zwar rief diese Entscheidung des BGH nicht nur Applaus aus den Kreisen der Wissenschaft hervor, jedoch wurden die Gesetzesmerkmale der Norm immerhin weiter konkretisiert (s. dazu Hinrichsen, Ende gut, alles gut? – Die unendliche Geschichte des § 52a UrhG. Bundesgerichtshof konkretisiert offene Fragen bei sog. Bildungsschranke, DFN-Infobrief Recht 2/2014).

Nach langen Diskussionen innerhalb der beteiligten Kreise und in den Gesetzgebungsorganen existiert seit dem 1.1.2014 eine neue urheberrechtliche Bestimmung mit Hochschulbezug, die auch neue Auslegungsfragen hervorruft. In § 38 Abs. 4 UrhG

ist ein Zweitveröffentlichungsrecht für die Urheber wissenschaftlicher Publikationen vorgesehen. Dort heißt es:

„Der Urheber eines wissenschaftlichen Beitrags, der im Rahmen einer mindestens zur Hälfte mit öffentlichen Mitteln geförderten Forschungstätigkeit entstanden und in einer periodisch mindestens zweimal jährlich erscheinenden Sammlung erschienen ist, hat auch dann, wenn er dem Verleger oder Herausgeber ein ausschließliches Nutzungsrecht eingeräumt hat, das Recht, den Beitrag nach Ablauf von zwölf Monaten seit der Erstveröffentlichung in der akzeptierten Manuskriptversion öffentlich zugänglich zu machen, soweit dies keinem gewerblichen Zweck dient. Die Quelle der Erstveröffentlichung ist anzugeben. Eine zum Nachteil des Urhebers abweichende Vereinbarung ist unwirksam."

§ 38 Abs. 4 UrhG wurde im Zuge des „Gesetzes zur Nutzung verwaister und vergriffener Werke und weiteren Änderungen des Urheberrechtsgesetzes" (BT-Drucks. 17/13423) in den Gesetzestext aufgenommen. Ziel der Norm ist es, die Potenziale des Internets für die digitale Wissensgesellschaft auszunutzen und für einen möglichst ungehinderten Wissensfluss zu sorgen. So sollen Forschungsergebnisse frei verfügbar sein, um auf Basis dieser Ergebnisse weiter forschen zu können.

Wesentlicher Beweggrund des Gesetzgebers, § 38 Abs. 4 UrhG einzufügen, ist das vertragliche Ungleichgewicht zwischen den Autoren wissenschaftlicher Beiträge und den Wissenschaftsverlagen. Auf dem teilweise quasi-monopolistischen Markt wissenschaftlicher Verlage sind die Autoren wissenschaftlicher Werke vielmals derart auf die Verlage angewiesen, dass die Verlage die Vertragsbedingungen frei vorgeben können und sich sämtliche ausschließlichen Nutzungsrechte – insbesondere auch für den Onlinebereich – einräumen lassen. Zugleich sind die Verlagsprodukte dann aber finanziell so kostspielig, dass die Bibliotheken kaum wissen, wie der Erwerb relevanter Literatur finanziert werden soll. Das gilt vor allem für die Bereiche Naturwissenschaft, Technik und Medizin. Hinter der Norm steht daher auch ein monetärer Beweggrund, der darin liegt, den Effekt der Doppelfinanzierung zu vermeiden: Werden die Forschungen schon aus öffentlicher Hand finanziert, erfordert der Status quo auch die Anschaffung der publizierten Forschungsergebnisse und damit den Einsatz von Steuergeldern. Das soll nun – zumindest im Bereich der wissenschaftlichen Zeitschriften und unter den gesetzlichen Einschränkungen (dazu sogleich) – begrenzt werden. Das Stichwort lautet Open Access, also freier Zugang zu wissenschaftlicher Literatur im Internet.

Der Gesetzgeber sah es als gebotene Lösung an, ein unabdingbares Zweitveröffentlichungsrecht im Urhebervertragsrecht (§§ 31 ff. UrhG) zu normieren. Es handelt sich gesetzestechnisch also nicht um eine urheberrechtliche Schranke (wie bspw. bei den angesprochenen §§ 52a, 52b UrhG), die eine erlaubnisfreie Nutzung des Werkes durch einen bestimmten Personenkreis oder die Allgemeinheit erlaubt. Vielmehr bestimmt der Urheber, ob er – im Falle des Vorliegens der Voraussetzungen – von seinem Zweitveröffentlichungsrecht Gebrauch macht.

II. Wissenschaftlicher Beitrag im Sinne von § 38 Abs. 4 UrhG

Das Zweitveröffentlichungsrecht des Urhebers gilt jedoch nicht für alle publizierten Beiträge von Wissenschaftlern und Forschern. Im Wesentlichen müssen drei Grundvoraussetzungen erfüllt sein, damit § 38 Abs. 4 UrhG zugunsten des Urhebers eingreift:

- Es muss sich um einen wissenschaftlichen Beitrag handeln.
- Die Entstehung des Beitrags ist im Rahmen einer mindestens zur Hälfte mit öffentlichen Mitteln geförderten Forschungstätigkeit entstanden.
- Der Beitrag erschien in einer periodisch erscheinenden Sammlung.

Keine allzu großen Probleme bereitet die Feststellung, ob es sich um einen wissenschaftlichen Beitrag handelt. Die Norm verlangt zunächst, dass ein urheberrechtlich geschütztes Werk vorliegt. Solche urheberrechtlich geschützten Werke führt § 2 Abs. 1 UrhG beispielhaft auf. Als „wissenschaftlicher Beitrag" kommen vor allem Texte (Sprachwerke) in Frage. Zu denken ist aber auch an wissenschaftliche oder technische Darstellungsformen, etwa Zeichnungen, Pläne, Karten, Skizzen und Tabellen. Diese müssen jeweils als persönliche geistige Schöpfungen zu qualifizieren sein, was sich in aller Regel bereits aus ihrer individuellen Gedankenführung oder Darstellungsform ergibt. Das Merkmal der „Wissenschaftlichkeit" wird im Urheberrecht sehr weit ausgelegt – auch einfachste wissenschaftliche Erkenntnisse sind davon umfasst.

Schon genauer untersucht werden muss, ob der Beitrag im Rahmen einer Forschungstätigkeit entstanden ist. Eine Forschungstätigkeit liegt immer dann vor, wenn nicht ausschließlich didaktische Inhalte vermittelt werden. Damit dürften in aller Regel selbst Klausurmusterlösungen als Forschungstätigkeit gelten, da es hier nicht ausschließlich um das „Wie" des Lehrens geht, sondern konkreter Lehrstoff aufbereitet wird. Etwas unklar ist, unter welchen Bedingungen der Beitrag als „im Rahmen" der Forschungstätigkeit entstanden gilt. Das Merkmal könnte sowohl zeitlich als auch inhaltlich verstanden werden. Die besseren Gründe sprechen jedoch dafür, „im Rahmen" als inhaltliches Kriterium zu begreifen. Daraus folgt, dass die jeweilige Publikation nicht während der Laufzeit der Forschung veröffentlicht werden muss. Ein gegenteiliges Verständnis würde die Norm in einem Maße beschränken, das ihrem Zweck zuwider liefe. Da regelmäßig Forschungsergebnisse und nicht bloß Zwischenstände publiziert werden, würde sonst die weit überwiegende Anzahl von Publikationen aus dem Anwendungsbereich der Norm herausfallen. Insofern ist lediglich zu verlangen, dass der Beitrag im unmittelbaren inhaltlichen Zusammenhang mit der jeweiligen Forschungstätigkeit steht.

Ein weiteres von der Publikation zu erfüllendes Kriterium liegt darin, dass sie im Rahmen einer zumindest zur Hälfte mit öffentlichen Mitteln geförderten Forschungstätigkeit entstanden sein muss. Blickt man auf das hitzig geführte Gesetzgebungsverfahren und vorangegangene in der Diskussion befindliche Formulierungsvorschläge, wird ersichtlich, dass es sich hierbei um eine den Anwendungsbereich beschränkende Voraussetzung handelt. Es sind ausschließlich Forschungstätigkeiten erfasst, die im Rahmen der öffentlichen Projektförderung oder an einer institutionell geförderten außeruniversitären Forschungseinrichtung durchgeführt werden. Der Gesetzgeber geht davon aus, dass hier ein weitergehendes öffentliches Interesse an den Forschungsergebnissen besteht als bei rein universitärer Forschung. Rein universitäre Forschung und deren Ergebnisse sind somit nämlich vom Zweitveröffentlichungsrecht ausgenommen. Der Bundesrat, aber auch die juristische Literatur üben scharfe Kritik an dieser Limitierung des Zweitveröffentlichungsrechts und plädieren für eine verfassungskonforme Auslegung. Durch eine verfassungskonforme Auslegung soll das gesamte wissenschaftliche Personal erfasst sein. Der Kritik ist darin beizupflichten, dass die Norm tatsächlich zu einer Ungleichheit führt, deren angeführter sachlicher Grund nicht zu überzeugen vermag. Auch die universitäre Forschung kann einen erheblichen Beitrag für die Forschung leisten, ohne dass es auf weitere Geldgeber ankommt. Rechtssicherheit verspricht derzeit allerdings nur eine öffentliche Zugänglichmachung von Artikeln, die im Rahmen von Drittmittelprojekten oder an außeruniversitären Einrichtungen entstanden sind.

Der wissenschaftliche Beitrag muss des Weiteren in einer periodisch mindestens zweimal jährlich erscheinenden Sammlung erschienen sein. Darunter können alle wissenschaftlichen Zeitschriften verstanden werden. Nicht umfasst sind – zumindest in aller Regel – Schriftenreihen, Monographien, Kommentare oder Tagungsbände. Außerdem ist zu beachten, dass die Sammlung unter Geltung des Zweitveröffentlichungsrechts erschienen sein muss – also frühestens am 1.1.2014.

III. Einschränkungen

Sollte die wissenschaftliche Publikation als Werk i.S.d. § 38 Abs. 4 UrhG bewertet werden können, müssen in einem nächsten Schritt die von der Norm vorgegebenen Einschränkungen beachtet werden. Diese Einschränkungen dienen überwiegend den Interessen der Wissenschaftsverlage und verfolgen das Ziel eines Interessenausgleichs.

Eine wesentliche Einschränkung ergibt sich daraus, dass die Zweitveröffentlichung keinem gewerblichen Zweck dienen darf. Es dürfen folglich keine Honorarzahlung oder andere geldwerte Vorteile eingestrichen werden. Im Übrigen darf auch das Webangebot, wo die Zweitveröffentlichung erfolgt, keinen gewerblichen Zweck verfolgen. Diese Feststellung kann in manchen Fällen schwierig sein, etwa wenn das Webangebot von einem (anderen) Verlag mit kostenfreiem Zugang betrieben wird. Hier stellt sich bereits die Frage, ob der Autor nicht gegen vertragliche Nebenpflichten verstößt, wenn er das Werk dort hochlädt. Letztlich sind die Universitäten gefragt: Diese sollen – nach der Vorstellung des Gesetzgebers – entsprechende Portale einrichten und etablieren. Die Intention des Autors muss es sein, der Wissenschaft und Allgemeinheit die Forschungsergebnisse zur Förderung weiterer Forschung zur Verfügung zu stellen.

Der Gesetzgeber hat zudem eine Sperrfrist für die Ausübung des Zweitveröffentlichungsrechts in das Gesetz aufgenommen. Diese beträgt zwölf Monate ab dem Zeitpunkt der Veröffentlichung. Hierbei handelt es sich abermals um ein

Zugeständnis an die Verleger, die die mit der Publikation verbundenen Kosten zunächst amortisieren können sollen. Insofern können Autoren frühestens seit dem 1.1.2015 erstmals von ihrem möglichen Zweitveröffentlichungsrecht Gebrauch machen.

Der Beitrag darf lediglich in der akzeptierten Manuskriptversion öffentlich zugänglich gemacht werden. Folglich dürfen keine Kopien oder Scans des Artikels, wie er in der Sammlung erschienen ist, eingestellt werden. Das vom jeweiligen Verlag genutzte Layout darf nicht genutzt und somit dürfen auch keine Druckfahnen zur Verfügung gestellt werden. Allerdings ist es zulässig – und wegen der Zitierfähigkeit des Beitrags sogar geboten –, kenntlich zu machen, welcher Seitenzahl der jeweilige Abschnitt zugeordnet werden kann. Dies kann durch Seitenumbrüche oder ähnliche Funktionen von Textverarbeitungsprogrammen erreicht werden. Weiterhin dürfen und sollten mit dem Verlag abgestimmte Änderungen und Überarbeitungen in das hochgeladene Manuskript eingearbeitet sein, um Unstimmigkeiten zwischen dem in der Sammlung erschienenen und dem öffentlich zugänglichen Dokument zu vermeiden.

IV. Fazit

Sind sämtliche der Voraussetzungen erfüllt und werden die Einschränkungen berücksichtigt, ist der Weg für eine Zweitveröffentlichung frei. „Open Access“ kann somit Einzug in die deutsche Wissenschaft halten. Die Manuskripte können zur freien Verfügung in das Internet hochgeladen werden.

Mit § 38 Abs. 4 UrhG existiert eine neue Vorschrift, die das Urheberrecht an das digitale Leben anpassen soll und der Wissenschaftsförderung dient. Es handelt sich dabei um eine Kompromisslösung, mit der sowohl Wissenschaftler als auch Verlage leben können. Ärgerlich ist jedoch die Beschränkung auf im Rahmen außeruniversitärer Forschung oder von Drittmittelprojekten entstandener Beiträge. Dies sorgt neben der beschränkten Verfügbarkeit der Forschungsergebnisse zugleich für eine vermeidbare Ungleichbehandlung der Hochschulmitarbeiter, deren sachliche Begründung nicht zu überzeugen vermag.

Der Spielball liegt nun bei den Ländern und Universitäten. Diese haben entsprechende Plattformen zu errichten, die es Wissenschaftlern ermöglichen, ihre Beiträge fachbezogen und ohne großen Aufwand zur freien Verfügung zu stellen. Weiterhin müssen diese Portale so strukturiert sein, dass die Werke seitens der Nutzer auch unkompliziert aufgefunden werden können. Es ist daher an die Universitäten zu appellieren, sich möglichst rasch dem Aufbau entsprechender Strukturen zu widmen. Das zu verfolgende Ziel muss eine „One-stop-Plattform“ sein, auf der sämtliche Werke aufzufinden sind. Eine Zersplitterung sollte vermieden werden, will man das hart erkämpfte Zweitveröffentlichungsrecht nicht selbst entwerten. Denkbar sind auch fachbezogene Portale, die jedoch mit einer großen Open-Access-Suchplattform kombiniert werden könnten.

Weiterhin muss die „frohe Kunde“ auch an die Hochschulmitarbeiter herangetragen werden. Nur Hochschulmitarbeiter, die sich der neuen Rechtslage bewusst sind, können und werden ihr Zweitveröffentlichungsrecht auch tatsächlich nutzen. Die Justiziariate sind daher aufgerufen, entsprechende Schulungen und Checklisten zu erstellen. Insbesondere die Nachricht, dass es sich bei dem Zweitveröffentlichungsrecht um ein unabdingbares Recht handelt – also ein Recht, das der Verlag nicht ausschließen oder einschränken kann –, muss sich bei den Wissenschaftlern verbreiten.

Noch steht „Open Access“ in der Hochschullandschaft am Anfang – sofern Universitäten, Hochschulmitarbeiter und Nutzer die Chancen des Zweitveröffentlichungsrechts nutzen, könnte es jedoch nicht weniger als den Startschuss für einen einschneidenden Wandel in der Wissensverbreitung bedeuten.

Die rechtlichen Herausforderungen von „Bring Your Own Device“ – Lifestyle contra Sicherheit

Teil 1: Allgemeines, Sicht der Aufsichtsbehörden, Haftungsrecht

von Kevin Kuta

Die Rechenleistung und Komplexität mobiler Endgeräte ist in den letzten Jahren derart gestiegen, dass sie mit herkömmlichen PCs mithalten oder diese sogar leistungstechnisch übersteigen. Überall und jederzeit ist damit der Zugriff auf lokale Anwendungen und Daten möglich, meist auch mit einer direkten Verbindung zum Internet. Gleichzeitig bieten die Cloud-Technologien einen nahezu unbegrenzten Zugang auf global gespeicherte Daten über diese Geräte. Neben der Wirtschaft hat auch die öffentliche Verwaltung die vielfältigen und flexiblen Möglichkeiten dieser Geräte für sich entdeckt. Mitarbeitern ist eine gewohnte und einfache Arbeitsumgebung sehr wichtig. Nirgends können sie derartige Umstände besser vorfinden als auf ihren eigenen Endgeräten. Es stellt sich daher die Frage, welche rechtlichen Probleme bei der Nutzung privater Endgeräte zu dienstlichen Zwecken („Bring Your Own Device“, kurz „BYOD“) bestehen.
Dieser Beitrag stellt den ersten Teil einer Reihe zu diesem Themenkomplex dar, wobei zunächst allgemeine Fragen besprochen, die Sicht der Aufsichtsbehörden dargestellt und haftungsrechtliche Gesichtspunkte erörtert werden. Am Ende der Darstellung des jeweiligen Rechtsgebietes werden Handlungsempfehlungen beschrieben, die gleichzeitig als eine Art Checkliste genutzt werden können.

I. Begriffsbestimmung

Unter „Bring Your Own Device“ (kurz: BYOD) versteht man die Einbringung und Einbindung privater IT-Endgeräte des Arbeitnehmers für die dienstliche Nutzung beim Arbeitgeber. Abweichend von der strikten Übersetzung des Wortes „Device“ mit „Gerät“ muss ein umfassendes Verständnis des Device-Begriffes angelegt werden, sodass neben IT-Endgeräten auch Softwares, Applikationen, Datenbanken, Services und ähnliches von diesem Begriff umfasst sind. Teilweise werden die Begriffe „Bring Your Own Device“ und „Consumerization of IT“ parallel verwendet. Im Detail beschreiben sie jedoch unterschiedliche Phänomene. Mit „Consumerization of IT“ ist die beliebte und steigende Nutzung von leicht bedienbaren und für den privaten Bereich optimierten mobilen Endgeräten (Consumer-Grade-Geräte wie Notebooks, Tablets oder Smartphones) im Privatbereich sowie in allen Ebenen eines Unternehmens bis in die Führungsetagen gemeint. Demgegenüber drückt „Bring Your Own Device“ die bewusste strategische Entscheidung aus, dass private Endgeräte für die dienstliche Nutzung zugelassen werden.

Die Initiative für die Einbringung der privaten Endgeräte in die IT-Landschaft des Arbeitgebers kann sowohl von diesem selbst als auch vom Arbeitnehmer ausgehen. Aktuell nutzen etwa

70% der Arbeitnehmer in Deutschland eigene IT-Endgeräte für dienstliche Zwecke am Arbeitsplatz. Am häufigsten werden dabei Personal Computer oder Laptops genutzt (45%), gefolgt von Smartphones (30%) und weiteren Geräten. Knapp 20% der von dem Phänomen „BYOD" betroffenen Unternehmen gewähren den privaten Endgeräten dabei (in Teilen sogar uneingeschränkten) Zugriff auf die dienstliche IT-Infrastruktur. Eine Vielzahl von Unternehmen (etwa 40%) möchte laut einer Umfrage sogar bis zum Jahr 2016 vollständig und verpflichtend auf „BYOD" umsteigen. Neben dem Cloud Computing handelt es sich bei „BYOD" nach den Aussagen vieler Experten um den nächsten Megatrend in der IT-Branche. Der Einsatz privater Endgeräte für dienstliche Zwecke wird in den nächsten Jahren vermutlich weiter zunehmen. Eine langfristige Durchsetzung hängt aber wahrscheinlich in erster Linie davon ab, inwieweit die (vor allem rechtlichen) Umsetzungsschwierigkeiten gelöst werden können.

II. Ausgangslage und Effekte

Es stellt sich natürlich die Frage, wie es zu diesem Trend der Einbringung eigener Endgeräte am Arbeitsplatz kommt. Die IT in Unternehmen sowie der öffentlichen Verwaltung ist oftmals veraltet und dementsprechend langsamer als der auf dem Markt übliche Standard, sodass als einer der Hauptbeweggründe für die Umsetzung von „BYOD" in der technischen Überlegenheit und Aktualität der privaten IT zu sehen ist. Gleichzeitig werden die vom Arbeitgeber auferlegten (und in den meisten Fällen auch notwendigen) Sicherheitsmaßnahmen vom Arbeitnehmer als Behinderung wahrgenommen. Die Entwicklung bei mobilen Endgeräten, insbesondere im Smartphone- und Tablet-PC-Sektor, schreitet schnell voran. Dementsprechend wollen die Mitarbeiter ihre privaten leistungsfähigeren und nutzerfreundlicheren Endgeräte einsetzen. Sie können ihre eigene, bekannte Hardware benutzen und müssen nicht noch ein weiteres, bisher fremdes Gerät verwenden, sodass eine Umgewöhnung auf eine komplett neue Hard- und Software vermieden wird, was auch einen sinkenden Schulungsbedarf für den Arbeitgeber zur Folge hat.

Auf diese Weise ist sogar eine Kombination von dienstlichen und privaten Aufgaben möglich. Berufliche und private Kontakte können mittels eines Gerätes unkompliziert gepflegt werden. Dies kann eine erhöhte Motivation der Beschäftigten zur Folge haben und gleichzeitig die Effizienz und Produktivität merklich steigern. Auch können sich dadurch Auswirkungen auf die Außendarstellung und Attraktivität des Arbeitgebers ergeben, da er so flexibler und mitarbeiterfreundlicher erscheint. Die erhöhte Zufriedenheit der Mitarbeiter und die gesteigerte Identifikation mit dem Arbeitgeber können neben einer erhöhten Produktivität zudem eine erhöhte Erreichbarkeit mit sich bringen. Gleichzeitig können für ihn Einsparungspotentiale entstehen, da der Arbeitgeber deutlich weniger Hardware anschaffen muss. Dieses letztgenannte Argument kann sich aber auch (wie einige Beispiele in den letzten Jahren beweisen) als Trugschluss erweisen, da durch den erhöhten Managementbedarf der mitarbeitereigenen Endgeräte sowie mögliche Ausgleichszahlungen an die Arbeitnehmer für die Einbringung der eigenen Endgeräte nicht zu unterschätzende Kosten entstehen.

Mit der Durchmischung von dienstlicher und privater Hardware sowie Daten gehen neben den Wohlfühl-Faktoren aber auch erhebliche Gefahren einher. Neben rechtlichen Vorkehrungen, wobei hier insbesondere der Datenschutz zu nennen ist, müssen technische Rahmenbedingungen geschaffen werden. Entscheidet sich ein Arbeitgeber für die Einführung von „BYOD", muss eine Gesamtstrategie unter Berücksichtigung sämtlicher Umstände des Einzelfalls entwickelt werden. Nur auf diese Weise kann man die rechtlichen und technischen Hürden angemessen überwinden.

III. Sicht der Aufsichtsbehörden

Obwohl sich die Länder nur sehr verhalten zum Thema „BYOD" äußern, ist die Meinung der einzelnen Aufsichtsbehörden der Länder zu diesem Thema recht einheitlich: Eine rechtssichere Handhabe der dienstlichen Nutzung von privaten Endgeräten ist nur äußerst schwer bis gar nicht möglich.

ULD Schleswig-Holstein

Das Unabhängige Zentrum für Datenschutz (ULD) Schleswig-Holstein hat sich im Jahre 2009 zu dieser Thematik geäußert. Danach sei die konsequente Einhaltung technisch-organisatorischer Maßnahmen auf privaten Endgeräten nicht möglich. Der Einsatz privater Endgeräte zur Verarbeitung dienstlicher Daten sei weder im einschlägigen Landesdatenschutzgesetz (LDSG) noch in der Landesdatenschutzverordnung (DSVO) vorgesehen und daher grundsätzlich unzulässig. Die Gewährleistung einer ordnungsgemäßen Ausgestaltung der Hardware, von Art und Umfang der zulässigen Nutzung sowie

einer effektiven Kontrolle der technischen und organisatorischen Sicherheitsmaßnahmen anhand der IT- und Sicherheitskonzepte der datenverarbeitenden Stelle sei nicht wirksam möglich. Die Verarbeitung personenbezogener dienstlicher Daten beim Einsatz privater Endgeräte sei nur ausnahmsweise mit sog. „Terminalserverdiensten" möglich, wobei spezielle technische und organisatorische Sicherheitsmaßnahmen notwendig seien. Mittels einer derartigen Lösung wird neben der Authentifizierung am privaten Endgerät eine weitere Authentifizierungs- und Autorisierungsebene eingefügt, mit der eine Terminalserversitzung separat aufgebaut wird, sodass im Ergebnis nur Bildschirminhalte übertragen werden, die Dateien jedoch zu jeder Zeit auf dem Server der datenverarbeitenden Stelle bleiben.

Mecklenburg-Vorpommern

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern empfiehlt nachdrücklich nur behördeneigene Geräte einzusetzen, da nur auf diese Weise eine Umsetzung der rechtlichen Vorgaben mit einem angemessenen Arbeitsaufwand möglich sei. Zudem wird zu einer sorgfältigen Planung und möglichst restriktiven Handhabung von mobilen Endgeräten hinsichtlich des Zugriffs dieser Geräte auf die Behördeninfrastruktur geraten. „BYOD" führe zu erheblichen Sicherheitsrisiken und sei eine schwere Aufgabe für die einzelnen Abteilungen der öffentlichen Verwaltung. Voraussetzung für eine Nutzung privater Endgeräte zu dienstlichen Zwecken sei eine geeignete Administrationsumgebung, mittels derer die dienstliche und private Nutzung getrennt und gleichzeitig die nutzerseitigen Administrationsmöglichkeiten wirksam verhindert oder zumindest erheblich eingeschränkt werden.

Hessen

Der Hessische Datenschutzbeauftragte hält die rechtlichen und technischen Probleme im Zuge des Einsatzes von spezifisch mitarbeitereigener Hardware zurzeit für unüberwindbar. In erster Linie sei eine Trennung von beruflicher und privater Ebene zwingend erforderlich, wobei aber eine Prüfung durch eine unabhängige Stelle zu erfolgen habe, ob die derzeit verfügbaren Produkte und technischen Ansätze eine wirksame Trennung der beiden Ebenen sicherstellen können. Zum gegenwärtigen Zeitpunkt könnten nur solche dienstliche Daten auf privaten Endgeräten verarbeitet werden, die zwangsläufig in den privaten Bereich des Mitarbeiters ausstrahlen, wie etwa Termine. Es müsse eine weitestgehende Reduzierung des Datenumfangs erfolgen. Gleichzeitig müsse gewährleistet werden, dass bei einer unbefugten Kenntnisnahme durch Dritte keine Beeinträchtigungen für die Betroffenen im Hinblick auf ihre gesellschaftliche Stellung oder wirtschaftlichen Verhältnisse zu erwarten sei.

Berlin

Nach dem Berliner Beauftragten für Datenschutz und Informationsfreiheit müsse das Phänomen „BYOD" weiter beobachtet werden. Die Probleme, Bedrohungen und Sicherheitsmaßnahmen seien einerseits bekannt, andererseits würden Lösungen dafür bereits eingehend diskutiert. Es bedürfe einer Kombination verschiedener rechtlicher und technischer Maßnahmen zur Beherrschung der durch die Nutzung von privaten Endgeräten im dienstlichen Umfeld entstehenden Risiken. Es wird in diesem Zuge eindringlich vor den Gefahren von „BYOD" gewarnt. Gleichzeitig hat der Berliner Beauftragte für Datenschutz und Informationsfreiheit die Einführung von „BYOD" für den Bereich der öffentlichen Verwaltung für unzulässig erklärt bzw. für eine Zulassung in der öffentlichen Verwaltung nur in absoluten Ausnahmefällen plädiert.

Düsseldorfer Kreis

Der Düsseldorfer Kreis, ein Gremium bestehend aus den obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen (= privaten) Bereich, hat die Problematik zwar bereits erkannt, jedoch noch keine gemeinsame Stellungnahme abgegeben. Bisher existiert nur ein Beschluss dieses Gremiums über die datenschutzgerechte Nutzung von Smartphones, wobei nicht auf die Besonderheiten von „BYOD" eingegangen wird.

Bundesamt für Sicherheit in der Informationstechnologie (BSI)

Seitens des Bundesamtes für Sicherheit in der Informationstechnologie wurde im Hinblick auf „BYOD" ein Papier angekündigt. Es ist auch zu erwarten, dass dieses Thema sowie Maßnahmenempfehlungen dazu in den Grundschutzkatalog des BSI Einzug nehmen werden. Dahingehende Maßnahmen sind zum gegenwärtigen Zeitpunkt jedoch noch nicht erfolgt.

IV. Haftungsrecht

Im Schadens- bzw. Haftungsrecht müssen zwei Problemkreise auseinander gehalten werden. Auf der einen Seite stehen sensible Daten des Arbeitgebers. In diesem Punkt steckt aufgrund der Zugriffsmöglichkeit Dritter ein hohes Gefahrenpotential. Auf der anderen Seite stehen die eingebrachten Endgeräte des Arbeitnehmers. Sobald der Arbeitnehmer mit Zustimmung des Arbeitgebers private Geräte für dienstliche Zwecke ins Unternehmen einbringt oder der Arbeitgeber eine solche Vorgehensweise zumindest duldet, trifft ihn eine Schutzpflicht für das vom Arbeitnehmer eingebrachte Eigentum. Außerdem ist der Mitarbeiter nicht zur Ersatzbeschaffung defekter oder verloren gegangener Geräte verpflichtet. Neben diesen zwei Problemkreisen kann auch der private Internetanschluss des Mitarbeiters einige Problemherde eröffnen.

Datenbestände des Arbeitgebers

In der heutigen Zeit sehen sich Arbeitgeber mit einer Vielzahl von Daten konfrontiert, wobei es sich sowohl um eigene Daten, als auch solche von Dritten handeln kann. Durch den Einsatz privater Endgeräte besteht die Gefahr, dass Dritte Zugriff auf betriebliche Datenbestände erlangen. Dabei kann es sich um Angehörige aus dem Familien- und Bekanntenkreis handeln, jedoch kommen auch fremde Personen in Betracht, etwa im Falle eines Diebstahls. Zwar ist die Kenntnisnahme als solche schon äußerst problematisch, beispielsweise vor dem Hintergrund des Datengeheimnisses. Die Löschung von Daten stellt aber den „worst case“ bei der Zugriffsmöglichkeit durch dritte Personen dar, wobei dies umso wahrscheinlicher wird, wenn Kinder auf die dienstlichen Daten zugreifen können. Diese gesamte Problematik wird noch gravierender, wenn die Daten dem Arbeitgeber von einem Dritten zur Be- oder Weiterverarbeitung überlassen wurden.

Oftmals bieten private Sicherheitssoftwares (wie etwa Antivirenprogramme oder Firewalls) im Vergleich zu Varianten für den gewerblichen bzw. geschäftlichen Bereich einen geringeren Schutz und sind zudem nicht auf die Verwendung im dienstlichen Rahmen abgestimmt und eingestellt. Dadurch entsteht die Gefahr der Infektion des privaten Geräts mit Schadsoftware. Sofern dieses Gerät, wie häufig im Rahmen von „BYOD“, auch noch gänzlich in die dienstliche IT-Infrastruktur eingebunden ist, ist die Wahrscheinlichkeit deutlich größer, dass auch diese Systeme infiziert werden. Daneben besteht die Gefahr der Ausspähung von Betriebs- und Geschäftsgeheimnissen sowie des Datenverlustes. Private Applikationen können unbemerkt auf dienstliche Daten zugreifen und so neben geheimhaltungsbedürftigen Informationen auch E-Mail-Bestände oder Kontaktdaten auslesen. In diesem Zusammenhang ist insbesondere das unter technisch versierten Mitarbeitern verbreitete „Jailbreak“ bzw. „Jailbreaking“ eine Bedrohung für die dienstlichen Systeme, da durch die Aufhebung der herstellerseitigen Sperrung bestimmter Funktionen und deren anschließender Veränderung viele Einfallstore für Angriffe geschaffen werden.

Hinzu kommt, dass im Schadensfall (etwa bei einem Datenverlust) möglicherweise nur eine beschränkte Haftung des Arbeitnehmers besteht. In diesem Falle finden nämlich die arbeitsrechtlichen Grundsätze des innerbetrieblichen Schadensausgleichs Anwendung. Daraus ergibt sich eine abgestufte Arbeitnehmerhaftung, die vom jeweiligen Verschuldensgrad des Arbeitnehmers abhängig ist. Bei Vorsatz oder grober Fahrlässigkeit haftet der Arbeitnehmer grundsätzlich in voller Höhe, wohingegen bei mittlerer Fahrlässigkeit eine anteilige Haftung besteht und der Arbeitnehmer nur bei leichter und leichtester Fahrlässigkeit gar nicht haftet. Anwendungsbeispiele im Rahmen von BYOD können die schuldhafte Verletzung von Sorgfaltspflichten oder der (bewusste oder unbewusste) Einsatz schadhafter Software sein. Bei der soeben dargestellten Einteilung handelt es sich jedoch nur um eine grobe Orientierungshilfe. Es kommt vielmehr immer auf die konkreten Umstände des Einzelfalles an. Neben dem Grad des Verschuldens sind insbesondere die konkrete Schadenshöhe und die sich daraus ergebende Zumutbarkeit der Schadensübertragung auf den Arbeitnehmer vor dem Hintergrund seiner wirtschaftlichen Leistungsfähigkeit zu beachten. Letztlich besteht für den Arbeitgeber aber immer die Gefahr, dass er den Arbeitnehmer bei Schäden nicht in Regress nehmen kann.

Schutzpflicht für private Endgeräte

Die Endgeräte der Mitarbeiter als solche bringen schon einige Haftungsrisiken mit sich. Auch die mitarbeitereigene Hardware bedarf der Wartung und Reparatur. Daneben sind in regelmäßigen Abständen Softwareupdates unumgänglich. Mit diesen Arbeiten an Hard- und Software geht auch ein Schadensrisiko einher, das je nach eingesetztem Produkt aus dem finanziellen Blickwinkel nicht zu unterschätzen ist.

Die Geräte können außerdem beschädigt werden, verloren gehen, gestohlen werden oder auf sonstige Art abhanden kommen. Bei Verlust oder Beschädigung besteht eine Benachrichtigungspflicht des Arbeitnehmers gegenüber dem Arbeitgeber, vor allem auch wegen der auf dem Gerät befindlichen dienstlichen Datenbestände. Dabei darf „BYOD“ nicht zur Umgehung des Betriebsrisikos führen, das der Arbeitgeber zu tragen hat. Dementsprechend ist der Arbeitgeber regelmäßig zur Zahlung eines Aufwendungsersatzes für die dienstliche Nutzung des Privatgeräts verpflichtet (vgl. §§ 670, 675 Bürgerliches Gesetzbuch (BGB)). Daneben steht dem Arbeitnehmer für risikotypische Schäden am Gerät nach § 670 BGB analog ein Ausgleichsanspruch zu, wobei es sich hierbei um eine verschuldensunabhängige Haftung handelt. In der Regel wird ein pauschaler vertraglicher Ausschluss dieser Ersatzpflichten gegen das AGB-Recht verstoßen und damit rechtswidrig sein. Der Arbeitgeber kann das Aufwendungsersatzverlangen hingegen dann zurückweisen und eine Zahlung verweigern, wenn die Vergütung seitens des Arbeitgebers im Rahmen der Anschaffung des Gerätes bereits das Schadensrisiko abdeckt, weshalb diesbezüglich eine klare Abrede zwischen den Parteien erforderlich ist.

Privater Internetanschluss

Die Nutzung des privaten Internetanschlusses zu dienstlichen Zwecken kann ebenfalls Probleme hervorbringen. An dieser Stelle findet zwar eine starke Vermengung von „BYOD“ und „Telearbeit“ statt, nichtsdestotrotz muss es im Rahmen von „BYOD“ berücksichtigt werden. Einige Internet-Service-Provider differenzieren zwischen der privaten und dienstlichen bzw. gewerblichen Nutzung. Für diese verschiedenen Nutzungsarten werden vom Diensteanbieter regelmäßig unterschiedliche Entgelte gefordert. Ist der private Internetanschluss nur für die private Nutzung ausgelegt, wird dieser aber für dienstliche Zwecke genutzt, kann möglicherweise eine Vertragsverletzung vorliegen, woraus sich ein Schadensersatzverlangen des Internet-Service-Providers sowie eine Kündigung des Telefon-/Internetprovidervertrags aus wichtigem Grund ergeben kann.

Handlungsempfehlungen

Zur Vorbeugung von Haftungsfällen können im Vorfeld einige Maßnahmen ergriffen werden, damit die Gefahren möglichst gering gehalten werden und die Einführung von „BYOD“ somit erleichtert wird. Die nachfolgende Darstellung der Handlungsempfehlungen dient gleichzeitig als eine Art Checkliste.

1. Als oberstes Gebot gilt vorweg, dass aus Gründen der Rechtssicherheit, Klarheit und Transparenz sämtliche Absprachen zwischen Arbeitgeber und Arbeitnehmer schriftlich festgehalten werden sollten.

2. Eine Vereinbarung über regelmäßige Sicherungskopien durch den Arbeitnehmer erscheint ratsam. Auf diese Weise kann ein Datenverlust weitestgehend eingeschränkt werden.

3. Zur Vermeidung von Sicherheitslücken und Datenverlusten ist eine einheitliche Administration durch den Arbeitgeber zu empfehlen. In diesem Zusammenhang sollte der Arbeitgeber einerseits geeignete Sicherheitssoftware zur Verfügung stellen, andererseits sollten betriebliche Vereinbarungen Regelungen über die Haftung bei Verlust oder Beschädigung der Geräte oder betrieblicher Daten enthalten und eindeutig festlegen, wer Reparaturen in Auftrag gibt und deren Kosten trägt. Dadurch kann für beide Parteien das Schadens- und Kostenrisiko eindeutig festgelegt werden, wer also in welchen Konstellationen haftet und welche Partei unter welchen Voraussetzungen das Betriebsrisiko trägt. Darüber hinaus sollte seitens des Arbeitgebers eine regelmäßige Wartung der Privatgeräte durchgeführt werden. Ergänzend kann der Mitarbeiter zur selbständigen Überprüfung des Geräts verpflichtet werden. Da die Betriebshaftpflichtversicherung mitarbeitereigene Hardware regelmäßig nicht abdeckt, ist der Abschluss einer gesonderten Geräteversicherung ratsam, wobei die sich daraus ergebende Kostentragungspflicht eindeutig zugewiesen und geregelt werden sollte.

4. Dem Arbeitnehmer sollte für den Fall des Verlustes eines Geräts eine Benachrichtigungspflicht auferlegt werden. Dies hat insbesondere dann zu gelten, wenn auf dem privaten Endgerät dienstliche Daten gespeichert wurden und dieses Gerät nun gestohlen worden, verloren gegangen oder auf andere Weise abhandengekommen ist. Jedoch kann ein Missbrauch selbst dann nicht ausgeschlossen werden, wenn keine Daten auf dem Gerät gespeichert wurden, da schon die Preisgabe von Verbindungsinformationen zu IT-Systemen des Arbeitgebers

diesen angreifbar machen können. Dementsprechend ist eine Benachrichtigungspflicht des Mitarbeiters bei einem Geräteverlust generell empfehlenswert.

5. Neben der einheitlichen Administration sollte die Einstellung der Geräte-Konfiguration ebenfalls zentral durch den Arbeitgeber vorgenommen werden. In diesem Zuge sollten die Arbeitnehmer im Rahmen einer Vereinbarung dazu verpflichtet werden, diese Einstellungen zu verwenden und nicht zu verändern. Ferner sollte der Zugriff auf das private Gerät von der Eingabe eines Passworts abhängig gemacht werden, sodass der Zugriff Dritter (etwa Familienangehörige) eingeschränkt wird. Auch im Hinblick auf den Schutz von Betriebs- und Geschäftsgeheimnissen ist die verbindliche Vorgabe eines Passworts ratsam, zumal diese Daten oftmals vertraglichen Geheimhaltungspflichten gegenüber Dritten unterliegen. Im Rahmen der Vereinbarung sollte der Arbeitnehmer auch verpflichtet werden, das Passwort gegenüber Dritten geheim zu halten und sicher aufzubewahren.

Teil 2: Arbeitsrecht, Urheberrecht

In diesem Teil wird das Konzept aus dem Blickwinkel des Arbeitsrechts sowie des Urheberrechts beleuchtet. Am Ende der Darstellung des jeweiligen Rechtsgebietes werden Handlungsempfehlungen beschrieben, die gleichzeitig als eine Art Checkliste genutzt werden können.

I. Arbeitsrecht

Derzeit bestehende Dienst- und Arbeitsverträge sowie Dienst- bzw. Betriebsvereinbarungen beinhalten in der Regel nur die private Nutzung der Kommunikationssysteme des Arbeitgebers mittels dienstlicher Geräte, wohingegen die dienstliche Nutzung dieser Systeme über private Endgeräte (noch) nicht vertraglich geregelt ist. Sofern sich der Arbeitgeber für eine Zulassung von „BYOD“ entscheidet, sind über die bisherigen Regelungen hinausgehende Dienst- bzw. Betriebsvereinbarungen notwendig. Daneben scheint die Anpassung bestehender Dienst- und Arbeitsverträge in Teilen sinnvoll. Im Zuge einer neuen Dienst- bzw. Betriebsvereinbarung können dann auch die datenschutzrechtlichen Belange der Mitarbeiter im Rahmen der §§ 12 Abs. 4, 32 Bundesdatenschutzgesetz (BDSG) (sowie der entsprechenden Vorschriften der Landesdatenschutzgesetze, vgl. § 36 LDSG BW, § 2 Abs. 2 BlnDSG, § 29 BbgDSG, § 20 BrDSG, § 32 HmbDSG, § 34 HDSG, § 35 DSG MV, § 24 NDSG, § 29 DSG NW, § 31 LDSG RP, § 31 SDSG, § 27 SächsDSG, § 28 DSG-LSA, § 23 LDSG SH, § 33 ThürDSG) geregelt werden, welcher die Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses betrifft. Auf die datenschutzrechtlichen Probleme bei der Einführung von „BYOD“ wird allerdings noch in einem gesonderten Beitrag eingegangen.

Bereitstellung betrieblicher Ressourcen

Grundsätzlich trifft den Arbeitgeber die Verpflichtung, betriebliche Ressourcen bereitzustellen und zu erhalten. Die privaten Endgeräte des Arbeitnehmers stehen in seinem Privateigentum. Dieses Privateigentum ist jedoch nicht vom Direktions- bzw. Weisungsrecht des Arbeitgebers umfasst, sodass ein verpflichtender „BYOD“-Einsatz dieser Geräte nicht angeordnet werden kann. Erlaubt der Arbeitgeber die Einbringung eigener Geräte, ist es ratsam, die jeweiligen Gerätetypen und Softwareversionen genau zu bezeichnen und zu dokumentieren. Eines der größten Probleme im Zuge von „BYOD“ ist nämlich die Verwaltung unterschiedlichster Mobilgeräte. Es ist daher eine hoch skalierbare Managementplattform erforderlich. Einer unbedingten Regelung bedarf im Zuge der Einführung von „BYOD“ aus haftungs- und datenschutzrechtlichen Gründen vor allem die konkrete Abgrenzung zwischen der privaten und betrieblichen Nutzung des eingebrachten Gerätes. Im Rahmen dieser Regelung ist auch eine klare Abgrenzung in zeitlicher Hinsicht angezeigt (zu diesem Punkt sogleich mehr). Auch der Vergütungsanspruch des Arbeitnehmers für die betriebliche Nutzung sollte vertraglich festgelegt werden. Entsprechend des Anteils der Nutzung sind die Kosten dort prozentual aufzuführen, wobei daneben eine Anpassungsklausel ratsam ist. Auf diese Weise kann Veränderungen in der Verteilung dieser Anteile besser nachgekommen werden. Eine anteilige Beteiligung des Arbeitgebers an den Kosten für Anschaffung und Wartung ist denkbar. Der Arbeitgeberanteil kann dabei als pauschale Vergütung oder in Form eines Einzelnachweises abgegolten werden.

Einhaltung der Arbeitszeit

Vor allem aus zeitlicher Sicht muss im Zuge der Einführung von „BYOD“ die konkrete Abgrenzung zwischen der privaten und betrieblichen Nutzung des eingebrachten Gerätes geregelt werden. Im Rahmen der heutigen Kommunikation vermengen sich Freizeit und Arbeitszeit in einem zunehmenden Maße. „BYOD“-Programme verstärken diesen Effekt durch die permanente Erreichbarkeit des Arbeitnehmers. Zu nennen ist hier etwa das Lesen dienstlicher E-Mails oder die Annahme von Kunden- sowie Mitarbeiteranrufen in der Freizeit. Dadurch könnte sich der Arbeitnehmer gezwungen fühlen, auch in seiner Freizeit und damit außerhalb der klassischen Arbeitszeit dienstliche Anfragen auf seinem Gerät zu beantworten. Darin kann möglicherweise eine Arbeitsaufnahme zu sehen sein, die arbeitszeitrechtlich relevant ist. Sofern der Arbeitnehmer außerhalb seiner regulären Arbeitszeit zu ständiger Erreichbarkeit auf seinem Endgerät verpflichtet ist, ist dies arbeitsrechtlich als Rufbereitschaft einzuordnen. Er muss nämlich zur Arbeitsaufnahme an einem Ort seiner Wahl außerhalb der Arbeitszeit auf Abruf stehen. Zu beachten ist

aber, dass die Arbeitszeit erst ab der tatsächlichen Arbeitsaufnahme beginnt. Die Rufbereitschaft als solche ist dagegen noch nicht als Arbeitszeit einzuordnen. Eine Rufbereitschaft wird aber dann nicht vorliegen, wenn der Arbeitnehmer nicht zur ständigen Erreichbarkeit verpflichtet ist. Sofern der Mitarbeiter freiwillig außerhalb seiner regulären Arbeitszeit tätig wird, kann darin grundsätzlich keine Arbeitszeit gesehen werden. Dementsprechend sind klare und verlässliche Regelungen zum arbeitszeitlichen Umgang mit den privaten Geräten außerhalb der vereinbarten Arbeitszeit sowie zum privaten Gebrauch während der Arbeitszeit festzulegen. Dies gilt insbesondere vor dem Hintergrund des § 5 Arbeitszeitgesetz (ArbZG), wonach die Arbeitnehmer nach Beendigung der täglichen Arbeitszeit eine ununterbrochene Ruhezeit von mindestens elf Stunden haben müssen. Ferner ist zu beachten, inwieweit der Arbeitnehmer Überstunden ableisten muss und wie diese vergütet oder durch Freizeitausgleich abgegolten werden.

Beteiligung des Personalrats bzw. des Betriebsrats

Aus arbeitsrechtlicher Perspektive ist im öffentlichen Sektor auch die Beteiligung des Personalrats von entscheidender Bedeutung. Eine Mitbestimmungspflicht des Personalrats kann sich bei der Einführung dementsprechend aus folgenden Vorschriften (sowie den entsprechenden Vorschriften der Landespersonalvertretungsgesetze) ergeben:

- § 75 Abs. 3 Nr. 15 Bundespersonalvertretungsgesetz (BPersVG) (Regelung der Ordnung in der Dienststelle und des Verhaltens der Beschäftigten);
- § 75 Abs. 3 Nr. 16 BPersVG (Gestaltung der Arbeitsplätze);
- § 75 Abs. 3 Nr. 17 BPersVG (Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen);
- § 76 Abs. 2 Nr. 7 BPersVG (Einführung grundlegend neuer Arbeitsmethoden).

Im nicht-öffentlichen Bereich müssen die Vorschriften des Betriebsverfassungsgesetzes (BetrVG) beachtet werden. Zunächst hat der Betriebsrat ein Kontrollrecht nach § 80 BetrVG, wozu nach § 80 Abs. 1 Nr. 1 BetrVG etwa die Überwachung der Einhaltung der zugunsten der Arbeitnehmer geltenden Gesetze durch den Arbeitgeber zählt. Daneben kann sich eine Mitbestimmungspflicht des Betriebsrates insbesondere aus folgenden Gründen ergeben:

- § 87 Abs. 1 Nr. 1 BetrVG: Fragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb, etwa im Hinblick auf Passwortverwaltung, Malwareschutz oder Updates;
- § 87 Abs. 1 Nr. 2 BetrVG: Beginn und Ende der täglichen Arbeitszeit einschließlich der Pausen sowie Verteilung der Arbeitszeit auf die einzelnen Wochentage, insbesondere mit Blick auf die Always-on-Connectivity, wodurch eine Vermischung von Arbeits- und Freizeitgestaltung erfolgt;
- § 87 Abs. 1 Nr. 3 BetrVG vorübergehende Verkürzung oder Verlängerung der betriebsüblichen Arbeitszeit;
- § 87 Abs. 1 Nr. 6 BetrVG: Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Hierbei ist die Geeignetheit zur Überwachung ausreichend, sodass der Arbeitgeber nicht gezielt Überwachungszwecke verfolgen muss. Eine solche Eignung zur Überwachung kann zum Beispiel schon vorliegen beim Protokollieren von Logins, Synchronisationsvorgängen, GPS-Lokalisierungsdaten sowie bei datenschutzrechtlichen Kontrollbefugnissen.

Gegenstand dieses Mitbestimmungsrechts können beispielsweise der Zeitpunkt der Einführung von „BYOD“, der Zeitraum der Nutzung und die überbetriebliche Vernetzung sein. Nach § 90 BetrVG bestehen im Hinblick auf die Planung von technischen Anlagen (§ 90 Abs. 1 Nr. 2 BetrVG), von Arbeitsverfahren und Arbeitsabläufen (§ 90 Abs. 1 Nr. 3 BetrVG) und der Arbeitsplätze (§ 90 Abs. 1 Nr. 4 Be-trVG) Unterrichtungspflichten gegenüber dem Betriebsrat. Daher muss der Arbeitgeber den Betriebsrat bereits im Planungsstadium hinsichtlich der Gestattung von „BYOD“ einbeziehen und diesen unter Vorlage der erforderlichen Unterlagen unterrichten.

Handlungsempfehlungen

Wie deutlich gemacht wurde, gilt es auch aus arbeitsrechtlicher Sicht einige Punkte zu beobachten, um eine rechtmäßige Einführung von „BYOD“ zu gewährleisten. Die nachfolgende Darstellung der Handlungsempfehlungen soll gleichzeitig als eine Art Checkliste dienen.

1. Als oberstes Gebot gilt vorweg, dass aus Gründen der Rechtssicherheit, Klarheit und Transparenz sämtliche Absprachen zwischen Arbeitgeber und Arbeitnehmer schriftlich festgehalten werden sollten. Bisher bestehende Dienst- bzw. Betriebsvereinbarungen sowie Dienst- und Arbeitsverträge werden keine Passus zum Themenkomplex „BYOD“ beinhalten. Daher sollten diese um entsprechende Abschnitte ergänzt werden, wobei in diesem Zusammenhang direkt auch datenschutzrechtliche Belange der Mitarbeiter konstituiert werden können. Neben Dienst- bzw. Betriebsvereinbarungen sollte daher auf Individualvereinbarungen zurückgegriffen werden. Es gilt zu beachten, dass Dienst- bzw. Betriebsvereinbarungen BDSG- und AGB-fest sein müssen (vgl. insbesondere §§ 305c Abs. 2, 307 Abs. 1 S. 2 Bürgerliches Gesetzbuch (BGB)). Dennoch sind Dienst- bzw. Betriebsvereinbarungen das „Mittel der Wahl“ bei fast allen Fragen mobiler Endgeräte in der jeweiligen Einrichtung, da mit ihnen einige Vorteile einhergehen. Es können verbindliche Vereinbarungen über sämtliche Gegenstände betrieblicher Mitbestimmung getroffen werden (vgl. § 77 Abs. 4 S. 1 BetrVG, wonach Betriebsvereinbarungen unmittelbar und zwingend gelten). Das BPersVG sowie weitestgehend die Personalvertretungsgesetze der Länder kennen keine solche Vorschrift, die Dienstvereinbarungen für unmittelbar und zwingend erklärt (vgl. § 73 BPersVG). Der Gesetzgeber hat es anscheinend als selbstverständlich angesehen, dass auch Dienstvereinbarungen unmittelbar und zwingend gelten. Dementsprechend kann § 77 Abs. 4 S. 1 BetrVG entsprechend angewendet werden. Gleichzeitig können mögliche Probleme der AGB-Inhaltskontrolle abgemildert werden (§ 310 Abs. 4 BGB). Da eine wirksame Betriebsvereinbarung zugleich als Rechtsvorschrift im Sinne des § 4 Abs. 1 BDSG gilt (vgl. die entsprechenden Vorschriften der Landesdatenschutzgesetze: § 4 Abs. 1 LDSG BW, Art. 15 Abs. 1 BayDSG, § 6 Abs. 1 BlnDSG, § 4 Abs. 1 BbgDSG, § 3 Abs. 1 BrDSG, § 5 Abs. 1 S. 1 HmbDSG, § 7 Abs. 1 HDSG, § 7 Abs. 1 DSG MV, § 4 Abs. 1 NDSG, § 4 Abs. 1 DSG NW, § 5 Abs. 1 LDSG RP, § 4 Abs. 1 S. 1 SDSG, § 4 Abs. 1 SächsDSG, § 4 Abs. 1 DSG-LSA, § 11 Abs. 1 LDSG SH, § 4 Abs. 1 ThürDSG), können datenschutzrechtliche Befugnisse des Arbeitgebers darin verankert werden, ohne auf eine Einwilligung des Arbeitnehmers angewiesen zu sein. Es muss aber beachtet werden, dass nur Pflichten des Arbeitgebers sowie Pflichten des Arbeitnehmers im Hinblick auf die Verbindung zur IT-Infrastruktur der jeweiligen Einrichtung festgelegt werden können, wohingegen Aspekte des Privatlebens des Arbeitnehmers (etwa Vorschriften über den Abschluss von Reparatur-, Wartungs- und Garantieverträgen, Software- und Hardwareanschaffung) darin nicht geregelt werden können und dafür daher individualvertragliche Vereinbarungen erforderlich sind.

2. Zur Verwaltung der im Rahmen von „BYOD“ in einer Vielzahl eingebrachten Endgeräte der Arbeitnehmer sollten die jeweiligen Gerätetypen und Softwareversionen genau bezeichnet und dokumentiert werden. Hierbei bietet sich eine hoch skalierbare Managementplattform an. Individualvertragliche Regelungen sollten in diesem Zusammenhang neben sämtlichen Kostenfragen im Hinblick auf Anschaffung, Wartung, Reparatur und Ersatz auch den Vergütungsanspruch des Arbeitnehmers für die betriebliche Nutzung beinhalten. Die Kosten sind dabei entsprechend des Anteils der jeweiligen Nutzung (dienstlich und privat) prozentual aufzuführen, wobei daneben eine Anpassungsklausel ratsam ist, da auf diese Weise Veränderungen in der Verteilung dieser Anteile besser nachgekommen werden kann.

3. Die Vorgaben hinsichtlich der Arbeitszeit müssen unbedingt beachtet und dementsprechende Regelungen zwischen den Parteien getroffen werden, damit keine Vermengung von Arbeitszeit und Freizeit erfolgt. Bei der Einführung von „BYOD“ sollte aus arbeitszeitrechtlicher Sicht insbesondere auf eine Verpflichtung der Arbeitnehmer zu einer ständigen Erreichbarkeit außerhalb der regulären Arbeitszeiten verzichtet werden. Dementsprechend sind klare und verlässliche Regelungen sowohl zum arbeitszeitlichen Umgang mit den privaten Geräten außerhalb der vereinbarten Arbeitszeit als auch hinsichtlich des privaten Gebrauchs während der Dienstzeit festzulegen. Hierbei können die üblichen arbeitsrechtlichen Maßstäbe zur Online-Nutzung am Arbeitsplatz als Richtwerte dienen, wobei es zu beachten gilt, dass ein zu strenges Management seitens des Arbeitgebers die Begeisterung der Arbeitnehmer für „BYOD“ schwinden lassen kann. Empfehlenswert sind Regelungen, durch die der Arbeitnehmer zur Einhaltung der Ruhezeiten nach § 5 ArbZG angehalten wird, wobei meist auch seitens des Personal- bzw. Betriebsrats dahingehende Forderungen aufkommen. Sofern absehbar ist, dass ein phasenweises Tätigwerden des Arbeitnehmers außerhalb

seiner regulären Arbeitszeit unausweichlich ist und dies sogar vom Arbeitgeber veranlasst wird (etwa die Weiterleitung einer E-Mail mit der Aufforderung zur Beantwortung, das Durchleiten eines Anrufs oder die Ansetzung einer Telefon-/Videokonferenz), sollte dies ausdrücklich geregelt werden. Neben dem Arbeitszeitgesetz kommen im Rahmen von „BYOD“ auch Fragen hinsichtlich der Ableistung und Vergütung bzw. Abgeltung von Überstunden auf. Diese Punkte können im Verlauf eines „BYOD“-Programms zu Streitigkeiten führen, sodass hier idealerweise schon im Vorfeld unter Beteiligung der betroffenen Kreise (Arbeitgeber sowie Arbeitnehmervertreter) interessengerechte und eindeutige Regelungen geschaffen werden sollten.

4. Die Einführung von „BYOD“ wird regelmäßig die Mitwirkung des Personalrats (im öffentlichen Bereich) sowie des Betriebsrats (im nicht-öffentlichen Bereich) zur Folge haben. Aufgrund bestehender Unterrichtungspflichten und zur Vermeidung von Verlangsamungs- oder Verhinderungsmaßnahmen ist eine frühzeitige Einbindung dieser Organe (schon im Planungsstadium) ratsam (vgl. die oben genannten Vorschriften). Durch eine offene und transparente Vorgehensweise seitens des Arbeitsgebers können Vorbehalte und Befürchtungen frühzeitig aufgeklärt und beiseite geschafft werden.

II. Urheberrecht

Auf den ersten Blick mag es befremdlich erscheinen, was das Urheberrecht mit dem Thema „BYOD“ zu tun haben kann. Schließlich bringen die Mitarbeiter ihre bereits funktionsfähigen Endgeräte am Arbeitsplatz ein. Es bestehen jedoch einige Fallstricke aus urheberrechtlicher Sicht, die es zu beachten gilt. Bei der Einbringung seiner Geräte samt Software geht das Eigentum daran nicht auf den Arbeitgeber über. Vielmehr bleibt der Arbeitnehmer weiterhin deren Eigentümer. Dies gilt auch im Falle der betrieblichen Nutzung dieser Endgeräte. Von dieser Eigentumslage sind aber die Nutzungsrechte an der installierten Software zu unterscheiden und müssen gesondert betrachtet werden.

Unterlizenzierung

Sobald der Arbeitnehmer private Endgeräte mit installierter Software für dienstliche Zwecke nutzt, können der Arbeitgeber und der Arbeitnehmer in Konflikt mit dem Urheberrecht kommen. Bei jedem Einsatz von Software müssen die entsprechenden Nutzungsrechte eingehalten werden. Meistens beziehen sich die Nutzungsrechte nur auf eine bestimmte Nutzungsart. Die auf dem privaten Endgerät installierte Software ist häufig lediglich auf die private Nutzung ausgerichtet und daher vom Hersteller ausschließlich zu diesem Zweck lizenziert. Die Lizenzbedingungen erlauben in diesem Fall regelmäßig eine dienstliche Nutzung der Software nicht. Anbieter von Freeware und Cloud-Anwendungen sehen in ihren Lizenzbedingungen üblicherweise besondere Modelle für die dienstliche Nutzung ihrer Produkte vor. Entsprechendes kann auch im umgekehrten Fall gelten, wenn also die durch den Unternehmer lizenzierte Software auf den privaten Geräten installiert wird und dann vom Arbeitnehmer auch privat genutzt wird. Die Konsequenz beider Konstellationen ist eine Unterlizenzierung hinsichtlich der installierten Software.

Der Arbeitnehmer wird die für die dienstliche Nutzung lizenzierte Software häufig auch privat nutzen und umgekehrt für private Zwecke erworbene Software gleichzeitig für dienstliche Angelegenheiten einsetzen. Dabei kann es teilweise vorkommen, dass die ursprünglich im Privatbereich genutzte Software, die im Zuge von „BYOD“ für dienstliche Zwecke verwendet wird, gar nicht lizenziert ist. Dadurch kann es zu verbotenen und strafbaren Verhaltensweisen in Form von vergütungsrelevanten Nutzungshandlungen sowie urheberrechtlich relevanten Vervielfältigungen und Weitergaben kommen. In diesem Zusammenhang kann gerade die dienstliche Nutzung der Software als solche bereits die Verletzungshandlung darstellen. Dementsprechend muss auf die konkrete Ausgestaltung der Lizenzbestimmungen geachtet werden, insbesondere auf die Unterscheidung zwischen privaten und gewerblichen Nutzungsbefugnissen, aber auch zwischen personen- oder gerätegebundenen Lizenzen sowie Mehrplatzlizenzen. Zur Kontrolle und zum Ausschluss einer Unterlizenzierung seitens des Arbeitgebers sind daher regelmäßige interne Audits unabdingbar.

Die soeben beschriebenen Handlungen können je nach Konstellation (insbesondere Umfang und Dauer der Unterlizenzierung) für Arbeitgeber und Arbeitnehmer erhebliche zivilrechtliche Folgen haben. So besteht zunächst ein Anspruch auf Schadensersatz und Unterlassung sowie Beseitigung gegen die handelnde Person aus § 97 UrhG. Nach § 99 UrhG haftet der Unternehmer verschuldensunabhängig für die Urheberrechts-

verletzungen seiner Mitarbeiter. „Unternehmer“ i. S. d. § 99 UrhG sind dabei auch Körperschaften des öffentlichen Rechts, also z. B. Hochschulen. Die Formulierung „in einem Unternehmen“ in § 99 UrhG ist zur Gewährleistung eines wirksamen Rechtsschutzes funktional sowie weit zu verstehen und bedeutet, dass die Verletzungshandlung des Mitarbeiters im Tätigkeitsbereich der jeweiligen Einrichtung erfolgen muss. Diese Voraussetzung ist bereits dann erfüllt, wenn der Arbeitgeber „BYOD“ gestattet. Zu beachten sind zudem die Straf- und Bußgeldvorschriften der §§ 106 ff. UrhG, die für rechtswidrige Vervielfältigungshandlungen eine Freiheitsstrafe von bis zu drei Jahren oder eine Geldstrafe vorsehen. Daneben kann mit einem Bekanntwerden von massiven Lizenzverstößen durch eine Einrichtung unabhängig davon, ob diese bewusst oder unbewusst erfolgten, ein hoher Ansehensverlust einhergehen.

Software aus zweifelhaften Quellen

Aus dem Blickwinkel der IT-Sicherheit weitaus gefährlicher als die soeben dargestellte Unterlizenzierung ist die Verwendung von illegaler Software aus zweifelhaften Quellen. Der Download von Software durch den Arbeitnehmer kann grundsätzlich nicht eingeschränkt werden. Daher kann es (insbesondere aus Kostengründen) möglich sein, dass der Arbeitnehmer nicht-lizenzierte Softwareversionen von Internetseiten herunterlädt, die vom Hersteller nicht mit der Verbreitung der Software betraut wurden. Meist handelt es sich dabei um genuin urheberrechtswidrig erstellte Kopien ohne jede Art von Lizenz, sodass das soeben besprochene Problem der Unterlizenzierung hier fortbesteht. Der Arbeitgeber hat kaum Kontrollmöglichkeiten über die herangezogenen Quellen, insbesondere wenn der Arbeitnehmer den Download und die Installation zu Hause durchführt. In vielen Fällen sind die aus diesen zweifelhaften Quellen bezogenen Softwareprodukte virenbehaftet oder „gehackt“. Aufgrund der erhöhten Anfälligkeit für Hacker- oder Virenangriffe bedeutet die Verwendung dieser Software eine erhöhte Gefahr für die IT- und Unternehmenssicherheit.

Handlungsempfehlungen

Bei Urheberrechtsverletzungen können neben Unterlassungs- und Beseitigungsansprüchen (§ 97 Abs. 1 UrhG) auch Schadensersatzansprüche (§ 97 Abs. 2 UrhG) auf den Verletzer zukommen, die gerade im Softwarebereich mit erheblichen Summen verbunden sein können und die Gefahr von Abmahnungen bergen. Daneben dürfen auch die speziellen Straf- und Bußgeldvorschriften (§§ 106 ff. UrhG) nicht aus dem Blickfeld verschwinden, die im Verletzungsfall empfindliche Strafen vorsehen. Dementsprechend sind zur Vorbeugung von Haftungsfällen aus dem urheberrechtlichen Bereich im Vorfeld einige Maßnahmen zu ergreifen, damit die Gefahren möglichst gering gehalten werden und die Einführung von „BYOD“ somit erleichtert wird. Die nachfolgende Darstellung der Handlungsempfehlungen dient wiederum als eine Art Checkliste.

1. Zur Verhinderung von urheberrechtlichen Verletzungshandlungen durch Unterlizenzierung muss auf die konkrete Ausgestaltung der Lizenzbestimmungen geachtet werden, insbesondere auf die Unterscheidung zwischen privaten und gewerblichen Nutzungsbefugnissen, aber auch zwischen personen- oder gerätegebundenen Lizenzen sowie Mehrplatzlizenzen. Diesbezüglich müssen seitens des Arbeitgebers regelmäßige interne Audits durchgeführt werden. Auf diese Weise kann einerseits kontrolliert werden, welche Softwares auf den privaten Endgeräten installiert sind, andererseits kann dadurch eine Unterlizenzierung verhindert werden. Die internen IT-Richtlinien sollten auf die Lizenzneuerungen im Zuge von „BYOD“ angepasst und deren Einhaltung regelmäßig überprüft werden.

2. Daneben sollte zur Minimierung des Haftungsrisikos für Urheberrechtsverletzungen sowie der aus Schadsoftware herrührenden Gefahren das betriebliche Lizenzmanagement auf die privaten Geräte in betrieblicher Nutzung erstreckt werden. Idealerweise sollten die Endgeräte der Mitarbeiter regelmäßig auf unlizenzierte, illegale oder schädliche Software überprüft werden. Dies könnte in einer Betriebsvereinbarung geregelt werden (siehe dazu bereits die obigen Ausführungen). Es erscheint jedoch unwahrscheinlich, dass ein Mitarbeiter den gesamten Inhalt seines Gerätes ohne weiteres offenlegen wird. Der Schutz der Privatsphäre der Arbeitnehmer sollte vom Arbeitgeber gefördert werden, da so mögliche Vorbehalte gegen eine Einführung von „BYOD“ abgemildert werden. Daher könnte man alternativ zu einer vollumfänglichen Offenlegungspflicht den Mitarbeiter dazu verpflichten, in regelmäßigen Abständen einen Nachweis über die ordnungsgemäße Lizenzierung der von ihm zu betrieblichen Zwecken eingesetzten Software zu erbringen. Mit dem Einverständnis des Mitarbeiters könnte man diesen

Nachweis durch eine stichprobenartige Überprüfung absichern. Sofern der Arbeitnehmer derartige Überprüfungen verweigert, sollte das private Gerät nicht betrieblich verwendet werden dürfen, was einem Widerruf von „BYOD“ in Bezug auf diesen Arbeitnehmer bedeutet. Eine sehr strikte Regelung könnte daneben vorschreiben, welche Software der Mitarbeiter auf dem dienstlichen Bereich seines Endgeräts (dazu sogleich mehr) installieren darf und dass dahingehende Kontrollen erlaubt sind. Bestehende Gewährleistungsansprüche für die eingesetzten Softwares könnten an den Arbeitgeber abgetreten oder für den Arbeitgeber geltend gemacht werden. Alternativ bieten sich auch der zentrale Einkauf sowie die Verwaltung der erforderlichen Softwares durch den Arbeitgeber an. Er kann diese direkt in sein betriebliches Lizenzmanagement einpflegen und verringert auf diese Weise die Gefahr einer Unterlizenzierung deutlich. Dabei sollte auch darauf geachtet werden, dass die erworbenen Nutzungsrechte sowohl die dienstliche als auch die private Nutzung der jeweiligen Software erlauben. Dadurch möglicherweise entstehende Mehrkosten können interessengerecht zwischen Arbeitgeber und Arbeitnehmer aufgeteilt werden, sofern die private Nutzung möglich ist, einen merklichen Anteil trägt und sich der Arbeitnehmer bewusst und freiwillig zur Teilnahme am BYOD-Programm entscheidet. Um Konflikte zu vermeiden, sollte die Kostenaufteilung schriftlich fixiert werden. Letztlich kann auch die Nutzung von Open-Source-lizenzierter Software eine Option sein.

3. Die Trennung von privaten und dienstlichen Daten auf technischer Ebene erscheint unabdingbar, um die notwendigen Kontrollmöglichkeiten seitens des Arbeitgebers umzusetzen. In diesem Zusammenhang ist an die Konfiguration virtueller Desktops (= multiple Arbeitsflächen(-bereiche)), die Partitionierung der Festplatten der Geräte, verschlüsselte Container (Container-Apps) oder Terminalserver-Lösungen zu denken. Auf diese Weise kann einerseits eine Kontrolle erfolgen, ohne dass private Daten des Arbeitnehmers betroffen wären, andererseits könnte illegal installierter Software der Zugriff auf das Unternehmensnetzwerk verweigert werden.

Teil 3: Datenschutzrecht, Datensicherheit

In diesem Teil wird das Konzept aus dem Blickwinkel des Datenschutzrechts sowie der Datensicherheit beleuchtet. Am Ende der Darstellung des jeweiligen Rechtsgebietes werden auch in diesem Artikel wieder Handlungsempfehlungen beschrieben, die gleichzeitig als eine Art Checkliste genutzt werden können.

I. Datenschutzrecht

Auf Hochschulen (= öffentliche Stellen) finden die Vorschriften der Landesdatenschutzgesetze Anwendung (vgl. § 1 Abs. 2 Nr. 2 Bundesdatenschutzgesetz (BDSG)). Der Übersichtlichkeit halber erfolgt die Darstellung im Folgenden allerdings anhand des BDSG, das sich inhaltlich ohnehin weitestgehend mit den Datenschutzgesetzen der Länder deckt.

Anwendbare Vorschriften

Sofern der Arbeitgeber „BYOD“ nicht ausdrücklich untersagt und private Endgeräte für dienstliche Zwecke genutzt werden, finden die datenschutzrechtlichen Vorschriften, denen der Arbeitgeber unterliegt, auch dabei Anwendung. Eine andere Beurteilung ergibt sich nur dann, wenn dieser eine sol-che Nutzung ausdrücklich und konsequent verbietet. Im Falle von „BYOD“ sind Mitarbeiter als Beschäftigte im Sinne des § 3 Abs. 11 BDSG und damit datenschutzrechtlich als Teil der verantwortlichen Stelle im Sinne des § 3 Abs. 7 BDSG anzusehen, sofern sie in Ausübung ihrer arbeitsvertraglichen Pflichten handeln. Daraus ergibt sich, dass die verarbeitende Stelle auch für den Datenumgang des Mitarbeiters auf dessen privaten Geräten verantwortlich ist, sofern personenbezogene Daten (gem. § 3 Abs. 1 BDSG sind dies Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person) betroffen sind. Als Auftragsdatenverarbeiter (§ 11 BDSG) für den Arbeitgeber ist der Arbeitnehmer im Rahmen von BYOD dagegen nicht anzusehen. Damit ist der Arbeitgeber für den Datenumgang des Arbeitnehmers voll verantwortlich, obwohl für ihn tatsächlich nur eingeschränkte Zugriffsmöglichkeiten bestehen. Die Integrität des Privatbereichs des Arbeitnehmers muss gewahrt bleiben. Der Arbeitgeber hat kein originäres Zugriffsrecht auf die Daten auf dem Gerät des Mitarbeiters, sondern vielmehr nur restriktive Kontrollbefugnisse.

Prüfungs- und Kontrollmöglichkeiten des Arbeitgebers

Derzeit mangelt es an einschlägiger Rechtsprechung im Hinblick auf Kontrollmöglichkeiten des Arbeitgebers bei der dienstlichen Nutzung privater Geräte. Derartige Kontrollbefugnisse bei der auch privaten Nutzung dienstlicher Geräte werden von Rechtsprechung und Literatur nur sehr restriktiv gewährt. Vor diesem Hintergrund werden im Fall der dienstlichen Nutzung privater Endgeräte im Zuge von „BYOD“ lediglich in seltenen Ausnahmefällen Kontrollmöglichkeiten des Arbeitgebers zu bejahen sein. Sowohl die Leitung der verantwortlichen Stelle als auch den Datenschutzbeauftragten treffen eine Vielzahl von Kontrollpflichten, die sich neben dem Datenschutzrecht auch aus gesellschafts-, handels- und steuerrechtlichen Vorschriften ergeben können. Zu berücksichtigen ist, dass bisherige Arbeitsverträge sowie Dienst- bzw. Betriebsvereinbarungen speziell zu diesem Themenkomplex äußerst selten Regelungen enthalten werden. Problematisch sind deshalb im Hinblick auf die Persönlichkeitsrechte der Mitarbeiter auch die gesetzlichen Vorgaben, die eine Einsichtsermöglichung in alle Unterlagen, wovon insbesondere auch auf den privaten Geräten der Mitarbeiter gespeicherte Daten und Datenverarbeitungsprogramme umfasst sind (§ 24 Abs. 4 S. 2 Nr. 1 BDSG), sowie die Gewährung eines jederzeitigen Zutritts in alle Diensträume (§ 24 Abs. 4 S. 2 Nr. 2 BDSG) verlangen.

Kein originäres Zugriffs- bzw. Zugangsrecht des Arbeitgebers

Ein originäres Zugriffs- bzw. Zugangsrecht auf die zu dienstlichen Zwecken eingesetzten privaten Endgeräte steht dem Arbeitgeber nicht zu. Aus diesem Grund muss ein solches Recht sowie dessen Bedingungen mit dem Beschäftigten vertraglich vereinbart werden. Mit Blick auf die Grundrechte (insbesondere Art. 14 GG sowie Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) der Arbeitnehmer sind derartige individualvertragliche Verein-

barungen mit Risiken behaftet. Daher müssen inhaltliche Kontrollmaßnahmen im privaten Bereich auf das betrieblich absolut notwendige Maß beschränkt werden. Nur auf diese Weise kann der restriktiven Rechtsprechung der Arbeitsgerichte im privaten Lebensbereich der Arbeitnehmer Rechnung getragen werden. Dementsprechend bedürfen Maßnahmen, welche die Nichteinsehbarkeit privater Arbeitnehmerdaten durch den Arbeitgeber gewährleisten, besonderer Beachtung.

Prüfungsrecht der Aufsichtsbehörde im öffentlichen Bereich

Im öffentlichen Bereich ist bei der Einführung von „BYOD" das Prüfungsrecht der Aufsichtsbehörde zu berücksichtigen, da die öffentlichen Stellen der Datenschutzaufsicht unterliegen (§ 24 Abs. 1 BDSG). Gleiches regeln die jeweiligen Landesdatenschutzgesetze für die Hochschulen (vgl. § 1 Abs. 2 Nr. 2 BDSG; die Parallelvorschriften der Landesdatenschutzgesetze lauten: § 28 Abs. 1 LDSG BW; Art. 30 Abs. 1 BayDSG; § 24 Abs. 1 S. 1 BlnDSG; § 23 Abs. 1 BbgDSG; § 27 Abs. 1 S. 1 BrDSG; § 23 Abs. 1 S. 1 HmbDSG; § 24 Abs. 1 S. 1 HDSG; § 30 Abs. 1 S. 1 DSG MV; § 22 Abs. 1 S. 1 NDSG; § 22 Abs. 1 S. 1 DSG NW; § 24 Abs. 1 S. 1 LDSG RP; § 26 Abs. 1 S. 1 SDSG; § 27 Abs. 1 S. 1 SächsDSG; § 22 Abs. 1 S. 1 DSG-LSA; § 39 Abs. 2 S. 1 LDSG SH; § 37 Abs. 1 ThürDSG). Nach § 24 Abs. 4 BDSG sind die öffentlichen Stellen dazu verpflichtet, der Behörde Auskunft zu erteilen sowie Einsicht in alle Unterlagen (insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme) und jederzeit Zutritt in alle Diensträume zu gewähren. Sofern der Aufsichtsbehörde im Rahmen dieser Überprüfungen private Endgeräte vorgelegt werden müssen, steht das Prüfungsrecht der Aufsichtsbehörde den Grundrechten der Beschäftigten gegenüber. Dabei wird eine Interessenabwägung im Einzelfall erforderlich sein. Im Gegensatz zur Telearbeit, welche in den Schutzbereich der Unverletzlichkeit der Wohnung (Art. 13 GG) eingreift, geht es bei „BYOD" um das aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) abgeleitete Recht auf Privatsphäre sowie die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Ersteres Grundrecht ist im Hinblick auf die privaten Daten relevant, die sich zwangsläufig auf den mitarbeitereigenen Endgeräten befinden, wohingegen letzteres Grundrecht privaten Daten schützt, die in informationstechnischen Systemen gespeichert und verarbeitet werden.

Kontrolle durch die Aufsichtsbehörde im nicht-öffentlichen Bereich

Im nicht-öffentlichen Bereich erfolgt die Kontrolle durch die zuständige Aufsichtsbehörde (§ 38 BDSG). Auch hier haben die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen nach § 38 Abs. 3 S. 1 BDSG der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Aus § 38 Abs. 4 S. 1 BDSG ergeben sich während der Betriebs- und Geschäftszeiten bezüglich der Grundstücke und Geschäftsräume der Stelle für die Aufsichtsbehörde Befugnisse und Rechte zum Betreten, zur Prüfung und zur Besichtigung. Diese Kontrollmaßnahmen sind erlaubt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich ist. Im Rahmen von „BYOD" kommt die Problematik auf, ob und in welchem Umfang eine Aufsichtsbehörde im Zuge einer Betriebsprüfung beim Arbeitgeber auch private Endgeräte von Mitarbeitern oder Familienangehörigen, die Mitarbeiter dienstlich nutzen dürfen, oder privat genutzte Dienste überprüfen darf. An dieser Stelle muss eine Lösung entwickelt werden, die einerseits den rechtlichen Vorgaben genügt, andererseits die Interessen der Arbeitnehmer in gebotenem Maße berücksichtigt.

Aufgabenwahrnehmung des behördlichen Datenschutzbeauftragten

Die soeben zum Prüfungsrecht der Aufsichtsbehörde genannte Problematik gilt entsprechend für die Wahrnehmung der Aufgaben durch den behördlichen Datenschutzbeauftragten. Dieser hat nämlich gem. § 4g Abs. 1 S. 4 Nr. 1 BDSG die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen. Diese Überwachungspflicht wird beim Einsatz privater Endgeräte für dienstliche Zwecke enorm erschwert. Grundsätzlich erscheint eine Überprüfung nur während der Arbeitszeiten und dann auch nur im Hinblick auf die dienstlichen Datenbestände möglich.

Löschungspflichten

Aus datenschutzrechtlicher Sicht ist ferner darauf zu achten, dass solche Daten, zu deren Löschung die verantwortliche Stelle verpflichtet ist (vgl. §§ 20 Abs. 2, 35 Abs. 2 BDSG), auch auf dem Gerät des Arbeitnehmers gelöscht werden müssen. Die

Legitimation zur Speicherung der jeweiligen Daten entfällt nämlich auf sämtlichen Systemen, auf denen diese Daten verarbeitet wurden. Dies gilt mit Blick auf den Zweckbindungsgrundsatz insbesondere immer dann, wenn die Bereithaltung zur Zweckerfüllung nicht mehr erforderlich ist (§§ 20 Abs. 2 Nr. 2, 35 Abs. 2 S. 2 Nr. 3 BDSG). Denn der Zweckbindungsgrundsatz besagt, dass personenbezogene Daten nur für von vornherein festgelegte eindeutige und rechtmäßige Zwecke erhoben werden dürfen und im Nachhinein nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen (vgl. etwa §§ 4 Abs. 3, 14 Abs. 1 oder 28 Abs. 1 S. 2 BDSG).

II. Datensicherheit

Neben den bisher ausgeführten Punkten müssen bei der Einführung von „BYOD“ auch die datenschutzrechtlichen Vorschriften zum Thema Datensicherheit berücksichtigt werden.

Datengeheimnis

Das Datengeheimnis aus § 5 S. 1 BDSG besagt, dass es den bei der Datenverarbeitung beschäftigten Personen untersagt ist, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Sobald ein Mitarbeiter Zugriff auf personenbezogene Daten hat oder mit dienstlichen personenbezogenen Daten umgeht, unterliegt er dem Datengeheimnis. Beim Einsatz von privaten Endgeräten für dienstliche Zwecke stellt dies wegen der mangelnden oder gar fehlenden Abschottung gegenüber Dritten ein erhebliches Sicherheitsproblem dar. Sofern nämlich neben dem Mitarbeiter auch Dritte – wie etwa Familienangehörige – das private Endgerät benutzen, kann eine Übermittlung der Daten durch Bereitstellen zur Einsicht i. S. d. § 3 Abs. 4 Nr. 3 lit. b BDSG vorliegen. Dies würde eine Verlet-zung geltenden Datenschutzrechts darstellen, da in einem solchen Fall weder eine Einwilligung noch ein anderer Erlaubnistatbestand einschlägig wäre. Des Weiteren ist auch an dieser Stelle die bereits oben dargestellte Problematik zu beachten, dass die Kontrollmöglichkeiten des Arbeitgebers bei der Nutzung privater Geräte zunächst stark eingeschränkt sind, sodass er kaum sicherstellen kann, dass betriebliche Daten nicht an Dritte weitergegeben werden.

Bei der Einführung von „BYOD“ sollte in einigen Branchen auch ein besonderes Augenmerk auf § 42a BDSG gerichtet werden. Nach dieser Vorschrift sind unberechtigte Zugriffe auf bestimmte, vom Gesetz privilegierte Datenarten dem Betroffenen und der Aufsichtsbehörde bekanntzugeben (sog. „Skandalisierungspflicht“). Diese Meldepflicht kann beispielsweise durch den Verlust eines privaten Endgerätes, auf dem einem Berufsgeheimnis unterliegende Daten gespeichert sind, ausgelöst werden. Dieser besonderen Informationspflicht bei unrechtmäßiger Kenntniserlangung unterfallen besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG; § 42a S. 1 Nr. 1 BDSG), personenbezogene Daten, die einem Berufsgeheimnis unterliegen (§ 42a S. 1 Nr. 2 BDSG), personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen § 42a S. 1 Nr. 3 BDSG, oder personenbezogene Daten zu Bank- oder Kreditkartenkonten (§ 42a S. 1 Nr. 4 BDSG). Die Bedeutung dieser Skandalisierungspflicht für Hochschulen ist indes gering, da nur wenige Landesdatenschutzgesetze eine ähnliche Vorschrift vorsehen (vgl. § 18a BlnDSG, § 18a LDSG RP, § 14b DSG-LSA, § 27a LDSG SH). Anders sieht es hingegen bei Forschungseinrichtungen aus, die den Vorschriften des BDSG unterliegen.

Technische und organisatorische Maßnahmen

Als verantwortliche Stelle ist der Arbeitgeber verpflichtet, bestimmte technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten. Diese Pflicht ergibt sich aus § 9 S. 1 BDSG und der dazugehörigen Anlage, in welcher die zu erfüllenden Anforderungen konkretisiert sind. Dazu gehören Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrollen sowie die Möglichkeit der getrennten Verarbeitung von zu unterschiedlichen Zwecken erhobener Daten. Sowohl öffentliche als auch nichtöffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, sind insofern als verantwortliche Stellen einzustufen.

Die einzelnen technischen und organisatorischen Maßnahmen sind nach § 9 S. 2 BDSG aber nur dann erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (sog. „Erforderlichkeitsgrundsatz“). Problematisch ist, dass die Offenbarung dienstlicher Daten an Dritte (etwa Familienangehörige, Freunde oder Bekannte), die ebenfalls Zugriff auf das mitarbeitereigene Endgerät haben, nicht gänzlich ausgeschlossen werden kann.

Durch die dienstliche Nutzung privater Endgeräte besteht somit die Gefahr, dass die erforderliche Datensicherheit durch die Mitarbeiter nicht garantiert wird. Im Zweifel kann sich der Arbeitgeber dann nicht auf § 9 S. 2 BDSG berufen, da die Erforderlichkeit einschlägiger Maßnahmen aufgrund der latenten Gefahr der Offenbarung dienstlicher Daten stets zu bejahen ist.

Dabei hängt der zu fordernde Standard stark von zwei entscheidenden Faktoren ab: einerseits spielt die Art der gespeicherten Daten eine Rolle, andererseits ist der Sicherheitsstandard der verwendeten Endgeräte entscheidend. Übliche kostenlose Anti-Virenprogramme oder Firewalls werden in diesem Zusammenhang regelmäßig nicht ausreichen. Als Faustformel gilt: Je sensibler die Daten sind, desto eher ist eine Verarbeitung dieser Daten auf privaten Endgeräten unzulässig! Eine Zulässigkeit ist allenfalls dann zu bejahen, wenn der Arbeitgeber den Zugang der zugelassenen Personenkreise durch Kontrollmechanismen sowohl auf private als auch auf dienstliche Geräte gleichermaßen kontrollieren kann und Kontrollmöglichkeiten hinsichtlich sämtlicher auf den Geräten gespeicherter Daten bestehen.

III. Handlungsempfehlungen

Wie deutlich gemacht wurde, gilt es sowohl aus datenschutzrechtlicher Sicht als auch im Bereich der Datensicherheit eine Vielzahl von Punkten zu beachten, um eine rechtmäßige Einführung von „BYOD“ zu gewährleisten. Die nachfolgende Darstellung der Handlungsempfehlungen soll gleichzeitig als eine Art Checkliste dienen.

1. Neben konkreten Regelungen in Dienst- bzw. Betriebsvereinbarungen ist der Abschluss einer schriftlichen Vereinbarung mit jedem Arbeitnehmer über den Einsatz der privaten Geräte für dienstliche Zwecke empfehlenswert. Zur Eindämmung der genannten Gefahren sollte sich der Arbeitgeber Kontrollrechte auf dem privaten Endgerät einräumen lassen. Auf diese Weise kann auch der Datenschutzbeauftragte seine Pflichten erfüllen. Gleiches ist im Hinblick auf die Kooperationspflicht mit der Datenschutzaufsicht notwendig. Die Kontrollmaßnahmen sind inhaltlich im Sinne des Verhältnismäßigkeitsprinzips im privaten Bereich der Arbeitnehmer aufgrund der oben erwähnten restriktiven Rechtsprechung der Arbeitsgerichte auf das betrieblich absolut notwendige Maß zu beschränken. Hier empfiehlt sich insbesondere ein abgestufter Maßnahmenkatalog. Dabei muss den Maßnahmen oberste Priorität zukommen, die gewährleisten, dass der Arbeitgeber keine privaten Daten zur Kenntnis nimmt.

2. Die Nutzung privater Geräte zu dienstlichen Zwecken hat die Eingliederung dieser Geräte in die dienstliche IT-Infrastruktur und damit eine Vermischung von privaten und dienstlichen Endgeräten zur Folge. Der Datenschutzbeauftragte ist grundsätzlich nicht zur Kontrolle der privaten Endgeräte befugt. Dennoch sollten Möglichkeiten geschaffen werden, mit denen er die Einhaltung des Datenschutzes auf privaten Geräten in dienstlicher Nutzung kontrollieren und die Ordnungsmäßigkeit der Anwendungen überwachen kann. Nur auf diese Weise kann der gebotene Datenschutz sowie die erforderliche Datensicherheit für die dienstlichen Daten gewährleistet werden. Dabei verlässt er aber den Bereich des Zulässigen, wenn er von privaten Daten Kenntnis erlangt, wie beispielsweise beim Einblick in private E-Mails.

3. Aufgrund der besonderen Umstände bei der dienstlichen Nutzung privater Endgeräte sollte der Arbeitgeber seine Mitarbeiter hinsichtlich des Umgangs mit „BYOD“ (nach-) schulen. Insbesondere muss dabei ausdrücklich klargestellt werden, dass eine Einsichtnahme durch Dritte in die sich auf dem Gerät befindlichen dienstlichen Daten unzulässig ist. im Idealfall ist die Weitergabe des Gerätes an Dritte (auch an Familienangehörige) zu untersagen. Letzteres kann aber nur bei einem Einverständnis des jeweiligen Mitarbeiters erfolgen. Daneben erscheint die tatsächliche Durchsetzbarkeit bzw. Überwachung eines dahingehenden Weitergabeverbots nahezu unmöglich.

4. Zwar ist ein Arbeitnehmer im Rahmen von „BYOD“ nicht als Auftragsdatenverarbeiter des Arbeitgebers anzusehen. Dennoch muss der Arbeitgeber die erforderlichen technischen und organisatorischen Maßnahmen nach § 9 BDSG treffen, um die Datensicherheit und den Datenschutz zu gewährleisten. Die Vorschrift des § 9 BDSG gilt nämlich gerade auch für eine Verarbeitung durch die verantwortliche Stelle selbst (was bei einer Datenverarbeitung durch die Mitarbeiter der Fall ist). Dementsprechend sollte der Arbeitnehmer auf die Beachtung und Umsetzung dieser Maßnahmen schriftlich verpflichtet und gleichzeitig regelmäßige Kontrollen

vereinbart werden. Auch an dieser Stelle wird deutlich, dass die Einzelheiten zur Gewährleistung der Datensicherheit und des Datenschutzes zwischen Arbeitgeber und Arbeitnehmer vertraglich vereinbart werden müssen. Dabei sollten diese Regelungen auch Informationen zur Ausgestaltungen der privaten Nutzung enthalten, was aufgrund der Verbindung und Vermischung von dienstlicher und privater Nutzung des Gerätes geboten erscheint. Vorgaben sind an dieser Stelle vor dem Hintergrund der Grundrechte jedoch wieder auf das betrieblich absolut notwendige Maß zu beschränken.

5. Abgesehen von den technischen Sicherungsmaßnahmen seitens des Arbeitgebers sollte der Arbeitnehmer in Korrespondenz mit der restriktiven Geräteweitergabe verpflichtet werden, dass unbefugte Dritte (etwa Ehepartner, Lebenspartner, Kinder, Freunde oder Bekannte) keinerlei Zugriff auf Unternehmensdaten haben. Aufgrund der möglicherweise bestehenden Skandalisierungspflicht nach § 42a BDSG ist auf eine zeitnahe Verlustanzeige hinzuwirken. Diesbezüglich kann eine Unterweisung der Mitarbeiter im Zuge der Einführung von „BYOD“ hilfreich sein. Im Übrigen dient die Pflicht zur unverzüglichen Verlustanzeige auch den eigenen Interessen der Hochschule, da somit gegebenenfalls über die Fernsperrung von Nutzeraccounts ein Bekanntwerden sonstiger geheimer Daten verhindert werden kann (s. auch Punkt 12).

6. Daneben sollten klare Regelungen hinsichtlich der Nutzung des Gerätes bei privaten oder dienstlichen Reisen ins Ausland getroffen werden. Beispielsweise die Sicherheitsorgane einiger Länder (insbesondere die Finanzbehörden) sind nämlich teilweise zum Zugriff auf private Daten berechtigt.

7. Die immer populärer werdenden Cloud-Dienste stellen ebenfalls ein Risiko im Rahmen von „BYOD“ dar. Der Arbeitgeber sollte die privaten Geräte vor der Freigabe für die betriebliche Nutzung auf die dort vorhandenen Cloud-Dienste und deren Konfiguration überprüfen. In diesem Zuge ist die Unterbindung automatischer Backups von betrieblichen Daten in der Cloud empfehlenswert. In gleicher Manier sollte mit systemeigenen oder durch die Mitarbeiter eingerichteten Backups auf den privaten Geräten der Arbeitnehmer verfahren werden, da die Daten im Zuge solcher Backups (möglicherweise auf externen Speichermedien der Arbeitnehmer) gänzlich der Kontrolle des Arbeitgebers entzogen sind. In diesem Zusammenhang können auch Wartungspflichten für die privaten Endgeräte geregelt werden, sofern dies nicht bereits an anderer Stelle geschehen ist.

8. Neben der rechtlichen Ausgestaltung muss der Arbeitgeber insbesondere auch für die entsprechende technische Umsetzung sorgen (wie etwa verschlüsselte Container oder Terminal-Lösungen). Hier sollte keine andere Behandlung als bei betrieblichen Geräten, die außerhalb des Betriebsgeländes genutzt werden, erfolgen. Der Einsatz von geeigneter Sicherheits- sowie Verschlüsselungssoftware ist unabdingbare Voraussetzung bei der Einführung von „BYOD“. Es empfiehlt sich die arbeitgeberseitige Bereitstellung von geeigneter Sicherheits- sowie Verschlüsselungssoftware für die dienstliche Nutzung der privaten Endgeräte. Auf diese Weise kann die notwendige Datensicherheit gewährleistet werden. An dieser Stelle sind allerdings die urheberrechtlichen Aspekte zu berücksichtigen, die bereits im zweiten Teil dieser Aufsatzreihe (siehe dazu: Kuta, Die rechtlichen Herausforderungen von „Bring Your Own Device“ – Lifestyle contra Sicherheit – Teil 2: Arbeitsrecht, Haftungsrecht, DFN-Infobrief Recht (06/2015)) besprochen wurden. Neben den vertraglichen Regelungen wird dazu geraten, den Arbeitnehmer auf technischer Ebene zur Trennung von privaten und dienstlichen Daten auf dem Endgerät zu verpflichten.

9. Im Rahmen der technischen Umsetzung schwirren hinsichtlich eines effektiven Mobile Device Managements (MDM) eine Vielzahl von Begriffen umher, wie etwa Verschlüsselungs- und Synchronisationssoftware, Sandboxing (= Container), Data-Loss-Prevention, Theft-Recovery, Remote-Wipe, VPN oder Remote-Desktop-Applikationen. Auf technischer Ebene kommen mit Blick auf den Datenschutz sowie die Datensicherheit diverse Möglichkeiten in Betracht, wobei an dieser Stelle einige exemplarisch angesprochen werden. So können verschlüsselte Container eingesetzt werden (Container-Apps; dabei wird ein Datenbereich in einem Container abgekapselt, wobei es sich bei diesen separierten Daten in den meisten Fällen um die dienstlichen Daten handelt). Häufig werden in diesem Zusammenhang auch Terminalserver-Lösungen (bzw. Remotedesktopdienste = RDP-Dienste) besprochen.

Andere PCs können die darauf laufenden zentralen Anwendungen als Ein-/Ausgabegeräte verwenden, wobei auf den einzelnen PCs keinerlei Dateien gespeichert werden. Das dahinterstehende Prinzip verfolgt den Zweck, dass eine Anwendung nur einmal zentral installiert wird und mehrere PCs dann über das Netz darauf zugreifen und diese Anwendung verwenden können. Insgesamt kann durch derartige technische Maßnahmen einerseits eine Kontrolle erfolgen, ohne dass private Daten des Arbeitnehmers betroffen wären. Andererseits kann illegal installierter Software der Zugriff auf das Unternehmensnetzwerk verweigert werden.

10. Eine technische Aufteilung des privaten Endgeräts in dieser Gestalt kann auch eine Lösungsmöglichkeit für weitere Elemente der IT-Struktur (Firewalls, Spam- und Virenschutz, Verschlüsselung, Serververwaltung) darstellen. Daneben erscheint die Nutzung der betrieblichen Daten auf dem privaten Gerät über einen gesicherten Fernzugriff als sehr empfehlenswert.

11. Die privaten Daten auf den Geräten der Mitarbeiter sind deren Privatsphäre zuzuordnen und daher vor dem Zugriff durch den Arbeitgeber geschützt. Nichtsdestotrotz muss der Arbeitgeber die betrieblichen Daten auf diesen privaten Geräten nutzen, bearbeiten und löschen können. Aus diesem Grund empfehlen sich entsprechende Regelungen, die ausdrücklich mit den Arbeitnehmern zu vereinbaren sind. Eine Löschung privater Daten seitens des Arbeitgebers sollte dabei nur für absolute Notfälle vorgesehen werden. Dabei spielt die Festlegung des Speicherortes für dienstliche Daten eine wichtige Rolle. Mit Blick auf die lokale Speicherung von Daten sollte ausdrücklich geklärt und festgehalten werden, ob und wie dienstliche Daten auf den privaten Geräten der Arbeitnehmer gespeichert werden dürfen. Durch eine lokale Speicherung dienstlicher Daten wird nämlich der Zugriff des Arbeitgebers auf diese Daten erheblich erschwert. Aus denselben Gründen sollten auch private und dienstliche E-Mails voneinander getrennt in separaten Ordnern oder Containern abgespeichert werden. Konkrete Handlungsanweisungen und Vereinbarungen mit den Arbeitnehmern sollten die technischen Vorkehrungen flankieren, um vor allem auch den Geheimnisschutz zu gewährleisten.

12. Ein effektives Identitätsmanagement zur Eingabekontrolle kann einen Drittzugriff wirksam beschränken. Daneben gewährleisten Synchronisations- und Backup-Tools die dauerhafte Verfügbarkeit dienstlicher Daten, wodurch insbesondere der Anlage zu § 9 S. 1 BDSG nachgekommen wird. Gleiches gilt für Verschlüsselungsmethoden sowohl alleine auf dem privaten Gerät als auch für die Kommunikation zwischen dem privaten Endgerät und der Unternehmens-IT. Die bereits angesprochenen Container-Lösungen können mit einem sog. Remote-Wipe kombiniert werden. Auf diese Weise kann der Container bei Verlust des privaten Endgeräts oder einem Missbrauchsverdacht per Fernzugriff gelöscht werden. Bei aller Euphorie für diese Funktion einer ferngesteuerten Löschung stößt sie in Technikerkreisen jedoch auf große Skepsis, da die Ausführung der Funktion nicht hinreichend sichergestellt ist oder sogar verhältnismäßig einfach verhindert werden kann.

13. Sofern der Mitarbeiter der Kontrolle durch den Arbeitgeber in Folge der aufgezeigten Maßnahmen nicht zustimmt, sollte explizit ein Widerruf zur Erlaubnis von BYOD vorbehalten werden (auf die Beendigungstatbestände wird in Teil 4 dieser Reihe genauer eingegangen).

Teil 4: Weitere rechtliche Facetten, Beendigungstatbestände

In diesem Teil wird das Konzept im Hinblick auf rechtliche Facetten (Aufbewahrungspflichten, Geheimnisschutz, Strafrecht, Steuerrecht), die von den bisherigen Ausgaben nicht abgedeckt wurden, sowie Beendigungstatbestände beleuchtet. Am Ende der Darstellung werden auch in diesem Artikel wieder Handlungsempfehlungen beschrieben, die gleichzeitig als eine Art Checkliste genutzt werden können.

I. Weitere rechtliche Facetten

Neben den rechtlichen Bereichen, mit denen sich die ersten drei Teile dieser Beitragsserie beschäftigt haben, gibt es weitere rechtliche Facetten, die bei der Einführung von „BYOD“ beachtet werden sollten. Da es sich hierbei aber nur um Randbereiche handelt, werden diese Themen hier gesammelt vorgestellt. Aufgrund der kurzen Darstellung werden die Handlungsempfehlungen diesmal am Ende jedes Rechtsbereichs beschrieben.

Aufbewahrungspflichten

Betriebliche Dokumente müssen revisionssicher archiviert werden. Es existiert eine Vielzahl von gesetzlichen Aufbewahrungspflichten (z. B. § 257 Handelsgesetzbuch (HGB), § 147 Abgabenordnung (AO), diverse Vorgaben aus den Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)), die es zu beachten gilt. Diese Vorschriften stellen zwingende steuer- und bilanzrechtliche Vorgaben an die Dokumentation von Geschäftsvorgängen auf. Die Aufbewahrungsfristen betragen dabei häufig 6 oder 10 Jahre.

Dementsprechend muss durch Vereinbarungen mit dem Arbeitnehmer sichergestellt werden, dass diesen Aufbewahrungs- und Archivierungspflichten nachgekommen wird. Dies gilt insbesondere für Geschäftsvorgänge, die über private Endgeräte abgewickelt werden. Einer Vermischung von privaten und geschäftlichen Daten ist schon auf der Ebene der technisch-organisatorischen Maßnahmen zu begegnen. Geschäftsrelevante Aufzeichnungen, insbesondere geschäftliche E-Mails, dürfen nicht ausschließlich im privaten Bereich des Endgerätes be- und verarbeitet werden, sodass sie am AG „vorbeilaufen“. Zur Erfüllung von Aufbewahrungspflichten ist es nämlich notwendig, dass die Daten zusätzlich auch beim Arbeitgeber (beispielsweise auf dessen Servern) gespeichert werden. Es ist gerade im Rahmen von „BYOD“ zu beachten, dass etwa die Finanzverwaltung für eine Überprüfung jederzeit unmittelbaren Zugriff auf alle privaten Geräte der Mitarbeiter erhalten muss, sofern die den Aufbewahrungspflichten unterliegenden Dokumente nur auf den privaten Endgeräten der Mitarbeiter gespeichert sind. Eine revisionssichere Archivierung beim Arbeitgeber und eine damit einhergehende regelmäßige Synchronisation der Datenbestände sind daher unumgänglich.

Geheimnisschutz und Strafrecht

Neben dem in anderen Artikeln bereits angesprochenem Schutz von personenbezogenen Daten ist im Zuge von „BYOD“ der Schutz von Betriebs- und Geschäftsgeheimnissen in Form eigener und fremder (Forschungs-/Hochschul-/Unternehmens-) Daten sowie der Schutz von Privatgeheimnissen Dritter zu berücksichtigen. Die Sicherheitsmaßnahmen (insbesondere Virenschutzprogramme und Firewalls) auf den privaten Geräten werden meist unter denen der dienstlichen Geräte liegen. Dadurch kann es zu einer Offenbarung gegenüber Providern und anderen Dritten kommen. An dieser Stelle rücken die Straftatbestände des Ausspähens von Daten nach § 202a Strafgesetzbuch (StGB) und des Abfangens von Daten nach § 202b StGB in den Fokus. Durch die Einbindung privater Endgeräte in die Kommunikationssysteme des Arbeitgebers sind ggfs. auch die §§ 202c StGB (Vorbereiten des Ausspähens und Abfangens von Daten), 203 StGB (Verletzung von Privatgeheimnissen) und 303a StGB (Datenveränderung) von Bedeutung. Beim Auslesen und Verändern von unternehmenseigenen Daten wird jedoch meist kein rechtswidriger Zugriff erfolgen, sodass in diesem Fall keine Strafbarkeit im Raum steht. Daneben muss die Tatbestandsvoraussetzung von § 202a StGB, die besondere Sicherung der Daten gegen einen

unberechtigten Zugang, in jedem Einzelfall genau geprüft werden. Eine pauschale Beurteilung ist diesbezüglich nicht möglich. Unter besonderen Sicherungsmaßnahmen sind in diesem Zusammenhang diejenigen der jeweiligen Einrichtung gemeint und gerade nicht die der Arbeitnehmer. Trotz dieser auf den ersten Blick bestehenden Einschränkungen kann jedoch auch im Rahmen von „BYOD“ eine Strafbarkeit wegen des Ausspähens, Abfangens und Veränderns von Daten vorliegen.

Die fahrlässige Begehung dieser Tatbestände durch den fehlerhaften Umgang mit dem Datenverarbeitungsgerät ist nach § 15 StGB straflos. Gegen die vorsätzliche Verwirklichung bestehen unterdessen keine IT-sicherheitstechnischen Mittel. Die vorsätzliche Begehung ist strafbar, jedoch stehen dem Arbeitgeber keine technischen Mittel zur Verfügung, um die Verwirklichung der Straftatbestände durch seine Arbeitnehmer von vornherein zu verhindern. In diesem Fall muss man auf die Lenkungswirkung des Strafrechts vertrauen. Neben diesen Regelungen aus dem Strafgesetzbuch sind die wettbewerbsrechtlichen Vorschriften der §§ 17, 18 Gesetz gegen den unlauteren Wettbewerb (UWG) zu berücksichtigen, die ebenfalls den Verrat von Geschäfts- und Betriebsgeheimnissen (§ 17 UWG) sowie die Verwertung von Vorlagen (§ 18 UWG) unter Strafe stellen.

Im Hinblick auf Geheimhaltungsinteressen müssen Arbeitnehmer geschult und sensibilisiert werden. Dabei können Hinweise in BYOD-Richtlinien auf die strafrechtlichen Sanktionen im Falle eines Verstoßes Lenkungswirkung haben. Mobile Device Management-Lösungen können einen Großteil der strafrechtlichen Probleme ausklammern, sodass ein Dateizugriff über diese Systeme eingerichtet werden sollte. Mitarbeitereigene Daten sollten von einem Zugriff konsequent ausgeschlossen werden. An dieser Stelle rückt auch der sog. Remote-Wipe in den Fokus, der schon im 3. Teil dieser „BYOD“-Serie beim Thema Datenschutzrecht und Datensicherheit angesprochen wurde. Durch die Initialisierung eines Remote-Wipe werden alle Daten auf dem betroffenen Gerät gelöscht und unbrauchbar gemacht. Dies kann strafrechtliche Probleme aufwerfen. Die vorherige Einwilligung des Arbeitnehmers in den Remote-Wipe stellt ein tatbestandsausschließendes Einverständnis (bei Straftatbeständen, die notwendigerweise ein Handeln gegen oder ohne den Willen des Betroffenen voraussetzen, willigt dieser dabei ein, dass schon der entsprechende Straftatbestand nicht gegeben ist) dar. Mit der Verlustanzeige an die Hochschule/die Forschungseinrichtung/das Unternehmen kann aber die Löschbewilligung gleichzeitig widerrufen werden. Die Durchführung des Remote-Wipe hätte in diesem Fall strafrechtliche Konsequenzen. Um alle Unwägbarkeiten bestmöglich abzusichern, ist eine Mobile Device Management-Lösung erforderlich, die bis ins kleinste Detail ideal auf die jeweilige Einrichtung und deren Besonderheiten abgestimmt ist. Dabei muss die selektive Löschung von Daten möglich sein. Vergegenwärtigt man sich den gesetzlichen Rahmen und hält diesen konsequent ein, gehen damit zwei Vorteile einher: Es hilft einerseits bei dem technischen Schutz vor Missbräuchen, andererseits unterstützt es die Einführung und Umsetzung von BYOD.

Steuerrecht

Die Vorteile des Mitarbeiters aus der privaten Nutzung von betrieblichen Endgeräten ist neuerdings nach § 3 Nr. 45 Einkommensteuergesetz (EStG) steuerfrei. Vom Wortlaut sind aber keine Geräte umfasst, die sowieso dem Arbeitnehmer gehören und deren Anschaffung vom Arbeitgeber besonders vergütet wird. Damit scheidet eine Anwendung von § 3 Nr. 45 EStG im Rahmen von „BYOD“ aus. Es kommt gegebenenfalls aber eine Steuerfreiheit für Auslagenersatz nach § 3 Nr. 50 EStG oder ein Abzug für Werbungskosten nach § 9 Abs. 1 S. 2 EStG infrage. Ausschließlich dem Privatbereich entspringende Aufwendungen dürfen nach § 12 Nr. 1 EStG aber keine Berücksichtigung finden. Im Hinblick auf das Umsatzsteuerrecht ist „BYOD“ derzeit nicht ausdrücklich vom Gesetz erfasst.

Es sind genaue arbeitsvertragliche Regelungen zur BYOD-Vergütung erforderlich, damit die soeben angesprochenen steuerlichen Vorteile genutzt werden können. Gleichzeitig wird durch solche Vereinbarungen auch Klarheit zwischen den Parteien geschaffen, sodass mögliche Ungereimtheiten über eine gesonderte Vergütung für eingebrachte Geräte gar nicht erst aufkommen können.

II. Beendigungstatbestände

Das eingebrachte Endgerät steht im Eigentum des Arbeitnehmers. Die dort abgespeicherten Daten können zum Teil nicht eindeutig dem privaten oder dienstlichen Bereich zugeordnet werden. Scheidet ein Mitarbeiter aus der Einrichtung aus, müssen sämtliche Dienstmittel an den Arbeitgeber zurückgegeben werden. Von dieser Rückgabepflicht sind auch Daten umfasst, wobei diese in der Regel schon aufgrund der

Synchronisation neben der lokalen Speicherung auf dem privaten Endgerät auch auf den Servern des Arbeitgebers liegen. Dementsprechend genügt die Löschung dieser dienstlichen Daten auf dem mitarbeitereigenen Gerät. Neben dem Ausscheiden des Mitarbeiters kann es auch vorkommen, dass Mitarbeiter den internen „BYOD“-Richtlinien nach einiger Zeit widersprechen.

Für die geschilderten Fälle sollten Beendigungstatbestände in die „BYOD“-Vereinbarung aufgenommen werden. Auf diese Weise können Unklarheiten von vornherein vermieden werden. Zu denken wäre hierbei an eine Befristungsregelung (etwa für eine Erprobungsphase), an ein Widerrufsrecht oder an ein Kündigungsrecht der „BYOD“-Erlaubnis. Insbesondere sollten dabei Regelungen zur Aushändigung der betrieblichen Daten an den Arbeitgeber nach Beendigung des Arbeitsverhältnisses getroffen werden. Aus dieser Regelung muss deutlich hervorgehen, welche Daten vom Mitarbeiter herauszugeben sind und welche Dateien sowie Dateikopien (möglicherweise auch auf externen Speichermedien) rückstandslos gelöscht werden müssen. Das Herausgaberecht ergibt sich aus § 667 Bürgerliches Gesetzbuch (BGB). Um den Löschungspflichten vorzubeugen, kann auch geregelt werden, dass dienstliche Daten nur auf dem „dienstlichen Container“ bzw. den virtuellen dienstlichen Laufwerken und nicht lokal auf dem mitarbeitereigenen Endgerät abgespeichert werden dürfen.

Teil 5: Fazit, Alternativen, Checkliste

In diesem abschließenden Teil wird ein Gesamtfazit zum Thema „BYOD“ gezogen, Alternativen aufgezeigt und eine Checkliste an die Hand gereicht, in der noch einmal die wichtigsten Punkte aufgeführt sind, die es zu beachten gilt.

I. Fazit

Die Nutzung privater Endgeräte zu dienstlichen Zwecken ist aus rechtlicher Sicht mit vielen Risiken behaftet. Mit der Einführung von „BYOD“ kann ein erheblicher Einfluss- und Kontrollverlust des Arbeitgebers einhergehen. Wie aus den vorherigen Beiträgen deutlich hervorgeht, besteht daneben ein hohes Haftungsrisiko des Arbeitgebers, etwa für Schäden an den Geräten sowie bei Datenverlusten, oder für Datenschutz- und Urheberrechtsverstöße. Diesen Risiken stehen Einsparungspotentiale, etwa bei der Anschaffung neuer IT oder dahingehenden Schulungen der Mitarbeiter, gegenüber. Letztlich handelt es sich also um eine betriebswirtschaftliche Entscheidung der jeweiligen Einrichtung. Zum gegenwärtigen Zeitpunkt ist noch unklar, ob die individual- sowie kollektivvertraglichen (insbesondere Dienst- und Betriebsvereinbarungen) Vereinbarungen den tendenziell restriktiven Anforderungen der Gerichte gerecht werden können. Eines der größten Probleme dabei ist die derzeit fehlende Rechtsprechung sowie die mangelnden spezifischen gesetzlichen Regelungen zu dieser Thematik. Die Risiken im Hinblick auf getroffene Vereinbarungen sind nicht kalkulierbar. Auch das Problem einer betrieblichen Übung sollte nicht unberücksichtigt bleiben. So kann ein Arbeitnehmer das Recht hinsichtlich der Benutzung eigener Endgeräte erwerben, obwohl die IT der betroffenen Einrichtung keine geeigneten Vorkehrungen dafür vorsieht. Im Gegensatz dazu ist eine für den Arbeitnehmer nachteilige betriebliche Übung in der Form, dass er seine privaten Endgeräte obligatorisch einsetzen muss, nicht zu erwarten.

Die Zulassung von „BYOD“ muss das Ergebnis einer umfassenden Analyse rechtlicher und IT-spezifischer Risiken sein, wobei die Risikobewertung anhand von konkreten Hard- und Softwarekombinationen erfolgen muss. Hierbei ist die Zusammenarbeit von IT-, Datenschutz- und Rechtsabteilung sinnvoll. Sollen die erforderlichen technischen und organisatorischen Maßnahmen durchgehend eingehalten werden, werden der Administrationsaufwand steigen und die Eigentumsrechte der Mitarbeiter an ihrem Endgerät erheblich beschränkt. Dadurch können sich die erwartete Kostenersparnis sowie die gesteigerte Mitarbeiterzufriedenheit schnell gegenteilig auswirken. In jedem Fall sind eindeutig formulierte „BYOD“-Richtlinien mit konkreten Hinweisen auf die genaue Ausgestaltung von „BYOD“ unumgänglich. Sofern insbesondere ein angemessenes Datenschutzniveau nicht gewährleistet werden kann, ist auf den Einsatz von „BYOD“ wohl oder übel komplett zu verzichten. Die ausdrückliche Untersagung der Nutzung privater Endgeräte für dienstliche Zwecke ist bis dato die einzig rechtssichere Möglichkeit zur Handhabung von „Bring Your Own Device“. Aus dem Schlagwort „BYOD“ wird somit eher „DBYOD“ („Don‘t Bring Your Own Device“). Durch eindeutige Regelungen (oder ggf. einen Totalvorbehalt) müssen „BYOD“-Wildwuchs und „Schatten-IT“ verhindert werden. Bei der Planung von „BYOD“ sollten daher auch alternative Konzepte in den Blickwinkel der jeweiligen Einrichtung rücken.

II. Alternativen

Neben „BYOD“ gibt es einige alternative Möglichkeiten, um das Thema der benutzerfreundlichen IT an Hochschulen, in Forschungseinrichtungen und Unternehmen anzugehen. Eine dem „BYOD“-Konzept sehr ähnliche Variante ist das sog. „Choose Your Own Device“ („CYOD“). Dabei schafft der Arbeitgeber die einzusetzenden Geräte selbst an, was dem derzeitigen Ablauf in den jeweiligen Einrichtungen entsprechen wird. Auf diese Weise können seitens der IT-Abteilung die möglichen Hard- und Softwarekombinationen eingegrenzt und die zu verwendenden Softwares sowie Apps reglementiert und freigegeben werden. Dies wirkt sich wiederum positiv auf den Administrationsaufwand aus. Widerrechtlich installierte Programme können umgehend gelöscht werden. Ein einheitliches Mobile Device Management wird sichergestellt und es bieten sich die Möglichkeiten von Mengenrabatten beim Einkauf sowie beim Abschluss von Wartungsverträgen. Der Arbeitgeber kann die Vorgaben im Hinblick auf die Gerätenutzung weitestgehend frei bestimmen, da die Geräte durch die arbeitgeberseitige Anschaffung für den geschäftlichen

Gebrauch in seinem Eigentum stehen. Sofern es sich um unternehmenseigene Hardware handelt, ist davon auszugehen, dass Arbeitnehmer die mit den datenschutzrechtlichen Vorgaben verbundenen Einschränkungen eher hinnehmen werden. Im Unterschied zur bisherigen Praxis wird dem Nutzer aber die Speicherung von persönlichen Daten erlaubt. Der Arbeitgeber kann wiederum festlegen, was zu den persönlichen Daten zählt und in welchen Festplattenbereichen diese abgespeichert werden dürfen.

Eine weitere Alternative ist das sog. „Mitarbeiter-PC-Programm“ (MPP). Hierbei handelt es sich um ein Programm der Initiative D21 (Deutschlands größte Partnerschaft von Politik und Wirtschaft zur Ausgestaltung der Informationsgesellschaft), das von der Bundesregierung unterstützt wird. Die Anschaffung der Geräte obliegt im ersten Schritt dem Arbeitgeber. Im zweiten Schritt least der Arbeitnehmer das Endgerät zur privaten Nutzung. Neben steuerlichen Vergünstigungen kommt der Arbeitgeber auch in den Genuss der soeben im Rahmen von „CYOD“ angesprochenen Vorteile.

III. Checkliste

Die Artikel in den Ausgaben 04/2015, 06/2015, 08/2015 sowie 09/2015 enthielten allesamt ausführliche Handlungsempfehlungen und Checklisten zu den einzelnen Rechtsgebieten. Die drei wichtigsten Kernpunkte bei der Einführung von „BYOD“ sollen hier aber noch einmal kurz wiedergegeben werden.

1. Sämtliche Absprachen zwischen Arbeitgeber und Arbeitnehmer sollten schriftlich festgehalten werden. Aus Gründen der Rechtssicherheit, Klarheit und Transparenz sollte dies als oberstes Gebot beachtet werden. Neben „BYOD“-Richtlinien sind hier Dienst- bzw. Betriebsvereinbarungen sowie Dienst- und Arbeitsverträge zu nennen.

2. Eine einheitliche Administration sowie die Einstellung der Geräte-Konfiguration sollte zentral durch den Arbeitgeber vorgenommen werden. Dabei wird ein effektives Mobile Device Management (MDM) erforderlich sein.

3. Der Personalrat (im öffentlichen Bereich) sowie der Betriebsrat (im nicht-öffentlichen Bereich) muss frühzeitig involviert werden, idealerweise bereits im Planungsstadium.

IV. Ausführliche Checklisten

Zur erleichterten Handhabung werden die Handlungsempfehlungen und Checklisten aus den vorhergehenden Ausgaben an dieser Stelle noch einmal gebündelt wiedergegeben.

Haftungsrecht

1. Als oberstes Gebot gilt vorweg, dass aus Gründen der Rechtssicherheit, Klarheit und Transparenz sämtliche Absprachen zwischen Arbeitgeber und Arbeitnehmer schriftlich festgehalten werden sollten.

2. Eine Vereinbarung über regelmäßige Sicherungskopien durch den Arbeitnehmer erscheint ratsam. Auf diese Weise kann ein Datenverlust weitestgehend eingeschränkt werden.

3. Zur Vermeidung von Sicherheitslücken und Datenverlusten ist eine einheitliche Administration durch den Arbeitgeber zu empfehlen. In diesem Zusammenhang sollte der Arbeitgeber einerseits geeignete Sicherheitssoftware zur Verfügung stellen, andererseits sollten betriebliche Vereinbarungen Regelungen über die Haftung bei Verlust oder Beschädigung der Geräte oder betrieblicher Daten enthalten und eindeutig festlegen, wer Reparaturen in Auftrag gibt und deren Kosten trägt. Dadurch kann für beide Parteien das Schadens- und Kostenrisiko eindeutig festgelegt werden, wer also in welchen Konstellationen haftet und welche Partei unter welchen Voraussetzungen das Betriebsrisiko trägt. Darüber hinaus sollte seitens des Arbeitgebers eine regelmäßige Wartung der Privatgeräte durchgeführt werden. Ergänzend kann der Mitarbeiter zur selbständigen Überprüfung des Geräts verpflichtet werden. Da die Betriebshaftpflichtversicherung mitarbeitereigene Hardware regelmäßig nicht abdeckt, ist der Abschluss einer gesonderten Geräteversicherung ratsam, wobei die sich daraus ergebende Kostentragungspflicht eindeutig zugewiesen und geregelt werden sollte.

4. Dem Arbeitnehmer sollte für den Fall des Verlustes eines Geräts eine Benachrichtigungspflicht auferlegt werden. Dies hat insbesondere dann zu gelten, wenn auf dem privaten Endgerät dienstliche Daten gespeichert wurden und dieses Gerät nun gestohlen worden, verloren gegangen oder auf andere Weise abhandengekommen ist. Jedoch kann ein Missbrauch selbst dann nicht ausgeschlossen

werden, wenn keine Daten auf dem Gerät gespeichert wurden, da schon die Preisgabe von Verbindungsinformationen zu IT-Systemen des Arbeitgebers diesen angreifbar machen können. Dementsprechend ist eine Benachrichtigungspflicht des Mitarbeiters bei einem Geräteverlust generell empfehlenswert.

5. Neben der einheitlichen Administration sollte die Einstellung der Geräte-Konfiguration ebenfalls zentral durch den Arbeitgeber vorgenommen werden. In diesem Zuge sollten die Arbeitnehmer im Rahmen einer Vereinbarung dazu verpflichtet werden, diese Einstellungen zu verwenden und nicht zu verändern. Ferner sollte der Zugriff auf das private Gerät von der Eingabe eines Passworts abhängig gemacht werden, sodass der Zugriff Dritter (etwa Familienangehörige) eingeschränkt wird. Auch im Hinblick auf den Schutz von Betriebs- und Geschäftsgeheimnissen ist die verbindliche Vorgabe eines Passworts ratsam, zumal diese Daten oftmals vertraglichen Geheimhaltungspflichten gegenüber Dritten unterliegen. Im Rahmen der Vereinbarung sollte der Arbeitnehmer auch verpflichtet werden, das Passwort gegenüber Dritten geheim zu halten und sicher aufzubewahren.

Arbeitsrecht

1. Als oberstes Gebot gilt auch hier, dass aus Gründen der Rechtssicherheit, Klarheit und Transparenz sämtliche Absprachen zwischen Arbeitgeber und Arbeitnehmer schriftlich festgehalten werden sollten. Bisher bestehende Dienst- bzw. Betriebsvereinbarungen sowie Dienst- und Arbeitsverträge werden keine Passus zum Themenkomplex „BYOD“ beinhalten. Daher sollten diese um entsprechende Abschnitte ergänzt werden, wobei in diesem Zusammenhang direkt auch datenschutzrechtliche Belange der Mitarbeiter konstituiert werden können. Neben Dienst- bzw. Betriebsvereinbarungen sollte daher auf Individualvereinbarungen zurückgegriffen werden. Es gilt zu beachten, dass Dienst- bzw. Betriebsvereinbarungen BDSG- und AGB-fest sein müssen (vgl. insbesondere §§ 305c Abs. 2, 307 Abs. 1 S. 2 Bürgerliches Gesetzbuch (BGB)). Dennoch sind Dienst- bzw. Betriebsvereinbarungen das „Mittel der Wahl“ bei fast allen Fragen mobiler Endgeräte in der jeweiligen Einrichtung, da mit ihnen einige Vorteile einhergehen. Es können verbindliche Vereinbarungen über sämtliche Gegenstände betrieblicher Mitbestimmung getroffen werden (vgl. § 77 Abs. 4 S. 1 BetrVG, wonach Betriebsvereinbarungen unmittelbar und zwingend gelten). Das BPersVG sowie weitestgehend die Personalvertretungsgesetze der Länder kennen keine solche Vorschrift, die Dienstvereinbarungen für unmittelbar und zwingend erklärt (vgl. § 73 BPersVG). Der Gesetzgeber hat es anscheinend als selbstverständlich angesehen, dass auch Dienstvereinbarungen unmittelbar und zwingend gelten. Dementsprechend kann § 77 Abs. 4 S. 1 BetrVG entsprechend angewendet werden. Gleichzeitig können mögliche Probleme der AGB-Inhaltskontrolle abgemildert werden (§ 310 Abs. 4 BGB). Da eine wirksame Betriebsvereinbarung zugleich als Rechtsvorschrift im Sinne des § 4 Abs. 1 BDSG gilt (vgl. die entsprechenden Vorschriften der Landesdatenschutzgesetze: § 4 Abs. 1 LDSG BW, Art. 15 Abs. 1 BayDSG, § 6 Abs. 1 BlnDSG, § 4 Abs. 1 BbgDSG, § 3 Abs. 1 BrDSG, § 5 Abs. 1 S. 1 HmbDSG, § 7 Abs. 1 HDSG, § 7 Abs. 1 DSG MV, § 4 Abs. 1 NDSG, § 4 Abs. 1 DSG NW, § 5 Abs. 1 LDSG RP, § 4 Abs. 1 S. 1 SDSG, § 4 Abs. 1 SächsDSG, § 4 Abs. 1 DSG-LSA, § 11 Abs. 1 LDSG SH, § 4 Abs. 1 ThürDSG), können datenschutzrechtliche Befugnisse des Arbeitgebers darin verankert werden, ohne auf eine Einwilligung des Arbeitnehmers angewiesen zu sein. Es muss aber beachtet werden, dass nur Pflichten des Arbeitgebers sowie Pflichten des Arbeitnehmers im Hinblick auf die Verbindung zur IT-Infrastruktur der jeweiligen Einrichtung festgelegt werden können, wohingegen Aspekte des Privatlebens des Arbeitnehmers (etwa Vorschriften über den Abschluss von Reparatur-, Wartungs- und Garantieverträgen, Software- und Hardwareanschaffung) darin nicht geregelt werden können und dafür daher individualvertragliche Vereinbarungen erforderlich sind.

2. Zur Verwaltung der im Rahmen von „BYOD“ in einer Vielzahl eingebrachten Endgeräte der Arbeitnehmer sollten die jeweiligen Gerätetypen und Softwareversionen genau bezeichnet und dokumentiert werden. Hierbei bietet sich eine hoch skalierbare Managementplattform an. Individualvertragliche Regelungen sollten in diesem Zusammenhang neben sämtlichen Kostenfragen im Hinblick auf Anschaffung, Wartung, Reparatur und Ersatz auch den Vergütungsanspruch des Arbeitnehmers für die betriebliche Nutzung beinhalten. Die Kosten sind dabei entsprechend des Anteils der jeweiligen Nutzung (dienstlich und privat) prozentual aufzuführen, wobei daneben eine Anpassungsklausel ratsam ist, da auf diese Weise Verän-

derungen in der Verteilung dieser Anteile besser nachgekommen werden kann.

3. Die Vorgaben hinsichtlich der Arbeitszeit müssen unbedingt beachtet und dementsprechende Regelungen zwischen den Parteien getroffen werden, damit keine Vermengung von Arbeitszeit und Freizeit erfolgt. Bei der Einführung von „BYOD“ sollte aus arbeitszeitrechtlicher Sicht insbesondere auf eine Verpflichtung der Arbeitnehmer zu einer ständigen Erreichbarkeit außerhalb der regulären Arbeitszeiten verzichtet werden. Dementsprechend sind klare und verlässliche Regelungen sowohl zum arbeitszeitlichen Umgang mit den privaten Geräten außerhalb der vereinbarten Arbeitszeit als auch hinsichtlich des privaten Gebrauchs während der Dienstzeit festzulegen. Hierbei können die üblichen arbeitsrechtlichen Maßstäbe zur Online-Nutzung am Arbeitsplatz als Richtwerte dienen, wobei es zu beachten gilt, dass ein zu strenges Management seitens des Arbeitgebers die Begeisterung der Arbeitnehmer für „BYOD“ schwinden lassen kann. Empfehlenswert sind Regelungen, durch die der Arbeitnehmer zur Einhaltung der Ruhezeiten nach § 5 ArbZG angehalten wird, wobei meist auch seitens des Personal- bzw. Betriebsrats dahingehende Forderungen aufkommen. Sofern absehbar ist, dass ein phasenweises Tätigwerden des Arbeitnehmers außerhalb seiner regulären Arbeitszeit unausweichlich ist und dies sogar vom Arbeitgeber veranlasst wird (etwa die Weiterleitung einer E-Mail mit der Aufforderung zur Beantwortung, das Durchleiten eines Anrufs oder die Ansetzung einer Telefon-/Videokonferenz), sollte dies ausdrücklich geregelt werden. Neben dem Arbeitszeitgesetz kommen im Rahmen von „BYOD“ auch Fragen hinsichtlich der Ableistung und Vergütung bzw. Abgeltung von Überstunden auf. Diese Punkte können im Verlauf eines „BYOD“-Programms zu Streitigkeiten führen, sodass hier idealerweise schon im Vorfeld unter Beteiligung der betroffenen Kreise (Arbeitgeber sowie Arbeitnehmervertreter) interessengerechte und eindeutige Regelungen geschaffen werden sollten.

4. Die Einführung von „BYOD“ wird regelmäßig die Mitwirkung des Personalrats (im öffentlichen Bereich) sowie des Betriebsrats (im nicht-öffentlichen Bereich) zur Folge haben. Aufgrund bestehender Unterrichtungspflichten und zur Vermeidung von Verlangsamungs- oder Verhinderungsmaßnahmen ist eine frühzeitige Einbindung dieser Organe (schon im Planungsstadium) ratsam (vgl. die oben genannten Vorschriften). Durch eine offene und transparente Vorgehensweise seitens des Arbeitsgebers können Vorbehalte und Befürchtungen frühzeitig aufgeklärt und beiseite geschafft werden.

Urheberrecht

1. Zur Verhinderung von urheberrechtlichen Verletzungshandlungen durch Unterlizenzierung muss auf die konkrete Ausgestaltung der Lizenzbestimmungen geachtet werden, insbesondere auf die Unterscheidung zwischen privaten und gewerblichen Nutzungsbefugnissen, aber auch zwischen personen- oder gerätegebundenen Lizenzen sowie Mehrplatzlizenzen. Diesbezüglich müssen seitens des Arbeitgebers regelmäßige interne Audits durchgeführt werden. Auf diese Weise kann einerseits kontrolliert werden, welche Softwares auf den privaten Endgeräten installiert sind, andererseits kann dadurch eine Unterlizenzierung verhindert werden. Die internen IT-Richtlinien sollten auf die Lizenzneuerungen im Zuge von „BYOD“ angepasst und deren Einhaltung regelmäßig überprüft werden.

2. Daneben sollte zur Minimierung des Haftungsrisikos für Urheberrechtsverletzungen sowie der aus Schadsoftware herrührenden Gefahren das betriebliche Lizenzmanagement auf die privaten Geräte in betrieblicher Nutzung erstreckt werden. Idealerweise sollten die Endgeräte der Mitarbeiter regelmäßig auf unlizenzierte, illegale oder schädliche Software überprüft werden. Dies könnte in einer Betriebsvereinbarung geregelt werden (siehe dazu bereits die obigen Ausführungen). Es erscheint jedoch unwahrscheinlich, dass ein Mitarbeiter den gesamten Inhalt seines Gerätes ohne weiteres offenlegen wird. Der Schutz der Privatsphäre der Arbeitnehmer sollte vom Arbeitgeber gefördert werden, da so mögliche Vorbehalte gegen eine Einführung von „BYOD“ abgemildert werden. Daher könnte man alternativ zu einer vollumfänglichen Offenlegungspflicht den Mitarbeiter dazu verpflichten, in regelmäßigen Abständen einen Nachweis über die ordnungsgemäße Lizenzierung der von ihm zu betrieblichen Zwecken eingesetzten Software zu erbringen. Mit dem Einverständnis des Mitarbeiters könnte man diesen Nachweis durch eine stichprobenartige Überprüfung absichern. Sofern der Arbeitnehmer derartige Überprüfungen verweigert, sollte das private Gerät nicht betrieblich verwendet werden

dürfen, was einem Widerruf von „BYOD“ in Bezug auf diesen Arbeitnehmer bedeutet. Eine sehr strikte Regelung könnte daneben vorschreiben, welche Software der Mitarbeiter auf dem dienstlichen Bereich seines Endgeräts (dazu sogleich mehr) installieren darf und dass dahingehende Kontrollen erlaubt sind. Bestehende Gewährleistungsansprüche für die eingesetzten Softwares könnten an den Arbeitgeber abgetreten oder für den Arbeitgeber geltend gemacht werden. Alternativ bieten sich auch der zentrale Einkauf sowie die Verwaltung der erforderlichen Softwares durch den Arbeitgeber an. Er kann diese direkt in sein betriebliches Lizenzmanagement einpflegen und verringert auf diese Weise die Gefahr einer Unterlizenzierung deutlich. Dabei sollte auch darauf geachtet werden, dass die erworbenen Nutzungsrechte sowohl die dienstliche als auch die private Nutzung der jeweiligen Software erlauben. Dadurch möglicherweise entstehende Mehrkosten können interessengerecht zwischen Arbeitgeber und Arbeitnehmer aufgeteilt werden, sofern die private Nutzung möglich ist, einen merklichen Anteil trägt und sich der Arbeitnehmer bewusst und freiwillig zur Teilnahme am BYOD-Programm entscheidet. Um Konflikte zu vermeiden, sollte die Kostenaufteilung schriftlich fixiert werden. Letztlich kann auch die Nutzung von Open-Source-lizenzierter Software eine Option sein.

3. Die Trennung von privaten und dienstlichen Daten auf technischer Ebene erscheint unabdingbar, um die notwendigen Kontrollmöglichkeiten seitens des Arbeitgebers umzusetzen. In diesem Zusammenhang ist an die Konfiguration virtueller Desktops (= multiple Arbeitsflächen (-bereiche)), die Partitionierung der Festplatten der Geräte, verschlüsselte Container (Container-Apps) oder Terminalserver-Lösungen zu denken. Auf diese Weise kann einerseits eine Kontrolle erfolgen, ohne dass private Daten des Arbeitnehmers betroffen wären, andererseits könnte illegal installierter Software der Zugriff auf das Unternehmensnetzwerk verweigert werden.

Datenschutzrecht

1. Neben konkreten Regelungen in Dienst- bzw. Betriebsvereinbarungen ist der Abschluss einer schriftlichen Vereinbarung mit jedem Arbeitnehmer über den Einsatz der privaten Geräte für dienstliche Zwecke empfehlenswert. Zur Eindämmung der genannten Gefahren sollte sich der Arbeitgeber Kontrollrechte auf dem privaten Endgerät einräumen lassen. Auf diese Weise kann auch der Datenschutzbeauftragte seine Pflichten erfüllen. Gleiches ist im Hinblick auf die Kooperationspflicht mit der Datenschutzaufsicht notwendig. Die Kontrollmaßnahmen sind inhaltlich im Sinne des Verhältnismäßigkeitsprinzips im privaten Bereich der Arbeitnehmer aufgrund der oben erwähnten restriktiven Rechtsprechung der Arbeitsgerichte auf das betrieblich absolut notwendige Maß zu beschränken. Hier empfiehlt sich insbesondere ein abgestufter Maßnahmenkatalog. Dabei muss den Maßnahmen oberste Priorität zukommen, die gewährleisten, dass der Arbeitgeber keine privaten Daten zur Kenntnis nimmt.

2. Die Nutzung privater Geräte zu dienstlichen Zwecken hat die Eingliederung dieser Geräte in die dienstliche IT-Infrastruktur und damit eine Vermischung von privaten und dienstlichen Endgeräten zur Folge. Der Datenschutzbeauftragte ist grundsätzlich nicht zur Kontrolle der privaten Endgeräte befugt. Dennoch sollten Möglichkeiten geschaffen werden, mit denen er die Einhaltung des Datenschutzes auf privaten Geräten in dienstlicher Nutzung kontrollieren und die Ordnungsmäßigkeit der Anwendungen überwachen kann. Nur auf diese Weise kann der gebotene Datenschutz sowie die erforderliche Datensicherheit für die dienstlichen Daten gewährleistet werden. Dabei verlässt er aber den Bereich des Zulässigen, wenn er von privaten Daten Kenntnis erlangt, wie beispielsweise beim Einblick in private E-Mails.

3. Aufgrund der besonderen Umstände bei der dienstlichen Nutzung privater Endgeräte sollte der Arbeitgeber seine Mitarbeiter hinsichtlich des Umgangs mit „BYOD“ (nach-) schulen. Insbesondere muss dabei ausdrücklich klargestellt werden, dass eine Einsichtnahme durch Dritte in die sich auf dem Gerät befindlichen dienstlichen Daten unzulässig ist. im Idealfall ist die Weitergabe des Gerätes an Dritte (auch an Familienangehörige) zu untersagen. Letzteres kann aber nur bei einem Einverständnis des jeweiligen Mitarbeiters erfolgen. Daneben erscheint die tatsächliche Durchsetzbarkeit bzw. Überwachung eines dahingehenden Weitergabeverbots nahezu unmöglich.

4. Zwar ist ein Arbeitnehmer im Rahmen von „BYOD“ nicht als Auftragsdatenverarbeiter des Arbeitgebers anzusehen. Dennoch muss der Arbeitgeber die erforderlichen techni-

schen und organisatorischen Maßnahmen nach § 9 BDSG treffen, um die Datensicherheit und den Datenschutz zu gewährleisten. Die Vorschrift des § 9 BDSG gilt nämlich gerade auch für eine Verarbeitung durch die verantwortliche Stelle selbst (was bei einer Datenverarbeitung durch die Mitarbeiter der Fall ist). Dementsprechend sollte der Arbeitnehmer auf die Beachtung und Umsetzung dieser Maßnahmen schriftlich verpflichtet und gleichzeitig regelmäßige Kontrollen vereinbart werden. Auch an dieser Stelle wird deutlich, dass die Einzelheiten zur Gewährleistung der Datensicherheit und des Datenschutzes zwischen Arbeitgeber und Arbeitnehmer vertraglich vereinbart werden müssen. Dabei sollten diese Regelungen auch Informationen zur Ausgestaltungen der privaten Nutzung enthalten, was aufgrund der Verbindung und Vermischung von dienstlicher und privater Nutzung des Gerätes geboten erscheint. Vorgaben sind an dieser Stelle vor dem Hintergrund der Grundrechte jedoch wieder auf das betrieblich absolut notwendige Maß zu beschränken.

5. Abgesehen von den technischen Sicherungsmaßnahmen seitens des Arbeitgebers sollte der Arbeitnehmer in Korrespondenz mit der restriktiven Geräteweitergabe verpflichtet werden, dass unbefugte Dritte (etwa Ehepartner, Lebenspartner, Kinder, Freunde oder Bekannte) keinerlei Zugriff auf Unternehmensdaten haben. Aufgrund der möglicherweise bestehenden Skandalisierungspflicht nach § 42a BDSG ist auf eine zeitnahe Verlustanzeige hinzuwirken. Diesbezüglich kann eine Unterweisung der Mitarbeiter im Zuge der Einführung von „BYOD“ hilfreich sein. Im Übrigen dient die Pflicht zur unverzüglichen Verlustanzeige auch den eigenen Interessen der Hochschule, da somit gegebenenfalls über die Fernsperrung von Nutzeraccounts ein Bekanntwerden sonstiger geheimer Daten verhindert werden kann (s. auch Punkt 12).

6. Daneben sollten klare Regelungen hinsichtlich der Nutzung des Gerätes bei privaten oder dienstlichen Reisen ins Ausland getroffen werden. Beispielsweise die Sicherheitsorgane einiger Länder (insbesondere die Finanzbehörden) sind nämlich teilweise zum Zugriff auf private Daten berechtigt.

7. Die immer populärer werdenden Cloud-Dienste stellen ebenfalls ein Risiko im Rahmen von „BYOD“ dar. Der Arbeitgeber sollte die privaten Geräte vor der Freigabe für die betriebliche Nutzung auf die dort vorhandenen Cloud-Dienste und deren Konfiguration überprüfen. In diesem Zuge ist die Unterbindung automatischer Backups von betrieblichen Daten in der Cloud empfehlenswert. In gleicher Manier sollte mit systemeigenen oder durch die Mitarbeiter eingerichteten Backups auf den privaten Geräten der Arbeitnehmer verfahren werden, da die Daten im Zuge solcher Backups (möglicherweise auf externen Speichermedien der Arbeitnehmer) gänzlich der Kontrolle des Arbeitsgebers entzogen sind. In diesem Zusammenhang können auch Wartungspflichten für die privaten Endgeräte geregelt werden, sofern dies nicht bereits an anderer Stelle geschehen ist.

8. Neben der rechtlichen Ausgestaltung muss der Arbeitgeber insbesondere auch für die entsprechende technische Umsetzung sorgen (wie etwa verschlüsselte Container oder Terminal-Lösungen). Hier sollte keine andere Behandlung als bei betrieblichen Geräten, die außerhalb des Betriebsgeländes genutzt werden, erfolgen. Der Einsatz von geeigneter Sicherheits- sowie Verschlüsselungssoftware ist unabdingbare Voraussetzung bei der Einführung von „BYOD“. Es empfiehlt sich die arbeitgeberseitige Bereitstellung von geeigneter Sicherheits- sowie Verschlüsselungssoftware für die dienstliche Nutzung der privaten Endgeräte. Auf diese Weise kann die notwendige Datensicherheit gewährleistet werden. An dieser Stelle sind allerdings die urheberrechtlichen Aspekte zu berücksichtigen, die bereits im zweiten Teil dieser Aufsatzreihe (siehe dazu: Kuta, Die rechtlichen Herausforderungen von „Bring Your Own Device“ – Lifestyle contra Sicherheit – Teil 2: Arbeitsrecht, Haftungsrecht, DFN-Infobrief Recht (06/2015)) besprochen wurden. Neben den vertraglichen Regelungen wird dazu geraten, den Arbeitnehmer auf technischer Ebene zur Trennung von privaten und dienstlichen Daten auf dem Endgerät zu verpflichten.

9. Im Rahmen der technischen Umsetzung schwirren hinsichtlich eines effektiven Mobile Device Managements (MDM) eine Vielzahl von Begriffen umher, wie etwa Verschlüsselungs- und Synchronisationssoftware, Sandboxing (=Container), Data-Loss-Prevention, Theft-Recovery, Remote-Wipe, VPN oder Remote-Desktop-Applikationen. Auf technischer Ebene kommen mit Blick auf den Datenschutz sowie die Datensicherheit diverse

Möglichkeiten in Betracht, wobei an dieser Stelle einige exemplarisch angesprochen werden. So können verschlüsselte Container eingesetzt werden (Container-Apps; dabei wird ein Datenbereich in einem Container abgekapselt, wobei es sich bei diesen separierten Daten in den meisten Fällen um die dienstlichen Daten handelt). Häufig werden in diesem Zusammenhang auch Terminalserver-Lösungen (bzw. Remotedesktopdienste = RDP-Dienste) besprochen. Andere PCs können die darauf laufenden zentralen Anwendungen als Ein-/Ausgabegeräte verwenden, wobei auf den einzelnen PCs keinerlei Dateien gespeichert werden. Das dahinterstehende Prinzip verfolgt den Zweck, dass eine Anwendung nur einmal zentral installiert wird und mehrere PCs dann über das Netz darauf zugreifen und diese Anwendung verwenden können. Insgesamt kann durch derartige technische Maßnahmen einerseits eine Kontrolle erfolgen, ohne dass private Daten des Arbeitnehmers betroffen wären. Andererseits kann illegal installierter Software der Zugriff auf das Unternehmensnetzwerk verweigert werden.

10. Eine technische Aufteilung des privaten Endgeräts in dieser Gestalt kann auch eine Lösungsmöglichkeit für weitere Elemente der IT-Struktur (Firewalls, Spam- und Virenschutz, Verschlüsselung, Serververwaltung) darstellen. Daneben erscheint die Nutzung der betrieblichen Daten auf dem privaten Gerät über einen gesicherten Fernzugriff als sehr empfehlenswert.

11. Die privaten Daten auf den Geräten der Mitarbeiter sind deren Privatsphäre zuzuordnen und daher vor dem Zugriff durch den Arbeitgeber geschützt. Nichtsdestotrotz muss der Arbeitgeber die betrieblichen Daten auf diesen privaten Geräten nutzen, bearbeiten und löschen können. Aus diesem Grund empfehlen sich entsprechende Regelungen, die ausdrücklich mit den Arbeitnehmern zu vereinbaren sind. Eine Löschung privater Daten seitens des Arbeitgebers sollte dabei nur für absolute Notfälle vorgesehen werden. Dabei spielt die Festlegung des Speicherortes für dienstliche Daten eine wichtige Rolle. Mit Blick auf die lokale Speicherung von Daten sollte ausdrücklich geklärt und festgehalten werden, ob und wie dienstliche Daten auf den privaten Geräten der Arbeitnehmer gespeichert werden dürfen. Durch eine lokale Speicherung dienstlicher Daten wird nämlich der Zugriff des Arbeitgebers auf diese Daten erheblich erschwert. Aus denselben Gründen sollten auch private und dienstliche E-Mails voneinander getrennt in separaten Ordnern oder Containern abgespeichert werden. Konkrete Handlungsanweisungen und Vereinbarungen mit den Arbeitnehmern sollten die technischen Vorkehrungen flankieren, um vor allem auch den Geheimnisschutz zu gewährleisten.

12. Ein effektives Identitätsmanagement zur Eingabekontrolle kann einen Drittzugriff wirksam beschränken. Daneben gewährleisten Synchronisations- und Backup-Tools die dauerhafte Verfügbarkeit dienstlicher Daten, wodurch insbesondere der Anlage zu § 9 S. 1 BDSG nachgekommen wird. Gleiches gilt für Verschlüsselungsmethoden sowohl alleine auf dem privaten Gerät als auch für die Kommunikation zwischen dem privaten Endgerät und der Unternehmens-IT. Die bereits angesprochenen Container-Lösungen können mit einem sog. Remote-Wipe kombiniert werden. Auf diese Weise kann der Container bei Verlust des privaten Endgeräts oder einem Missbrauchsverdacht per Fernzugriff gelöscht werden. Bei aller Euphorie für diese Funktion einer ferngesteuerten Löschung stößt sie in Technikerkreisen jedoch auf große Skepsis, da die Ausführung der Funktion nicht hinreichend sichergestellt ist oder sogar verhältnismäßig einfach verhindert werden kann.

13. Sofern der Mitarbeiter der Kontrolle durch den Arbeitgeber in Folge der aufgezeigten Maßnahmen nicht zustimmt, sollte explizit ein Widerruf zur Erlaubnis von BYOD vorbehalten werden (auf die Beendigungstatbestände wird in Teil 4 dieser Reihe genauer eingegangen).

Aufbewahrungspflichten

Durch Vereinbarungen mit dem Arbeitnehmer muss sichergestellt werden, dass den gesetzlichen Aufbewahrungs- und Archivierungspflichten nachgekommen wird. Dies gilt insbesondere für Geschäftsvorgänge, die über private Endgeräte abgewickelt werden. Einer Vermischung von privaten und geschäftlichen Daten ist schon auf der Ebene der technisch-organisatorischen Maßnahmen zu begegnen. Geschäftsrelevante Aufzeichnungen, insbesondere geschäftliche E-Mails, dürfen nicht ausschließlich im privaten Bereich des Endgerätes be- und verarbeitet werden, sodass sie am AG „vorbeilaufen". Zur Erfüllung von Aufbewahrungspflichten ist es nämlich notwendig, dass die Daten zusätzlich auch beim Arbeitgeber (beispielsweise auf dessen Servern) gespeichert werden. Es

ist gerade im Rahmen von „BYOD“ zu beachten, dass etwa die Finanzverwaltung für eine Überprüfung jederzeit unmittelbaren Zugriff auf alle privaten Geräte der Mitarbeiter erhalten muss, sofern die den Aufbewahrungspflichten unterliegenden Dokumente nur auf den privaten Endgeräten der Mitarbeiter gespeichert sind. Eine revisionssichere Archivierung beim Arbeitgeber und eine damit einhergehende regelmäßige Synchronisation der Datenbestände sind daher unumgänglich.

Geheimnisschutz und Strafrecht

Im Hinblick auf Geheimhaltungsinteressen müssen Arbeitnehmer geschult und sensibilisiert werden. Dabei können Hinweise in BYOD-Richtlinien auf die strafrechtlichen Sanktionen im Falle eines Verstoßes Lenkungswirkung haben. Mobile Device Management-Lösungen können einen Großteil der strafrechtlichen Probleme ausklammern, sodass ein Dateizugriff über diese Systeme eingerichtet werden sollte. Mitarbeitereigene Daten sollten von einem Zugriff konsequent ausgeschlossen werden. An dieser Stelle rückt auch der sog. Remote-Wipe in den Fokus, der schon im 3. Teil dieser „BYOD“-Serie beim Thema Datenschutzrecht und Datensicherheit angesprochen wurde. Durch die Initialisierung eines Remote-Wipe werden alle Daten auf dem betroffenen Gerät gelöscht und unbrauchbar gemacht. Dies kann strafrechtliche Probleme aufwerfen. Die vorherige Einwilligung des Arbeitnehmers in den Remote-Wipe stellt ein tatbestandsausschließendes Einverständnis (bei Straftatbeständen, die notwendigerweise ein Handeln gegen oder ohne den Willen des Betroffenen voraussetzen, willigt dieser dabei ein, dass schon der entsprechende Straftatbestand nicht gegeben ist) dar. Mit der Verlustanzeige an die Hochschule/die Forschungseinrichtung/das Unternehmen kann aber die Löschbewilligung gleichzeitig widerrufen werden. Die Durchführung des Remote-Wipe hätte in diesem Fall strafrechtliche Konsequenzen. Um alle Unwägbarkeiten bestmöglich abzusichern, ist eine Mobile Device Management-Lösung erforderlich, die bis ins kleinste Detail ideal auf die jeweilige Einrichtung und deren Besonderheiten abgestimmt ist. Dabei muss die selektive Löschung von Daten möglich sein. Vergegenwärtigt man sich den gesetzlichen Rahmen und hält diesen konsequent ein, gehen damit zwei Vorteile einher: Es hilft einerseits bei dem technischen Schutz vor Missbräuchen, andererseits unterstützt es die Einführung und Umsetzung von BYOD.

Steuerrecht

Es sind genaue arbeitsvertragliche Regelungen zur BYOD-Vergütung erforderlich, damit die im Zuge von BYOD möglichen steuerlichen Vorteile genutzt werden können. Gleichzeitig wird durch solche Vereinbarungen auch Klarheit zwischen den Parteien geschaffen, sodass mögliche Ungereimtheiten über eine gesonderte Vergütung für eingebrachte Geräte gar nicht erst aufkommen können.

Beendigungstatbestände

Das eingebrachte Endgerät steht im Eigentum des Arbeitnehmers. Die dort abgespeicherten Daten können zum Teil nicht eindeutig dem privaten oder dienstlichen Bereich zugeordnet werden. Scheidet ein Mitarbeiter aus der Einrichtung aus, müssen sämtliche Dienstmittel an den Arbeitgeber zurückgegeben werden. Von dieser Rückgabepflicht sind auch Daten umfasst, wobei diese in der Regel schon aufgrund der Synchronisation neben der lokalen Speicherung auf dem privaten Endgerät auch auf den Servern des Arbeitgebers liegen. Dementsprechend genügt die Löschung dieser dienstlichen Daten auf dem mitarbeitereigenen Gerät. Neben dem Ausscheiden des Mitarbeiters kann es auch vorkommen, dass Mitarbeiter den internen „BYOD“-Richtlinien nach einiger Zeit widersprechen.

Für die geschilderten Fälle sollten Beendigungstatbestände in die „BYOD“-Vereinbarung aufgenommen werden. Auf diese Weise können Unklarheiten von vornherein vermieden werden. Zu denken wäre hierbei an eine Befristungsregelung (etwa für eine Erprobungsphase), an ein Widerrufsrecht oder an ein Kündigungsrecht der „BYOD“-Erlaubnis. Insbesondere sollten dabei Regelungen zur Aushändigung der betrieblichen Daten an den Arbeitgeber nach Beendigung des Arbeitsverhältnisses getroffen werden. Aus dieser Regelung muss deutlich hervorgehen, welche Daten vom Mitarbeiter herauszugeben sind und welche Dateien sowie Dateikopien (möglicherweise auch auf externen Speichermedien) rückstandslos gelöscht werden müssen. Das Herausgaberecht ergibt sich aus § 667 Bürgerliches Gesetzbuch (BGB). Um den Löschungspflichten vorzubeugen, kann auch geregelt werden, dass dienstliche Daten nur auf dem „dienstlichen Container“ bzw. den virtuellen dienstlichen Laufwerken und nicht lokal auf dem mitarbeitereigenen Endgerät abgespeichert werden dürfen.

Anmerkung:

Einen ausführlichen Leitfaden zur Handhabung von „Bring Your Own Device“ finden Sie unter: https://www.dfn.de/fileadmin/3Beratung/Recht/handlungsempfehlungen/Bring_Your_Own_Device.pdf

„Share on Facebook“ – Lesen, teilen, haften?

Zur Frage einer möglichen Verletzung von Urheberrechten durch die Share-Funktion von Facebook

von Lennart Sydow

Nach der Abmahnung einer Fahrlehrerin wegen des Teilens eines Artikels des Online-Portals bild.de auf ihrer Facebook-Seite entwickelte sich innerhalb kürzester Zeit eine lebhafte Diskussion über eine mögliche neue Abmahnwelle. In dieser Situation werden Ausführungen, die das Landgericht Frankfurt am Main im letzten Sommer zu Urheberrechtsverletzungen auf Facebook gemacht hat (Urteil vom 17.7.2014 – 2-03 S 2/14), erneut relevant. Dabei geht es vor allem um die Frage einer möglichen Einwilligung in die Nutzung urheberrechtlich geschützter Inhalte durch das Setzen eines „Share-Buttons“ zwecks Weiterleitung an Facebook. Im Ergebnis dürfte eine Verletzung von Urheberrechten durch die bloße Nutzung dieser Funktion jedoch unwahrscheinlich sein, auch wenn noch keine ausreichende Rechtsprechung vorliegt, die hier Rechtssicherheit schafft.

I. Hintergrund

Die Vielzahl von Möglichkeiten, Inhalte über das Internet weiterzuverbreiten, scheint eine ebenso große Zahl an Haftungsrisiken mit sich zu bringen. Diesen Eindruck kann man zumindest gewinnen, wenn man den Beiträgen einiger Autoren in Print- und Onlinemedien Glauben schenkt. So wurde im März dieses Jahres mit dem Bekanntwerden einer Abmahnung einer Fahrlehrerin, die einen Artikel des Online-Portals Bild.de über die „Share-Funktion“ von Facebook geteilt hatte, auf vielen Nachrichtenseiten schon eine neue Abmahnwelle vorhergesagt. Dabei wurde schnell übersehen, dass sich kein Gericht mit dieser Frage zu befassen hatte, sondern lediglich eine Abmahnung verschickt wurde. Diese wurde dann, im aufkommenden Medienrummel teils unbemerkt, einen Tag nach ihrem Bekanntwerden in der Öffentlichkeit zurückgenommen. Während eine gewisse Vorsicht bei der Weiterleitung von Inhalten grundsätzlich angebracht ist, ist die Angst vor einer neuen Abmahnwelle bei genauerer rechtlicher Betrachtung nicht begründet. In diesem Zusammenhang wurde häufig ein Urteil des Landgerichts Frankfurt am Main angesprochen, welches angeblich die Verletzung von Urheberrechten durch Facebooks „Share-Funktion“ zum Inhalt habe. Dass dies nur schwerlich aus der Urteilsbegründung zu entnehmen ist, ergibt sich aber bei genauerem Hinsehen.

II. Rechtliche Betrachtung

Die Tatsache, dass grundsätzlich beim Umgang mit urheberrechtlich geschützten Inhalten im Internet ein gewisses Haftungsrisiko besteht, dürfte mittlerweile den meisten Nutzern bekannt sein. Solche geschützten Inhalte können im Internet vor allem Fotos, Videos, Musikdateien und Texte, aber auch sonstige Werke sein, die die erforderliche Individualität zum Ausdruck bringen. An diesen Werken hat der Urheber umfangreiche Ausschließlichkeitsrechte. Er alleine ist unter anderem zur Veröffentlichung, Vervielfältigung und öffentlichen Zugänglichmachung seines Werkes berechtigt, wenn nicht eine der gesetzlichen Schranken des Urheberrechts, wie beispielsweise das Zitatrecht, die jeweilige Nutzung erlaubt.

Ist letzteres nicht der Fall, kann der Urheber über die Verwertung seines Werkes alleine entscheiden und gegebenenfalls in die Nutzung durch einen Dritten einwilligen. Werden also urheberrechtlich geschützte Inhalte über die „Share-Funktion“ von Facebook geteilt, stellt sich zunächst die Frage, ob dies eine Handlung darstellt, welche ausschließlich dem Urheber vorbehalten ist. Nur wenn dies der Fall ist, ist weiterhin zu klären, ob es für die Nutzung eine gesetzliche Erlaubnis oder eine Einwilligung des Urhebers gibt.

III. Verfahren am Landgericht Frankfurt am Main

Vorliegend hatten die Richter über einen Fall zu entscheiden, in dem ein Redakteur Schadensersatz und Ersatz der Abmahnkosten dafür verlangte, dass ein von ihm geschriebener Artikel auf der Facebook-Seite des Beklagten verwendet wurde. Der Beklagte hatte diesen Artikel allerdings nicht lediglich über die von Facebook zur Verfügung gestellte „Share-Funktion“ geteilt, sondern den vollständigen Beitrag auf die eigene Facebook-Seite eingestellt. Das Gericht sah darin, wenig überraschend, eine Verletzung des Urheberrechts des Redakteurs. Interessant sind aber Teile der Begründung, die für dieses Ergebnis angeführt werden. Zwar wird die Frage, ob es sich bei bloßem Teilen über die „Share-Funktion“ schon um ein urheberrechtlich relevantes Verhalten handelt, nicht angesprochen, da in diesem Fall eine vollständige Übernahme des Textes vorlag. Dafür geht das Urteil aber ausführlicher auf die Frage einer möglichen Einwilligung oder Zustimmung zur Nutzung durch das Setzen des „Share-Buttons“ ein.

Der Urheber kann Dritten die Nutzung seines Werkes gestatten. Erforderlich dafür ist eine Erklärung des Urhebers, durch die er eindeutig zum Ausdruck bringt, dass einem Dritten ein bestimmtes Nutzungsrecht eingeräumt werden soll. Dies kann entweder ausdrücklich oder durch schlüssiges Verhalten erfolgen. Ob ein solcher Wille des Urhebers zum Ausdruck kommt, ist im Einzelfall und unter Berücksichtigung der gesamten Begleitumstände aus objektiver Sicht zu bestimmen. Im Verfahren vor dem LG Frankfurt am Main wollte der Beklagte eine solche Einräumung der Nutzungsrechte durch schlüssiges Verhalten dem Umstand entnehmen, dass der Urheber selbst den Online-Artikel mit dem „Share-Button“ von Facebook versehen hatte. Die entscheidende Frage, die das Gericht hier zu klären hatte, war daher, ob in diesem Verhalten des Urhebers tatsächlich eine Einwilligung zur vollständigen Übernahme des Artikels zu sehen ist. Dabei ist zunächst zu betrachten, was die „Share-Funktion“ technisch beinhaltet.

Facebook selbst beschreibt diese wie folgt: “Mit der Teilen-Schaltfläche kannst du einen Kommentar zu einem Link hinzufügen und das Publikum für den Beitrag auswählen.” Zudem ist nach den Standardeinstellungen von Facebook die Funktion so konfiguriert, dass nur die Überschrift und die Quelle eines Inhalts, sowie ein kurzer Ankündigungstext oder ein Vorschaubild übernommen wird. Nach Ansicht des Gerichts bestehe zwar für den Nutzer die Möglichkeit, einen Ankündigungstext so zu verändern, dass der vollständige Text verwendet wird. Dies sei aus objektiver Sicht nach dem Verkehrsverständnis aber nicht so zu verstehen, dass der Urheber durch Einbinden dieser Funktion eindeutig zum Ausdruck bringe, dass er die Rechte für die Nutzung des vollständigen Artikels über die Weiterleitung durch Facebooks „Share-Funktion“ hinaus einräumen wolle. Das Gericht verweist diesbezüglich auf ein Urteil des Bundesgerichtshofs vom 29. April 2010 (Az. I ZR 69/08), in dem dieser sich zur Auslegung von Erklärungen zur Einräumung von Nutzungsrechten geäußert hatte. Danach gilt gemäß dem im Urheberrecht geltenden Zweckübertragungsgrundsatz, dass die Rechte des Urhebers grundsätzlich so weit wie möglich beim Urheber verbleiben, um diesem eine angemessene Beteiligung an den Erträgen seines Werkes zu ermöglichen. Nutzungsrechte werden demnach im Zweifel nur so weit übertragen, wie dies für den Zweck der Rechteeinräumung erforderlich ist. Insofern überrascht es nicht, dass das Gericht im Falle der Nutzung der „Share-Funktion“ keine darüber hinausgehende Nutzung des vollständigen Artikels als von der Rechteeinräumung umfasst angesehen hat. Vielmehr ist folgerichtig der Umfang der Zustimmung auf die Anwendung dieser Funktion beschränkt. Dass es innerhalb dieser ein freies Textfenster für Kommentare und Anmerkungen gibt, welches die Möglichkeit eröffnet, per „copy&paste“ auch den Artikeltext einzufügen, beschreibt keine Besonderheit dieses konkreten „Share“-Verfahrens, sondern lediglich die allgemeine Möglichkeit der einfachen Vervielfältigung digitaler Texte. So kann dieser Umstand richtigerweise nicht für eine erweiterte Rechteeinräumung sprechen. Während also im vorliegenden Fall relativ unproblematisch ein eindeutiges Ergebnis erzielt werden konnte, stellt sich die Frage, inwiefern die Ausführungen allgemeine Hinweise zur rechtlichen Einordnung der „Share-Funktion“ enthalten.

IV. Fazit

Das Gericht geht in seiner Argumentation zwar nicht direkt auf den Umfang einer erteilten Einwilligung durch Einbinden der „Share-Funktion“ ein. Allerdings war dies vorliegend auch nicht erforderlich, nachdem festgestellt wurde, dass jedenfalls die Verwendung des vollständigen Artikels nicht mehr von der Einwilligung gedeckt war. Dass im vorliegenden Fall im Teilen des Inhaltes eine Urheberrechtsverletzung zu sehen ist und keine Handlung, die von der Zustimmung des Urhebers gedeckt ist, begründet das Gericht damit, dass der Beklagte von der bloßen Nutzung der „Share-Funktion“ abgewichen ist. Wenn aber mit dem Abweichen vom Funktionsumfang der „Share-Funktion“ argumentiert wird, um eine Urheberrechtsverletzung zu begründen, spricht dies dafür, dass eine Weiterleitung innerhalb dieser Funktion als zulässig erachtet wird. Eine Auslegung, in der das bewusste Einbinden dieser Funktion nicht als ausreichend für die Zulässigkeit von deren Verwendung durch die Nutzer angesehen wird, erscheint zudem schwer begründbar.

Unklar ist noch, ob darin tatsächlich eine Einräumung von Nutzungsrechten bezogen auf die Nutzung durch die „Share-Funktion“ oder lediglich ein tatsächliches Einverständnis mit der Weiterverbreitung über diese Funktion zu sehen ist. In beiden Fällen wäre dem Nutzer die Weiterverbreitung in dieser Weise erlaubt. Ginge man aber von einer Einräumung von Nutzungsrechten aus, hieße dies darüber hinaus, dass derjenige, der den „Facebook-Button“ gesetzt hat (wie zum Beispiel der Betreiber eines Online-Portals) an den Inhalten Nutzungsrechte soweit innehaben müsste, dass ihm die Weitereinräumung von Nutzungsrechten an Dritte gestattet ist. Eine solche Vereinbarung mit den jeweiligen Werkerstellern (zum Beispiel Autoren und Fotographen) ist in der Praxis bisher wohl nicht geläufig. Denkbar ist stattdessen, im Einbinden der Schaltfläche lediglich ein tatsächliches Einverständnis zu sehen. Dieses räumt dem Nutzer der die Inhalte teilt keine Nutzungsrechte ein. Das Einverständnis lässt allerdings die Rechtswidrigkeit seines Handelns entfallen.

Für die letztgenannte Einordnung spricht darüber hinaus, dass die „Share-Funktion“ vom Prinzip her dem Setzen eines Links mit einem Vorschaubild entspricht. Das Setzen eines bloßen Links ist schon kein urheberrechtlich relevantes Verhalten, wie der Bundesgerichtshof im Jahr 2003 entschieden hat (Urteil vom 17.7.2003 - I ZR 259/00, siehe dazu auch: Overbeck, „Verlinkt, verändert, verantwortlich!“, DFN-Infobrief Recht 9/2013 und Klein, „Das mach‘ ich doch mit Links!“, DFN-Infobrief Recht 7/2014). Dafür ist daher auch keine Einräumung von Nutzungsrechten erforderlich. Die Verwendung von Vorschaubildern ist zwar grundsätzlich urheberrechtlich (als Vervielfältigung oder öffentliche Zugänglichmachung) problematisch, wenn es sich dabei um geschützte Inhalte handelt. Sobald aber der Urheber durch Einbinden der „Share-Funktion“ diese Möglichkeit veranlasst, gleicht die Situation eher der der Anzeige von Vorschaubildern in Suchmaschinen, welche sogar ohne rechtsgeschäftliche Einwilligung des Urhebers zulässig ist. Im Fall der Suchmaschinen wird dies damit begründet, dass der Urheber die Möglichkeit hat, durch die Robots. txt-Datei die Auflistung der eigenen Inhalte in einer Suchmaschine zu verhindern und ansonsten davon auszugehen ist, dass zumindest ein tatsächliches Einverständnis mit der Anzeige vorliegt, welches die Rechtswidrigkeit der Nutzung ausschließt. Wenn der Urheber aber durch das Einbinden der „Share-Funktion“ selbst die Möglichkeit zur Weiterverwendung gibt, geht das noch deutlich weiter als bloße Untätigkeit. Es ist daher nicht ersichtlich, weshalb in dieser Situation anders entschieden werden sollte.

Zwar ist zu beachten, dass diesbezüglich noch keine Rechtsprechung vorliegt, welche sich genau mit der Verletzung durch die bloße Nutzung der „Share-Funktion“ auseinandersetzt. Dennoch ist es unwahrscheinlich, dass die Gerichte in diesem Verhalten eine Verletzung der Rechte des Urhebers sehen werden, wenn nicht weitere Umstände hinzutreten. Eine neuerliche Abmahnwelle, wie sie einige Autoren prophezeien, wäre unter dieser Annahme folglich nicht zu befürchten.

V. Auswirkungen für Hochschulen

Für die Hochschulpraxis ergibt sich aus diesem Urteil kein neues Haftungsrisiko, es sollten aber gewisse Gegebenheiten beachtet werden. Soweit eine „Facebook-Seite“ betrieben wird, über die nicht ausschließlich eigene Inhalte verbreitet werden, ist beim Einstellen von Inhalten anderer Autoren darauf zu achten, dass die daran bestehenden Urheberrechte nicht verletzt werden. Solange nur Inhalte verlinkt werden, besteht diese Gefahr nicht. Auch wenn Inhalte über die „Share-Funktion“ geteilt werden, ist eine Verletzung von Urheberrechten aus den genannten Gründen höchst unwahrscheinlich. Insofern sollte die Nutzung der „Share-Funktion“ weitgehend risikolos möglich sein. Werden aber Inhalte geteilt, zum

Beispiel indem eigenständig geschützte Texte oder Bilder bei Facebook eingestellt werden, obwohl der jeweilige Autor diese nicht über den „Share-Button“ selbst verfügbar gemacht hat, kann dies urheberrechtlich problematisch werden. Es sollte daher sicherheitshalber lediglich ein Link gesetzt und auf die Verwendung von Vorschaubildern und Textausschnitten verzichtet werden.

Wo „Urheber“ drauf steht, ist auch „Urheber“ drin

Über die Vermutung der Urheberschaft und den Ort des zuständigen Gerichts im Internet

von Susanne Thinius

Gleich zwei spannende Entscheidungen aus der Sparte „Urheberrecht im Internet“ wurden innerhalb der letzten Monate veröffentlicht. Zum einen die des Bundesgerichtshofes (BGH) vom 18.9.2014 (I ZR 76/13), in der es um Themen wie Urhebervermutung und Urheberrechtsverletzungen im Internet per se ging. Zum anderen die Entscheidung des Europäischen Gerichtshofes (EuGH) zur Durchsetzung urheberrechtlicher Ansprüche mit Auslandsbezug (Urteil vom 22.1.2015, C-441/13). Die Urteile erläutern recht anschaulich das Urheberrecht und seine Fallstricke im Internet. Auch für Hochschulen ein Themenbereich, der aktueller denn je ist, da Urheberrechtsverletzungen an der Tagesordnung sind.

Hintergründe des BGH-Urteils

Dem BGH-Fall liegen Teddybären-Sammlerstücke zugrunde. Der Kläger verkaufte Sammelfiguren in Form von Teddies über seine Internetseite www.ct-paradies.de und fertigte zu diesem Anlass Fotografien (Lichtbilder) an. Die Fotografien verwendete die Beklagte ohne Einverständnis des Klägers, um die Teddies auf eBay anzupreisen. Der Kläger sah darin eine Urheberrechtsverletzung und verlangte Schadensersatz und die Unterlassung ähnlicher Handlungen. Obwohl die Beklagte dem Begehren nachkam und den Verkauf über Ebay einstellte, fanden sich mit Hilfe von Suchmaschinen weiterhin streitgegenständliche Lichtbilder in Unterkategorien der Plattform Ebay. Der Kläger verlangte abermals Unterlassung und Schadensersatz. Der BGH stellte an erster Stelle fest, dass der Kläger tatsächlich Urheber der Fotografien sein kann, was im Berufungsverfahren von der Beklagten bestritten wurde. Der BGH befasste sich ausführlich mit der sogenannten Urhebervermutung, wenngleich er sie im Ergebnis ablehnte.

Urhebervermutung

Doch was verbirgt sich hinter diesem urheberrechtlichen Konstrukt der Urhebervermutung? Das Urheberrecht schützt die Belange der Urheber umfassend. Ausfluss dessen ist die Urhebervermutung aus § 10 UrhG, sie erleichtert dem Urheber den Beweis seiner Urheberschaft, insbesondere wenn seine Schöpfung lange zurück liegt und kaum mehr Zeugen oder andere Beweise für die entsprechende Urheberschaft zu finden sind. Die Vorschrift gilt nur zu Gunsten des Urhebers, nicht zu seinen Lasten. Die Vermutung erstreckt sich auf die konkrete Frage, wer die persönliche geistige Leistung erbracht hat. Die eigentliche Werkqualität im Sinne des § 2 Abs. 2 UrhG muss das Gericht gesondert feststellen. Die Urhebervermutung gilt für alle Werkformen aus dem Urheberrecht. Bei § 10 Abs. 1 UrhG handelt es sich um eine gesetzliche Urheberschaftsvermutung.

Voraussetzung ist, dass der Urheber auf einem „Vervielfältigungsstück eines bereits erschienenen Werkes in der üblichen Weise als Urheber bezeichnet ist“. Dann wird der Urheber bis zum Beweis des Gegenteils als „Urheber des Werks“ angesehen. Wie die Bezeichnung genau auszusehen hat, bleibt dem Urheber überlassen – sei es anhand eines Decknamens, Künstlernamens etc. Davon sind auch Logos, Initialen oder sonstige Zeichen umfasst. Der Urheber muss jedoch unter diesem Decknamen, dem Logo etc. bekannt sein, § 10 Abs. 1 S. 1 2. HS UrhG. Bei Angabe seines vollen Vor- und Nachnamens entfällt das Bekanntheitserfordernis. Im Streitfall muss derjenige, der die Urheberschaft bestreitet, den Gegenbeweis antreten (sog. Beweislastumkehr).

„In üblicher Weise“ bedeutet hier, dass der Urheber an üblicher Stelle und mit üblichem Inhalt bezeichnet werden muss. Die Stelle darf nicht ganz versteckt oder außergewöhnlich sein, auch der im Copyright Vermerk enthaltene Name zählt beispielsweise dazu. Das Copyright bezeichnet im Übrigen die Rechtsinhaberschaft, welche nicht gleichbedeutend mit der Urheberschaft sein muss, sondern genauso gut der Verlag oder andere Rechteverwerter von Nutzungsrechten innehaben können (also auch juristische Personen). An dieser Stelle bekannt ist das ©-Zeichen. Meistens ist jedoch neben dem Copyright-Vermerk (welcher wie gesagt die Rechtsinhaberschaft vermutet) auch eine natürliche Person namentlich angegeben. Wenn es in diesem Fall keinerlei andere Urhebervermerke gibt und sich der Copyright Vermerk an der üblichen Stelle befindet, kann die Urheberschaft dieser Person vermutet werden. Häufig werden auch Zusätze verwendet wie „von“, „bearbeitet von“, „Bild/Text/Musik von“, „Text: Name“ - diese gelten als Indiz für die Üblichkeit. § 10 Abs. 2 UrhG wiederum besagt, dass bei fehlender Urheberbezeichnung auf dem Werk der als Herausgeber auf dem Werk Bezeichnete beziehungsweise der Verleger als ermächtigt gilt, die Rechte des anonymen Urhebers im eigenen Namen geltend zu machen. Die Vorschrift dient dem persönlichkeitsrechtlichen Schutz von Urhebern anonymer Werke.

Urhebervermutung im BGH-Fall

Das Ergebnis erscheint für den juristischen Laien verwirrend: der BGH verneint zwar die Voraussetzungen der (erleichterten) Urhebervermutung nach § 10 Abs. 1 UrhG, schließt eine Urheberschaft des Klägers per se aber dennoch nicht aus, da der Kläger insbesondere durch den Besitz der Originalfotodateien mit hoher Auflösung und die Benennung seiner Frau als Zeugin Beweise für seine Urheberschaft erbracht hat. Diesbezüglich verweist der BGH die Entscheidung zurück an das Berufungsgericht, welches sich nun erneut mit der Sache zu befassen hat. Die Verneinung der Voraussetzungen einer Urhebervermutung aus § 10 Abs. 1 UrhG schließt also die Annahme einer Urheberschaft nicht aus, letztere ist auch mit anderen Mitteln beweisbar. Die Urhebervermutung stellt lediglich eine Beweiserleichterung für den Urheber dar.

Doch warum lehnte der BGH die Urhebervermutung im konkreten Fall ab? Nach dessen Ansicht sind zwar Lichtbilder im Sinne von § 72 UrhG von der Urhebervermutung erfasst. Die auf der Internetseite des Klägers eingestellten Lichtbilder stellten außerdem Vervielfältigungsstücke dar. An dieser Stelle liegt eben auch die Krux des Falles: auch wenn Werke (wie die Lichtbilder) ins Internet gestellt werden, handelt es sich trotzdem um Vervielfältigungsstücke eines Werkes (=körperliche Festlegungen), da das Einstellen ins Internet eine Übertragung des Werkes auf eine Vorrichtung zur wiederholbaren Wiedergabe von Bild- und Tonfolgen voraussetzt, also die Herstellung eines Vervielfältigungsstückes im Sinne des § 16 Abs. 2 UrhG. Der eigentliche Vervielfältigungsprozess findet etwa beim Hochladen einer elektronischen Datei auf die Festplatte eines Servers statt, um sie sodann ins Internet zu stellen, so der BGH.

Nun nimmt der BGH jedoch dem Kläger den Wind schnell wieder aus den Segeln: auf die Urhebervermutung könne sich der Kläger vorliegend nicht stützen, da er auf den Fotografien nicht in üblicher Weise als Lichtbildner und mithin Urheber bezeichnet ist. Die Bezeichnung „CT Paradies“ lasse für den Verkehr keine natürliche Person erkennen. Der BGH verlangt jedoch, dass die fragliche Bezeichnung einer natürlichen Person zuzuordnen ist und vom Verkehr auch als Hinweis auf eine natürliche Person verstanden wird, da nach dem Schöpferprinzip des § 7 UrhG lediglich eine natürliche Person Urheber sein kann. Sofern die Bezeichnung auf eine juristische Person hinweist (Firma, Unternehmen etc.), kommt für sie nur die Vermutung einer Ermächtigung durch den Urheber in Betracht. Beides ist vorliegend zu verneinen.

Weitere interessante Feststellungen des BGH

An späterer Stelle befasst sich der BGH noch mit den gängigen Auslegungsregeln, was ebenfalls besonders im Rahmen von Vertragsstrafen bei Urheberrechtsverletzungen (§ 97 UrhG) interessant sein dürfte. Insbesondere Unterlassungsverträge (beispielsweise gerichtet auf Unterlassen der Verbreitung, Vervielfältigung oder Bearbeitung von Bildern fremder Urheber ohne deren Zustimmung) sind gemäß §§ 133, 157 Bürgerliches Gesetzbuch (BGB) hinsichtlich Erklärungswortlaut, den beidseitig bekannten Umständen sowie Zweck der Vereinbarung und Interessenlage der Parteien auszulegen.

Der BGH traf ferner Feststellungen zu den Ansprüchen, die aus einer Urheberrechtsverletzung resultieren. Diese sind das (zukünftige) Unterlassen einer Handlung sowie die Beseitigung eines fortdauernden Störungszustandes. Letzter

Anspruch besteht neben dem Unterlassungsanspruch, wenn eine Verletzungshandlung (wie hier das Verbreiten der Fotografien) einen „andauernden rechtswidrigen Verletzungszustand hervorgerufen hat“. Das Einstellen der Fotografien in die Internetplattform Ebay stellt einen solchen Verletzungszustand dar. Die Beklagte muss demnach im Rahmen des ihr „Möglichen und Zumutbaren“ bei Ebay auf eine Löschung der über die Suchfunktion „erweiterte Suche/beobachtete Artikel“ unter der Rubrik beendete Aktionen“ abrufbaren Fotografien hinwirken.

Eine letzte interessante Feststellung trifft der BGH bezüglich des Verschuldens im Sinne des § 97 Abs. 2 UrhG, welches wiederum für einen Schadensersatzanspruch Voraussetzung ist. In diesem Zusammenhang war es für den BGH unerheblich, dass die Beklagte nach erfolgter Abmahnung die Angebote bei Ebay beendet und die Lichtbilder entfernt hatte - es komme allein auf das schuldhafte Verhalten der Beklagten beim Einstellen der Bilder bei Ebay an.

Europäischer Gerichtshof und Zuständigkeit bei Internet-Urheberrechtsverletzungen

Mit einer ähnlichen Thematik wie der BGH beschäftigte sich auch der EuGH Anfang des Jahres. Hierbei ging es im Wege eines Vorabentscheidungsersuchens des Staates Österreich um die Auslegung des Art. 5 Nr. 3 der Verordnung EH NR. 44/2001 des Rates vom 22.Dezember 2000 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (EuGVVO), kurz: um die internationale Zuständigkeit bei Urheberrechtsverletzungen im Internet.

Eine österreichische Architektur-Fotografin und Urheberin von Lichtbildern wandte sich gegen die ungenehmigte Nutzung ihrer Lichtbilder ohne Urheberbezeichnung auf der Webseite der beklagten deutschen „EnergieAgentur“ (Bereithalten der Fotografien zum Abruf und Download). Sie erhob Schadensersatzklage vor dem Handelsgericht Wien in Höhe von 4.050 €. Die deutsche Beklagte bestritt die Zuständigkeit des österreichischen Gerichts, da ihre Webseite nicht auf Österreich ausgerichtet sei und deren bloße Abrufbarkeit in Österreich für die Zuständigkeit nicht ausreiche. Das Gericht in Wien wollte nun vom EuGH klären lassen, ob die Gerichtszuständigkeit im Land der Niederlassung des angeblichen Urheberrechtsverletzers gegeben ist (in diesem Falle: Deutschland) sowie in dem Mitgliedstaat, auf den die Webseite inhaltlich ausgerichtet ist (hier: Deutschland) oder ob auch das österreichische Gericht selbst angerufen werden könne.

Das Gericht wies zunächst darauf hin, dass Urheberrechte gemäß der Richtlinie 2001/29 (Harmonisierungsrichtlinie für das Urheberrecht) automatisch in allen EU-Mitgliedstaaten einheitlich zu schützen sind, allerdings unterlägen sie dem Territorialitätsprinzip. Dieses besagt, dass für Werke beziehungsweise für eine durch ein Leistungsschutzrecht geschützte Leistung in jedem Staat ein räumlich begrenztes Schutzrecht nach Maßgabe des jeweiligen nationalen Urheberrechts besteht – Urheberrechte werden also nach dem jeweils anwendbaren materiellen Recht verletzt.

Der EuGH beantwortete die Frage des österreichischen Gerichts dahingehend, dass auch das nationale Gericht des Geschädigten (hier: Österreich) angerufen werden kann im Falle von Schadensersatzansprüchen aus der Verletzung von Urheberrechten und verwandten Schutzrechten. Voraussetzung sei lediglich, dass die Webseite im Mitgliedstaat des verhandelnden Gerichts zugänglich sein muss. Insofern sei also auf den Ort der Verwirklichung des Schadenserfolges und den Ort des für den Schaden ursächlichen Geschehens abzustellen, so besagt es Art. 5 Abs. 3 EuGVVO.

Der EuGH macht also mit Art. 5 Abs. 3 eine Ausnahme von Art. 2 Abs. 1 EuGVVO, der grundsätzlich die Zuständigkeit dem Gericht des Mitgliedstaates zuweist, in welchem der Beklagte seinen Wohnsitz hat. Im Ergebnis hat die Klägerin also die Wahl zwischen den beiden Gerichtsorten und wählt natürlich den, der für sie strategisch günstig gelegen ist.

Fazit und Schlussfolgerungen

Auch ins Internet gestellte Werke können körperliche Festlegungen des Werkes und somit Vervielfältigungsstücke darstellen – hier passt sich der BGH also dem technischen Fortschritt an und stärkt insoweit den Urheberschutz auch – und gerade – im Internet.
Für Nutzer fremder Werke bedeutet dies mehr Achtsamkeit bei ihrer Auswahl. Sollte sich eine Urheberbezeichnung an üblicher Stelle befinden, so ist von einer genehmigungsfreien Nutzung unbedingt abzuraten, um mögliche Schadensersatzansprüche zu vermeiden. Der Urheber beziehungsweise die

zuständigen Rechteverwerter sind in diesem Fall immer zu konsultieren, es müssen Lizenzen erworben werden.
Das Urteil bringt zugleich stärkeren Schutz beziehungsweise Beweiserleichterungen für Urheber mit sich, sofern sie hinreichend auf ihrem Werk als Urheber zu erkennen sind. Eine Ausstellung der Werke im Internet schließt die Urhebervermutung aus § 10 Abs. 1 UrhG nicht aus.

Um von der Urhebervermutung zu profitieren, müssen die Urheber spezielle Voraussetzungen erfüllen – diese erläutert der BGH in seinem Urteil ausführlich – und verneint sie vorliegend. Für potentielle Urheber liest es sich fast schon wie ein Leitfaden, insbesondere bezüglich der korrekten Urheberbezeichnung. Auch hier ist – diesmal auf Urheberseite- Achtsamkeit und Exaktheit geboten.

Insbesondere die Passagen zu gängigen Auslegungsregeln bei Unterlassungsverträgen dürften auch für Hochschulen interessant sein, da Rechtsverletzungen im Urheberrecht an der Tagesordnung sind (so die unbefugte Nutzung von Kartenausschnitten, von fremden Bildern auf Facebook-Fanpages etc.). Hier lohnt es sich allemal, einen zusätzlichen Blick ins Urteil zu werfen.

Die Passage zu Unterlassungs- und Beseitigungsansprüchen bei Urheberrechtsverletzungen ist ferner dahingehend zu verstehen, dass bei fortdauernden Verletzungszuständen der Kläger die Wahl zwischen diesen zwei Ansprüchen hat, sofern die Parteien nicht ausdrücklich zwischen Beseitigung und Unterlassung differenziert haben. Jedem potentiellen Urheber, der in seinen Rechten verletzt ist, ist zu raten, keine Unterscheidung hinsichtlich möglicher Ansprüche zu vereinbaren. Auch an dieser Stelle ist nochmals auf die Konsultierung der Rechtsabteilung bei Urheberrechtsstreitigkeiten hinzuweisen.

Das Urteil kommt ebenfalls zu dem Ergebnis, dass potentielle Urheberrechtsverletzer verpflichtet sind, aktiv auf Internetakteure wie Ebay einzuwirken, um Löschungsbegehren durchzusetzen. Andernfalls bringen sie sich in die Gefahr, Unterlassungs- und Schadensersatzansprüchen ausgesetzt zu sein. Im Zusammenhang mit dem Möglichen und Zumutbaren überlässt es der BGH leider dem Berufungsgericht zu überprüfen, inwieweit die Beklagte auf die Entfernung der Lichtbilder durch Ebay hinwirken konnte und musste. Das erneute Urteil bleibt abzuwarten.

Erfreulich ist die Drosselung der Höhe von Schadenersatzforderungen: der vom Kläger geforderten Schadensersatzsumme in Höhe von 620 € pro Fotografie erteilt der BGH eine klare Absage, stattdessen setzt er einen Richtwert von 10 € pro Bild an, für den Fall der fehlenden Urhebernennung bei Benutzung einer fremden Fotografie 20 €. Dies ist eine Entwicklung, die zum einen praxistauglich und nicht völlig realitätsfern ist und zum anderen die Interessen von Urhebern und Nutzern im Netz gleichermaßen berücksichtigt.

Auch bezüglich der Zuständigkeit der Gerichte bei Urheberrechtsverletzungen im Internet ändert sich etwas zu Gunsten der Urheber: sie können die Verletzer ihrer Urheber- und verwandten Schutzrechte in ihrem eigenen (Sitz-)Land verklagen, da dort der Schaden eingetreten ist, auch wenn der Sitz beziehungsweise die Niederlassung des Verletzers und somit auch die streitgegenständliche Webseite in einem anderen Land gelegen sind. Vom bisherigen Grundsatz der Zuständigkeit beim Beklagtenwohnsitz macht das Urteil also eine Ausnahme. Auch hier lässt sich schlussfolgern: es gibt immer Ausnahmen, von denen die Gerichte hin und wieder im Sinne der Rechtsanwender Gebrauch machen. Der Kläger als Verletzter hat demnach die Wahl zwischen zwei möglichen Gerichtsorten.

Viel ist im Fluss im Urheberrecht. Sowohl nationale wie auch europäische Gerichte sind erfreulicherweise im Internetzeitalter angekommen.

My home is my office

Landesarbeitsgericht Düsseldorf zur einseitigen Beendigung von Home-Office-Vereinbarungen

von Clara Ochsenfeld

Die flexible Arbeit von Zuhause aus ist inzwischen in vielen Unternehmen und auch in den Hochschulen zur gängigen Praxis geworden. Das Landesarbeitsgericht (LAG) Düsseldorf hat in einer kürzlich ergangenen Entscheidung vom 10. September 2014 (Az.: 12 Sa 505/14) der einseitigen Beendigung von Home-Office-Vereinbarungen (sog. alternierenden Telearbeitsvereinbarungen) durch den Arbeitgeber deutliche Grenzen gesetzt. Entscheidet sich das Unternehmen, die mit dem Mitarbeiter getroffene Vereinbarung über alternierende Telearbeit aufzuheben, sind die Interessen des Arbeitnehmers stets in die Entscheidung mit einzubeziehen.

I. Ausgangslage

Viele Unternehmen gestatten ihren Mitarbeitern, dass ein gewisser Anteil der zu erbringenden Arbeitsleistung nicht mehr ausschließlich an der Betriebsstätte des Unternehmens, sondern teilweise flexibel zuhause erbracht werden kann (sog. alternierende Telearbeit). Hierzu werden oftmals Ergänzungsvereinbarungen zum Arbeitsvertrag geschlossen. Hinsichtlich der Beendigungsklauseln in solchen Vereinbarungen hat das LAG Düsseldorf die einseitige Beendigung durch den Arbeitgeber nun insoweit eingeschränkt, als es Klauseln für unwirksam erachtet, die eine voraussetzungslose Beendigung durch den Arbeitgeber gestatten. In Beendigungsklauseln müsse demnach stets das Interesse des Arbeitnehmers Berücksichtigung finden. Die Konsequenz einer derartig unwirksamen Klausel ist, dass die Ergänzungsvereinbarung über die Telearbeit nur noch durch eine Änderungskündigung beseitigt werden kann. Die Beendigung der alternierenden Telearbeit stelle darüber hinaus eine Versetzung i.S.d. Betriebsverfassungsgesetzes (BetrVerfG) dar, weshalb der Betriebsrat im Falle der einseitigen Aufhebung der Vereinbarung zu beteiligen sei.

II. Die Entscheidung des LAG Düsseldorf

1. Sachverhalt

Der Entscheidung des LAG Düsseldorf lag der Fall eines Angestellten zugrunde, der bei einer Bank als Firmenkundenbetreuer tätig war. Im Jahr 2005 traf die Bank mit dem Mitarbeiter eine Ergänzungsvereinbarung über alternierende Telearbeit. Bei dieser handelte es sich um eine vorformulierte Vereinbarung, die die Bank in einer Vielzahl von Verträgen verwendete. Die Aufnahme der Telearbeit sollte auf dem Prinzip der beiderseitigen Freiwilligkeit beruhen und keinen Rechtsanspruch auf einen alternierenden Telearbeitsplatz begründen. Im Rahmen der Vereinbarung sollte der Angestellte mindestens 40% seiner Tätigkeit an der häuslichen Arbeitsstätte verrichten. Darüber hinaus wurde vereinbart, dass die außerbetriebliche Arbeitsstätte von beiden Parteien mit einer Ankündigungsfrist von vier Wochen aufgegeben werden könne. In diesem Falle solle die gesamte Arbeitsleistung an der Betriebsstätte der Bank erfolgen, sofern das Arbeitsverhältnis nicht insgesamt beendet werde. Nachdem die Parteien im Herbst 2013 erfolglos über die einvernehmliche Beendigung des Arbeitsverhältnisses verhandelt hatten, kündigte die Bank die Vereinbarung der Telearbeit, ohne den Betriebsrat des Unternehmens zu beteiligen. Der Angestellte klagte daraufhin gegen diese aus seiner Sicht unwirksame Beendigung der Ergänzungsvereinbarung.

2. Urteil

Das LAG Düsseldorf hielt die Beendigung der Ergänzungsvereinbarung zur alternierenden Telearbeit ebenfalls für unwirksam. Nach Auffassung des Gerichts fanden in der vereinbarten Beendigungsmöglichkeit die Interessen des Arbeitnehmers keine ausreichende Berücksichtigung. Darüber hinaus habe es an der erforderlichen Beteiligung des Betriebsrates gefehlt. Die Bank wurde verurteilt, den Mitarbeiter weiterhin zu mindestens 40% an seiner häuslichen Arbeitsstätte zu beschäftigen.

Unwirksamkeit der Klausel

Das Gericht begründete seine Entscheidung damit, dass die verwendete Klausel über den Ausschluss des Rechtsanspruchs auf Telearbeit in Verbindung mit der Klausel zur vierwöchigen Kündigungsfrist unwirksam sei, da sie einer Prüfung anhand der zivilrechtlichen Bestimmungen über allgemeine Geschäftsbedingungen (§§ 305 ff. Bürgerliches Gesetzbuch (BGB)) nicht standhalte. Die voraussetzungslose und grundlose Rückkehrmöglichkeit ohne Berücksichtigung der Interessen des Angestellten stelle einen Verstoß gegen § 307 Abs. 1 S. 1 BGB dar, da die verwendete Klausel den Arbeitnehmer entgegen Treu und Glauben benachteilige. Eine derartige unangemessene Benachteiligung liegt nach ständiger Rechtsprechung vor, wenn der Verwender von Allgemeinen Geschäftsbedingungen durch einseitige Vertragsgestaltung missbräuchlich eigene Interessen auf Kosten seines Vertragspartners durchzusetzen versucht, ohne von vornherein auch dessen Belange hinreichend zu berücksichtigen und ihm einen angemessenen Ausgleich zuzugestehen. Für die Bewertung der Wirksamkeit einer derartigen Klausel ist demnach eine Interessenabwägung vorzunehmen, in welcher im Zuge einer Gesamtbetrachtung des Vertrages das Interesse des Verwenders an der Aufrechterhaltung mit dem Interesse des Vertragspartners am Wegfall der Klausel unter Berücksichtigung der arbeitsrechtlichen Besonderheiten abzuwägen ist.

Nach § 307 Abs. 2 Nr.1 und Nr. 2 BGB ist eine unangemessene Benachteiligung im Zweifel dann anzunehmen, wenn die vertragliche Regelung von dem wesentlichen Grundgedanken der gesetzlichen Regelung abweicht oder wesentliche Rechte und Pflichten, die sich aus der Natur des Vertrages ergeben, insoweit Einschränkung finden, als die Erreichung des Vertragszweckes gefährdet ist.

Das Gericht zieht für die Anforderungen an die Ausgestaltung der Klausel das gesetzliche Leitbild des § 106 Gewerbeordnung (GewO) heran. Die Norm regelt einheitlich für alle Arbeitsverhältnisse das – auch Direktionsrecht genannte – Weisungsrecht des Arbeitgebers, durch welches er die im Arbeitsvertrag festgelegten Pflichten durch genaue Anweisungen hinsichtlich Inhalt, Arbeitszeit und -ort näher bestimmen kann. Die Heranziehung dieser Norm begründet das Gericht damit, dass mit der Vereinbarung von Telearbeit der Ort der Arbeitsleistung festgelegt wird. Deshalb müsse sich eine entsprechende Klausel, bei der es um die Bestimmung des Arbeitsortes geht, an dem Mindestmaßstab einer Direktionsrechtsklausel messen lassen. Hierfür sei zwar grundsätzlich nicht erforderlich, dass die Gründe für die Ausübung des Weisungsrechts angegeben werden, jedoch müsse die Klausel dem gesetzlichen Leitbild, welches das billige Ermessen des Arbeitgebers bei Ausübung seines Weisungsrechts erfordert, entsprechen. Das Gericht ging in seiner Entscheidung davon aus, dass die hier verwendete Klausel eine unangemessene Abweichung von dem gesetzlichen Leitbild des § 106 S.1 GewO darstelle. Zwar bestimmte die Vereinbarung lediglich, dass für die einseitige Beendigung keine Angabe von Gründen erforderlich sei. Aus der Formulierung ginge jedoch nicht hervor, dass diese Gründe grundsätzlich vorliegen müssten und das Interesse des Arbeitnehmers in die Entscheidung einfließe. Dies zeige sich bereits dadurch, dass laut Vereinbarung kein Rechtsanspruch auf einen alternierenden Televertrag bestehen sollte, was in Verbindung mit der Beendigungsklausel impliziere, dass die alternierende Telearbeit ohne jeglichen Grund und ohne Rücksicht auf die Interessen der anderen Vertragspartei beendet werden könne. Das Gericht verglich darüber hinaus die Vereinbarung mit dem regulären Arbeitsvertrag des Arbeitnehmers, welcher für Um- und Versetzungen gerade eine Vereinbarung enthält, die an die Kenntnisse und Fähigkeiten des Arbeitnehmers anknüpft.

In seiner Entscheidung berücksichtigt das Gericht zwar auch, dass Freiwilligkeitsvorbehalte für zusätzliche Leistungen von der Rechtsprechung grundsätzlich anerkannt sind. Mit solchen Vorbehalten kann der Arbeitgeber bestimmte Leistungen versehen, um das Entstehen einer betrieblichen Übung und damit eines Anspruches des Arbeitnehmers auf diese Leistung von Anfang an zu unterbinden. Im vorliegenden Fall sei laut der getroffenen Ergänzungsvereinbarung jedoch höchstens die Aufnahme der Telearbeit unter einen solchen Freiwilligkeitsvorbehalt gestellt worden, nicht jedoch deren Beendigung.

Nur über diese würden die Parteien jedoch streiten. Zudem widerspreche ein völlig voraussetzungsloser Freiwilligkeitsvorbehalt für die Beendigung der alternierenden Telearbeit in Formularverträgen ebenfalls dem Leitbild des § 106 S. 1 GewO, da die Vorschrift, obwohl im Rahmen des Direktionsrechts kein Anspruch auf einen bestimmten Arbeitsplatz bestehe, dennoch die Ausübung eines billigen Ermessens fordere. So lautet der Gesetzestext: „Der Arbeitgeber kann Inhalt, Ort und Zeit der Arbeitsleistung nach billigem Ermessen näher bestimmen, […]". Dieses Ermessen werde nach Ansicht des Gerichts im Falle eines vollkommen vorbehaltslosen Freiwilligkeitsvorbehalts jedoch nicht ausgeübt, weswegen eine solche Klausel nicht zulässig sei. Zudem sei kein Interesse ersichtlich, weshalb der Arbeitgeber ohne jegliche Berücksichtigung der Interessen des Arbeitnehmers die alternierende Telearbeit einseitig und anlasslos beenden können sollte. Zwar sei es richtig, dass sich Umstände verändern und der Arbeitgeber hierauf reagieren können muss, was § 106 GewO auch vorsieht. Jedoch ginge dies gerade nicht einseitig und unter Außerachtlassung des Interesses des Arbeitnehmers, da die Vorschrift gerade die Ausübung eines billigen Ermessens verlange. Hierdurch würden auch keine unüberwindbaren Hürden zur Beendigung von Telearbeit aufgestellt.

Notwendige Beteiligung des Betriebsrats

Das LAG Düsseldorf sah die Beendigung der alternierenden Telearbeit seitens des Arbeitgebers darüber hinaus deshalb als rechtsunwirksam an, weil es sich hierbei um die personellen Einzelmaßnahme der Versetzung i.S.d. Betriebsverfassungsgesetzes handele und eine hierfür gem. § 99 Abs. 1 S. 1 BetrVG erforderliche Beteiligung des Betriebsrates nicht stattgefunden hatte. Die Vorschrift verlangt, dass u.a. im Falle der Versetzung eines Arbeitnehmers die Zustimmung des Betriebsrates eingeholt werden muss, sofern ein Betriebsrat besteht und das Unternehmen mehr als zwanzig wahlberechtigte Arbeitnehmer beschäftigt.

Das Gericht geht davon aus, dass nicht nur aufgrund der Veränderung des Arbeitsortes, sondern auch aufgrund der Veränderung der Arbeitsumstände in der Zuweisung von Telearbeit eine Versetzung zu sehen sei, sodass für deren Beendigung nichts anderes gelten könne. Das Bundesarbeitsgericht (BAG) hat in früheren Entscheidungen die Versetzung i.S.d. Betriebsverfassungsgesetzes als die Zuweisung eines anderen Arbeitsbereiches, die die Dauer von einem Monat überschreitet oder die mit erheblichen Änderungen der Umstände verbunden ist, unter denen die Arbeit zu leisten ist, definiert. Unter die Begrifflichkeit des Wortes „Arbeitsbereich" – der sowohl räumlich als auch funktional zu verstehen ist – fallen sowohl die Aufgabe und Verantwortung des Arbeitnehmers als auch die Art seiner Tätigkeit und ihre Einordnung in den Arbeitsablauf des Betriebes. Um die Zuweisung eines anderen Arbeitsbereiches handelt es sich dann, wenn das Gesamtbild der Tätigkeit des Arbeitnehmers durch die Beendigung so verändert wird, dass die Tätigkeit aus der Sicht eines betrieblichen Betrachters als eine „andere" zu sehen ist. Das Gericht ging in dem zugrunde liegenden Fall davon aus, dass die Beendigung der Telearbeit für den Arbeitnehmer dazu führe, dass der Arbeitnehmer völlig anders in den betrieblichen Ablauf eingebunden werde. Zwar handele es sich um alternierende Telearbeit, so dass der Arbeitnehmer nicht ausschließlich zuhause arbeite, jedoch hätte die Beendigung der Vereinbarung zur Folge, dass sich der Dienstort für einen erheblicher Teil der Arbeitszeit (nämlich 40%) ändern würde, sodass die funktionale Erbringung der Arbeitsleistung ohne außerbetriebliche Arbeitsstätte eine völlig andere sei. Das Gericht hat in seiner Entscheidung jedoch darüber hinaus angedeutet, dass auch im Falle eines geringeren Anteils an häuslicher Telearbeit nichts anderes gelten könnte.

III. Fazit und Bedeutung der Entscheidung für die Hochschulen

Aus der Entscheidung des LAG Düsseldorf lassen sich grundlegende Rückschlüsse hinsichtlich der Ausgestaltung von Vereinbarungen zur alternierenden Telearbeit für die Hochschulen ziehen. Zwar erheben sich bereits kritische Stimmen, die berechtigterweise der Ansicht sind, das LAG Düsseldorf habe das Home-Office als Arbeitsort nicht richtig definiert. Es sei nicht ausreichend berücksichtigt worden, dass es gerade keinen gewöhnlichen Arbeitsort darstelle, da dem Arbeitnehmer mit der Aufnahme von Teleheimarbeit zusätzliche Pflichten auferlegt werden und die Vereinbarung seiner ausdrücklichen Zustimmung bedarf. Konsequenz ist in diesem Falle, dass nach dieser Ansicht die Beendigungsmöglichkeit der Vereinbarung durch eine Teilkündigung besteht. Da eine Teilkündigung nicht das gesamte Vertragsverhältnis beendet, wären die arbeitsrechtlichen Anforderungen daran geringer als an eine Änderungskündigung, zumal die Rechtsprechung Teilkündigungsklauseln regelmäßig in Widerrufsvorbehalte umdeutet.

Dennoch ist den Hochschulen bis auf weiteres dringend zu empfehlen, sich bei der Vertragsgestaltung an die vorgegebenen Grenzen des LAG Düsseldorf zu halten. Das gesetzliche Leitbild des § 106 GewO gilt grundsätzlich für alle Arbeitnehmer und kommt demnach auch im Angestelltenverhältnis zwischen Hochschulen und ihren Mitarbeitern zur Anwendung. Auch wenn man die Regelung des § 4 des Tarifvertrags für den öffentlichen Dienst (TVöD), die als Konkretisierung des Direktionsrechts für Angestellte im Öffentlichen Dienst dient, darüber hinaus als Leitbild heranzieht, kann sich hinsichtlich der durch das LAG Düsseldorf gesetzten Grenzen der Klauselgestaltung nichts anderes ergeben. Grundsätzlich ist bei der Verwendung formularmäßiger Klauseln – also solcher, die für eine Vielzahl von Verträgen verwendet werden – stets gesonderte Vorsicht geboten. Dies gilt unabhängig davon, ob sie als Ergänzungsvereinbarung zum Arbeitsvertrag oder unmittelbar in diesen einbezogen werden. Arbeitsrechtliche Besonderheiten sollten generell immer gesondert geprüft und sorgfältig abgewogen werden. Die Wahrung billigen Ermessens kann nach der Rechtsprechung des BAG darin zum Ausdruck kommen, dass ausweislich der Klausel das Direktionsrecht unter dem Vorbehalt der Interessen des Arbeitnehmers steht. Im Falle der Vereinbarung über alternierende Telearbeit sollten die Hochschulen demnach explizit darauf achten, dass in den zwischen ihnen und ihren Angestellten geschlossenen Vereinbarungen lediglich Klauseln verwendet werden, die hinsichtlich der einseitigen Beendigung alternierender Telearbeit deutlich zum Ausdruck bringen, dass stets das Interesse des Arbeitnehmers am Fortbestand der Telearbeit umfassende Berücksichtigung findet und gegen das Interesse der Hochschulen an der Beendigung der Telearbeitsvereinbarung umfassend abgewogen wird. Soweit bereits bestehende Vereinbarungen, die nicht den genannten Grundsätzen entsprechen, seitens der Hochschulen einseitig beendet werden sollen, kommt nur noch die Möglichkeit einer Änderungskündigung gem. § 2 Kündigungsschutzgesetz (KSchG) in Betracht.

Darüber hinaus könnten sich auch aus der vom LAG Düsseldorf vorgegebenen Linie, dass die Beendigung von Telearbeit eine Versetzung i.S.d. BetrVG darstellt, für die Personalpraxis der Hochschulen zu beachtende Verfahrensregeln ergeben. Dies könnte daraus folgen, dass auch die dem Betriebsverfassungsgesetz vergleichbaren Vorschriften der Personalvertretungsgesetze der Länder im Falle der Umsetzung eines Mitarbeiters ein Mitbestimmungsrecht des Personalrates vorsehen (so z. B. § 72 Abs. 1 Nr. 5 Landespersonalvertretungsgesetz NRW (LPVG NRW)). Daher könnten bei der Beendigung von Telearbeit für die Beteiligung des Personalrats die gleichen Anforderungen gelten wie im Falle eines privatrechtlich organisierten Betriebes. Allerdings ist der betriebsverfassungsrechtliche Begriff der Versetzung weiter gefasst als der personalvertretungsrechtliche Begriff der Umsetzung. Das LAG Düsseldorf stellte hinsichtlich der Versetzung auf die erhebliche Änderung der Umstände (i.S.d. § 95 Abs. 3 S. 1 BetrVG), unter denen die Arbeit zu leisten ist, ab. An dieser Stelle lässt sich nicht vorhersehen, wie sich die Gerichte im Hinblick auf eine Umsetzung im personalvertretungsrechtlichen Sinne in Zukunft positionieren werden, da die Personalvertretungsgesetze ein Abstellen auf die erheblichen Änderungen von Umständen dem Gesetzeswortlaut nach nicht explizit vorsehen. Grundsätzlich sind dennoch Einzelfälle denkbar, in denen die Beendigung von Telearbeit durchaus als Umsetzung i.S.d. Landespersonalvertretungsgesetze einzuordnen wäre. Um daher in allen möglichen Fällen rechtlich auf der sicheren Seite zu stehen, sollte demnach der Personalrat bei der einseitigen Beendigung alternierender Telearbeit zu Lasten des Angestellten bei öffentlichen Hochschulen beteiligt und dessen Zustimmung eingeholt werden. Für den Betriebsrat bei privaten Hochschulen, sofern ein solcher besteht, gilt das Mitwirkungserfordernis nach dieser Entscheidung ohnehin.

Anmerkung:

In einer früheren Version dieses Artikels wurde nicht näher auf die Unterschiede des Betriebsverfassungsgesetzes und der Personalvertretungsgesetze eingegangen. Dies wurde nachträglich zur Verdeutlichung geändert.

Doppelt hält besser

Oberverwaltungsgericht NRW bestätigt „Doppeltür-Modell“ bei der Bestandsdatenauskunft

von Florian Klein

Im Rahmen der Strafverfolgung oder Gefahrenabwehr sind staatliche Stellen häufig auf die Mithilfe von Internetprovidern angewiesen, denn diese haben die technischen Möglichkeiten, Internetnutzer anhand ihrer IP-Adresse zu identifizieren. Ein gängiges Ermittlungsinstrument ist dabei die sogenannte Bestandsdatenauskunft, die unter anderem in § 113 Telekommunikationsgesetz (TKG) geregelt ist. Welche Reichweite dieser Vorschrift dabei zukommt und inwiefern die Bundesnetzagentur befugt ist, gegenüber Telekommunikationsdiensteanbietern Anordnungen zu erlassen, um die Erfüllung von Auskunftsansprüchen zu sichern, war jüngst Gegenstand eines Urteils des Oberverwaltungsgerichts für das Land Nordrhein-Westfalen (OVG NRW, Urt. v. 10.11.2014 – 13 A 1973/13).

I. Hintergrund

Das Internet ist aufgrund seiner nahezu unbeschränkten Kommunikations- und Informationsmöglichkeiten häufig Schauplatz von Straftaten. So lassen sich beispielsweise auf einfachste Art und Weise urheberrechtlich geschützte Werke einer breiten Öffentlichkeit zugänglich machen. Doch selbst wenn eine Straftat nicht unmittelbar im Internet verübt wird, kann es eine besondere Funktion bei der Vorbereitung von Straftaten oder bei der Kommunikation zwischen Tätern wahrnehmen. Nicht zuletzt kann es bei der Vernetzung krimineller oder terroristischer Vereinigungen hilfreich sein. Ein großer Vorteil für Straftäter besteht dabei darin, dass man meist nicht mit seinem Namen, sondern nur mit einer IP-Adresse im „Netz“ unterwegs ist. Insofern versteht es sich von selbst, dass die Sicherheitsbehörden in diesem Bereich nicht untätig bleiben dürfen. Für ihre Ermittlungen ist es von großer Bedeutung, bestimmte Internetnutzer identifizieren zu können. Dies hat auch der Gesetzgeber gesehen und Rechtsgrundlagen geschaffen, die den Sicherheitsbehörden einige Ermittlungsinstrumente und -befugnisse an die Hand geben. Da die Identifizierung einer Person im Internet in der Regel voraussetzt, dass man den Nutzer einer bestimmten IP-Adresse kennt, gibt es Auskunftsansprüche gegen Anbieter, die ihren Nutzern Zugang zum Internet vermitteln. Denn nur diese verfügen über die nötigen Anmeldedaten der Nutzer, um zuverlässig sagen zu können, wer eine dynamische IP-Adresse zu welchem Zeitpunkt genutzt hat. Dies ist also auch für Hochschulen relevant, die ihren Studierenden und Mitarbeitern den Zugang zum Internet über das Hochschulnetz ermöglichen. Geht es um die Auskunft über Daten aus dem Vertragsverhältnis zwischen Nutzer und Telekommunikationsdiensteanbieter, ist die sogenannte Bestandsdatenauskunft einschlägig.

Für diese gelten seit dem 1.7.2013 aufgrund des Gesetzes „zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft“ neue Regelungen. Bestandsdaten sind diejenigen Daten des Nutzers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden. Dies sind insbesondere Name, Anschrift, sonstige Kontaktdaten, Geburtsdatum, Anschlusskennung und (im Falle eines entgeltlichen Vertrages) Zahlungsdaten des Nutzers, durch welche er dem Telekommunikationsdiens-teanbieter gegenüber individualisiert wird.

Die Neuregelung der Bestandsdatenauskunft zeichnet sich durch eine Art Doppeltür-Modell aus. Dies bedeutet, dass zwei

Dinge zusammen kommen müssen, damit eine Bestandsdatenauskunft rechtmäßig ist: Einerseits muss es auf Seiten der Diensteanbieter eine Rechtsgrundlage geben, die es ihnen erlaubt, die Daten an die Behörden zu übermitteln, und andererseits muss es für die Behörden eine andere Rechtsgrundlage geben, die sie dazu ermächtigt, die Daten vom Diensteanbieter abzufragen, und die diesen zur Mitwirkung verpflichtet.

Die „erste Tür", also die Rechtsgrundlage für die Übermittlung der Daten durch die Diensteanbieter, findet sich nun zentral in § 113 TKG. Die jeweilige Ermächtigung zur Abfrage durch die Behörden ist dagegen in den jeweiligen Fachgesetzen geregelt. So findet sich beispielsweise für den Bereich der Strafverfolgung durch Staatsanwaltschaft und Polizei eine Regelung in § 100j der Strafprozessordnung (StPO) (s. zu den Voraussetzungen dieses Anspruchs im Detail: Klein, „Sag mir alles, was du weißt!" in: DFN-Infobrief Recht 11/2013).

II. Die Entscheidung des Gerichts

Mit der Norm des § 113 TKG hatte sich kürzlich nun das OVG NRW zu beschäftigen, nachdem sich ein Telekommunikationsdiensteanbieter geweigert hatte, einem bestimmten Auskunftsersuchen Folge zu leisten. Daraufhin hatte sich die Bundesnetzagentur eingeschaltet und diesem gegenüber eine Anordnung erlassen, die ihn verpflichten sollte, bestimmte Auskunftsansprüche zukünftig zu erfüllen. Diese Anordnung wurde von den Richtern jedoch aufgehoben, welche zugleich eindeutig feststellten, dass § 113 TKG keine Auskunftspflicht der TK-Diensteanbieter begründet.

1. Sachverhalt

Kläger war ein Internetzugangsanbieter. An diesen war das Landeskriminalamt (LKA) NRW mit einem Auskunftsersuchen herangetreten, weil es Nutzerbestandsdaten in einem Ermittlungsverfahren wegen der Verbreitung kinderpornographischer Inhalte benötigte. Konkret verlangte das LKA NRW von dem Kläger, dass er prüfen solle, ob die Nutzerbestandsdaten während der laufenden Nutzung einer dynamischen IP-Adresse – „on the fly" – an die Ermittler übermittelt werden könnten. Eine solche Datenübermittlung lehnte der Internetzugangsanbieter jedoch aus rechtlichen, technischen und organisatorischen Gründen ab. Hierfür sei es nämlich erforderlich, in den durch das Fernmeldegeheimnis geschützten Verkehrsdaten zu recherchieren. Verkehrsdaten sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden, d. h. alle Daten, welche bei einer Inanspruchnahme des Telekommunikationsdienstes entstehen (z. B. Beginn, Dauer und Ende einer Verbindung, beteiligte Nummern, etc.).

Der technische Hintergrund sah dabei wie folgt aus: Der Kläger vergab vollautomatisch dynamische IP-Adressen an seine Internetnutzer. Hierzu wurde ein Breitband-Zugangsserver (Broadband Remote Access Server = BRAS) genutzt, welcher die verfügbaren IP-Adressen aus dem von ihm verwalteten Pool dem Netzwerkanschluss zuordnete, über welchen der Internetzugang erfolgen sollte. Eine Speicherung der jeweils genutzten IP-Adresse erfolgte dabei nicht, sodass sie nach Ende der jeweiligen Verbindung nicht mehr im System des Klägers vorhanden war.

Nachdem der Kläger die Auskunft verweigert hatte, wurde die Bundesnetzagentur tätig, welche im Hinblick auf die Einhaltung der Vorschriften des TKG durch die TK-Diensteanbieter eine Kontrollfunktion innehat. Sie verpflichtete ihn, entsprechende Auskunftsersuchen im Hinblick auf die Bestandsdaten von Nutzern dynamischer IP-Adressen zukünftig auch dann unverzüglich zu erfüllen, wenn zur Feststellung der Bestandsdaten eine Auswertung von Verkehrsdaten erforderlich ist und auf diese im konkreten Fall tatsächlich zugegriffen werden kann. Gegen diese Anordnung der Bundesnetzagentur erhob der betroffene Provider schließlich Klage, über welche die Richter des OVG NRW in zweiter Instanz zu entscheiden hatten.

2. Urteil

Das OVG NRW gab der Klage des Internetzugangsanbieters statt und hob den Bescheid der Bundesnetzagentur auf, weil er rechtswidrig sei. Zur Begründung führten die Richter an, dass die Bundesnetzagentur nicht generell zur Überwachung der Tätigkeiten von Telekommunikationsunternehmen befugt sei. Vielmehr gewähre § 115 TKG ihr nur das Recht, Anordnungen gegen TK-Diensteanbieter zu erlassen, wenn diese Verpflichtungen, die sich aus bestimmten Vorschriften des Telekommunikationsgesetzes (§§ 88-115 TKG) ergeben, nicht erfüllt hätten. Bei Verstößen gegen andere Gesetze bestehe dagegen keine Eingriffsmöglichkeit.

An einer entsprechenden Nichterfüllung von telekommunikationsrechtlichen Verpflichtungen fehlte es im vorliegenden

Fall jedoch, da § 113 TKG, auf den sich die Bundesnetzagentur bei ihrer Anordnung gestützt hatte, keine Verpflichtung zur Auskunftserteilung vorsieht. Hierbei war unter anderem entscheidend, dass die Bundesnetzagentur den Kläger verpflichten wollte, bestimmte Auskunftsersuchen zukünftig unverzüglich zu erfüllen, und sie sich somit anmaßte, über das „Ob" der Auskunftserteilung zu entscheiden anstatt nur über die Art und Weise (das „Wie") der Bereitstellung der geforderten Auskünfte. Eine derartige Anordnung wäre nur möglich, wenn sich die Pflicht zur Auskunftserteilung unmittelbar aus den Vorschriften des TKG ergäbe. Eine solche Interpretation von § 113 TKG in seiner seit dem 1.7.2013 geltenden Fassung hält das Gericht allerdings nicht für möglich. § 113 TKG regelt nur die Frage, unter welchen Voraussetzungen TK-Diensteanbieter befugt sind, Auskünfte über Bestandsdaten zu erteilen. Er stellt also lediglich eine datenschutzrechtliche Erlaubnis dar, durch welche die Übermittlung der Daten an die Behörden als datenschutzrechtlich relevanter Vorgang gerechtfertigt wird. Die Verpflichtung zur Erteilung der Auskunft ergibt sich indes erst aus den jeweiligen Fachgesetzen für die Sicherheits- und Strafverfolgungsbehörden, die darin zugleich ermächtigt werden, die entsprechenden Daten abzufragen. Zu diesem Ergebnis kommen die Richter unter Heranziehung der üblichen juristischen Auslegungsmethoden: Wortlaut, Systematik und Entstehungsgeschichte des Gesetzes.

§ 113 Abs. 1 TKG öffne also die bei den privaten TK-Diensteanbietern vorhandenen Datenbestände unter datenschutzrechtlichen Gesichtspunkten für die staatliche Aufgabenwahrnehmung. Nur dieses Verständnis könne dem verfassungsrechtlich gebotenen „Doppeltür-Modell" gerecht werden, bei dem eine Tür die Befugnis zur Übermittlung der Daten symbolisiert, während die zweite Tür für die Befugnis zur Abfrage dieser Daten durch die staatlichen Stellen steht.

Da also kein Verstoß gegen § 113 TKG festgestellt werden konnte, lagen die Voraussetzungen für ein Tätigwerden der Bundesnetzagentur nicht vor. Eine darüber hinausgehende „Dachkompetenz" der Bundesnetzagentur für alle Fragen im Zusammenhang mit der Beantwortung von Auskunftsersuchen der Fachbehörden bestehe indes nicht. Im vorliegenden Fall richtete sich die Auskunftsverpflichtung des TK-Diensteanbieters nicht nach dem TKG, sondern nach den Vorschriften des nordrhein-westfälischen Polizeigesetzes, welches bestimmt, unter welchen Voraussetzungen das LKA NRW Bestandsdaten abfragen darf. Mangels einschlägiger Rechtsgrundlage war die Anordnung der Bundesnetzagentur daher rechtswidrig und von den Richtern aufzuheben.

III. Fazit und Konsequenzen für die Hochschulpraxis

Das Urteil des OVG NRW führt klar vor Augen, dass sich das vom Bundesverfassungsgericht geforderte Doppeltür-Modell bei der Bestandsdatenauskunft seit mittlerweile fast zwei Jahren im geltenden Recht wiederfindet. § 113 TKG ermächtigt staatliche Stellen nicht mehr dazu, Bestandsdaten von TK-Diensteanbietern abzufragen, sondern sichert letztere nur datenschutzrechtlich ab, wenn diese auf ein anderweitig begründetes Auskunftsverlangen hin Daten ihrer Nutzer an staatliche Stellen übermitteln. Eine alleinige Berufung auf § 113 TKG kann ein staatliches Auskunftsersuchen deshalb nicht mehr rechtfertigen. Unentbehrlich bleibt insofern eine spezialgesetzliche Regelung, die den Sicherheits- und Strafverfolgungsbehörden eine entsprechende Abfrage erlaubt.

Darüber hinaus zeigt das OVG NRW mit diesem Urteil aber auch klar die Grenzen der Handlungsbefugnisse der Bundesnetzagentur auf: Eine „Dachkompetenz" für alle Tätigkeiten der TK-Diensteanbieter besitzt sie gerade nicht. Stattdessen ist sie darauf beschränkt, die Einhaltung bestimmter telekommunikationsrechtlicher Vorschriften durchzusetzen. Insoweit Hochschulen ihren Studierenden und Mitarbeitern einen Internetzugang zur Verfügung stellen, werden sie damit ebenfalls zum Telekommunikationsdiensteanbieter, der von den zuständigen staatlichen Stellen potentiell zur Auskunftserteilung aufgefordert werden kann. Eine entsprechende Verpflichtung zur Erfüllung dieser Ersuchen darf die Bundesnetzagentur einer Hochschule dagegen nicht auferlegen, wie sich aus dem vorliegenden Urteil ergibt. Erlässt sie dennoch eine entsprechende an die Hochschule gerichtete Anordnung, sollte diese jedoch keinesfalls schlicht ignoriert werden, da dies wohl meist in Form eines Verwaltungsakts geschehen wird, der auch trotz Rechtswidrigkeit grundsätzlich wirksam ist. Um zu verhindern, dass die Anordnung als Verwaltungsakt Bestandskraft erlangt, muss dagegen deshalb mit einem Widerspruch bzw. einer Anfechtungsklage vorgegangen werden, sodass spätestens dann die Einschaltung des Hochschuljustiziariats angezeigt ist.

Im Hinblick auf die Art und Weise der Auskunftserteilung darf die Bundesnetzagentur jedoch aufgrund von § 115 Abs. 1 TKG

Einfluss nehmen, sofern diese Modalitäten in § 113 TKG geregelt sind. Davon erfasst ist beispielsweise die Verpflichtung, bei einer Bestandsdatenauskunft die Daten unverzüglich und vollständig zu übermitteln und sowohl über das Auskunftsersuchen als auch die Auskunftserteilung Stillschweigen gegenüber dem Betroffenen und Dritten zu wahren. Ebenso gilt dies für die Pflicht, sämtliche unternehmensinternen – im Fall der Hochschulen hochschulinternen – Datenquellen zu berücksichtigen. Diese Regelungen zum „Wie" der Auskunftserteilung ergeben sich unmittelbar aus § 113 TKG und fallen daher in den Normbereich, dessen Einhaltung die Bundesnetzagentur kontrollieren kann. Nur die Frage, ob überhaupt eine Auskunftspflicht besteht, kann nicht anhand des TKG beantwortet werden, weshalb die Bundesnetzagentur insoweit nicht anordnungsbefugt ist.

Insgesamt sollten Hochschulen umsichtig mit staatlichen Auskunftsersuchen umgehen, da nach den Fachgesetzen meist tatsächlich eine Auskunftspflicht bestehen wird, wenn Sicherheits- und Strafverfolgungsbehörden bestimmte Daten anfragen. Eine Verweigerung der Mitwirkung kann dann ggf. durch den Einsatz von Zwangs- oder Ordnungsmitteln geahndet werden. Interventionen durch die Bundesnetzagentur sind dagegen nur in eng begrenztem Rahmen zulässig, sodass hier stets geprüft werden sollte, ob Gegenstand einer etwaigen Anordnung Verpflichtungen sind, die sich unmittelbar aus dem TKG ergeben.

Die Welt ist nicht genug...!

OLG Celle urteilt zur Reichweite von Unterlassungserklärungen im Internet

von Marten Hinrichsen

Urheberrechtsverletzungen stehen im Internet an der Tagesordnung. Um sich gegen die unerlaubte Verwendung von geschützten Werken dauerhaft abzusichern, drängen die Rechteinhaber im Rahmen des außergerichtlichen Abmahnungsverfahrens zusätzlich auf die Abgabe einer strafbewehrten Unterlassungserklärung. In diesem Zusammenhang ergeben sich jedoch immer wieder rechtliche Probleme hinsichtlich der Reichweite solcher Erklärungen. Im Kern dreht sich die rechtliche Auseinandersetzung um die Frage, welche Pflichten zur Unterlassung und Beseitigung einer Rechtsverletzung im Internet noch als zumutbar angesehen werden können. In einem aktuellen Urteil hat sich jetzt auch das Oberlandesgericht (OLG) Celle zu der Reichweite dieser Unterlassungserklärungen geäußert und den Rahmen des Zumutbaren dabei sehr weit abgesteckt.

Hintergrund

Urheberrecht und Internet erscheinen auf den ersten Blick als zwei Dinge, die nur schwer miteinander in Einklang zu bringen sind. Tagtäglich kommt es im Internet zu einer Vielzahl von Urheberrechtsverletzungen. Die technischen Möglichkeiten gestatten es, schnell und ohne viel Aufwand Bilder und andere Inhalte zu kopieren und für andere Zwecke zu nutzen. Dass diese Inhalte häufig durch das Urheberrecht geschützt werden, wird dabei teils bewusst, teils unbewusst übersehen. Um sich gegen diese massenhaften Urheberrechtsverletzungen zur Wehr zu setzen, hat sich seitens der Rechteinhaber eine außergerichtliche Abmahnpraxis etabliert. Hierbei werden dem Schädiger, sofern dieser feststellbar ist, in erster Linie der entstandene Schaden und die für die Rechtsverfolgung notwendigen (Anwalts-) Kosten auferlegt.

Als weitere Absicherungsmittel werden zudem Beseitigungs- und Unterlassungsansprüche geltend gemacht. Zu diesem Zweck wird oftmals die Abgabe einer sogenannten strafbewehrten Unterlassungserklärung gefordert. Hierbei verpflichtet sich die betreffende Person zukünftige Rechtsverletzungen zu unterlassen und bei einer Zuwiderhandlung eine hohe Vertragsstrafe zu zahlen. Eine solche Erklärung birgt sowohl hinsichtlich ihrer Formulierung, aber auch im Hinblick auf ihre Reichweite erhebliche Haftungspotentiale. Zugleich besteht in diesem Bereich eine erhebliche Rechtsunsicherheit, da die damit einhergehenden rechtlichen Fragen nicht alle hinreichend geklärt sind.

Rechtsverletzungen im Internet und die Reichweite der Unterlassungserklärung

Neben der Formulierung solcher Erklärungen (vgl. dazu zuletzt bspw. Landgericht Hamburg, B. v. 11.1.2013, 308 O 442/12 in: Klein, Die strafbewehrte Unterlassungserklärung – schmaler Grat in rechtlichem Minenfeld, DFN-Infobrief Recht 7/2013) erweisen sich oftmals die technischen Möglichkeiten des Internets als problematisch. Entgegen dem laienhaften Verständnis reicht es beispielsweise bei der urheberrechtswidrigen Verwendung eines Bildes nicht aus, lediglich die betroffene Webseite zu löschen.

Je nach Webdesign sind die Inhalte oft isoliert über eine gesonderte URL abrufbar oder auf mehreren Servern hinterlegt. (U. v. 12.9.2012 – 6 U 58/11), dass allein die technische Möglichkeit der Erreichbarkeit ausreiche, um einen Verstoß gegen die Unterlas-

sungserklärung im konkreten Fall zu begründen. (vgl. dazu ausführlich: Klein, Die strafbewehrte Unterlassungserklärung – schmaler Grat in rechtlichem Minenfeld, DFN-Infobrief Recht 7/2013.) Die Reichweite von Unterlassungserklärungen wird somit gerade im Internet drastisch erhöht, da hier die technische Erreichbarkeit bereits eine Zugänglichmachung im Sinne von § 19a Urheberrechtsgesetz (UrhG) darstellt und eine Verletzung der Unterlassungserklärung bedeuten kann.

Urteil des OLG Celle

In einem kürzlich ergangenen Urteil hat sich auch das OLG Celle zu der Reichweite von Unterlassungserklärungen bei Urheberrechtsverletzungen im Internet geäußert (OLG Celle, Urt. v. 29.1.2015 – 13 U 58/14). Wie im Urteil des OLG Karlsruhe stand dabei die weiter bestehende Erreichbarkeit und somit die fortdauernde Rechtsverletzung im Blickpunkt. In dem Verfahren hatte sich der Beklagte im Wege einer Unterlassungserklärung dazu verpflichtet, es zukünftig zu unterlassen, Ferienwohnungen der Klägerin auf seiner Internetpräsenz darzustellen und zu bewerben.

Nach Abgabe dieser Unterlassungserklärung waren im Internet zwar keine Lichtbilder der Wohnungen mehr abrufbar, Namens- und Adressdaten der Klägerin fanden sich jedoch weiterhin auf der Webseite des Beklagten. Da anhand dieser Daten weiterhin der Eindruck vermittelt würde, dass der Beklagte die Wohnungen der Klägerin vermittle, nahm das Gericht grundsätzlich einen Verstoß gegen die abgegebene Unterlassungserklärung an.

Zur Verteidigung berief sich der Beklagte darauf, dass es sich lediglich um Datenreste handle, die nur noch über den Cache der Suchmaschine abrufbar seien, da dieser seitens des Suchmaschinenbetreibers noch nicht aktualisiert worden sei. Insofern stellte das OLG Celle unter Berufung auf weitere obergerichtliche Rechtsprechung fest, dass der Unterlassungsschuldner durch geeignete Maßnahmen sicherstellen müsse, dass die betroffenen Inhalte nicht mehr im Internet abgerufen werden können. Diese Pflicht umfasst nach Ansicht des Gerichts nicht nur die unmittelbare Löschung von der Webseite, sondern auch die Zugangsverhinderung mittels Internetsuchmaschinen. So müsse zumindest eine Abrufbarkeit über Google als gängigste Internetsuchmaschine unterbunden werden. Im Rahmen einer Zumutbarkeitsprüfung könne höchstens fraglich sein, ob diese Pflicht auch weitere Suchmaschinenanbieter umfasse oder ob der Verweis auf deren laufende Aktualisierungen ausreiche.

Fazit und Auswirkungen auf die Hochschulpraxis

Das Urteil des OLG Celle fügt sich in die bisherige obergerichtliche Entscheidungspraxis ein. Dabei wird durchgehend die faktische technische Erreichbarkeit von Inhalten, die gegen abgegebene Unterlassungserklärungen verstoßen, in den Vordergrund gestellt. Die Gerichte verfolgen damit einen umfassenden Ansatz, bei dem die bloße technische Erreichbarkeit der Inhalte als ausreichend erachtet wird, um eine Rechtsverletzung annehmen zu können. Dass ein Abruf oftmals nur umständlich und für den Durchschnittsinternetnutzer nur in seltenen Fällen möglich ist, spielt in der Rechtsprechung keine Rolle. Bereits die bloße Möglichkeit einer Erreichbarkeit wird als ausreichend erachtet.

Das Urteil des OLG Celle erweitert den Rahmen der zumutbaren Handlungspflichten auf die Bereinigung des Cache großer Suchmaschinenanbieter. Dies erscheint insoweit nicht als zwingend notwendig, da sich der Cache im Rahmen der Aktualisierungsvorgänge der Suchmaschinen ohnehin regelmäßig ändert und somit das Fortbestehen der Rechtsverletzung nur von kurzer Dauer ist. Auf der anderen Seite erscheint es vor dem Hintergrund, dass die faktische Erreichbarkeit als ausreichend für einen Verstoß erachtet wird, jedoch auch als inkonsequent, die zumutbaren Handlungspflichten auf einzelne große Suchmaschinenanbieter zu beschränken. Hier besteht im Rahmen der Zumutbarkeit ein Widerspruch.

Das Urteil des OLG Celle wirft zudem die Frage auf, inwiefern seitens der Verpflichteten auch auf Internetarchivangebote eingewirkt werden muss. Mittels dieser Angebote lässt sich der Zustand vieler Webseiten zeitlich zurückversetzt anzeigen und somit die Rechtsverletzung reproduzieren. In diesem Zusammenhang stellt sich die Frage, wann die Grenze des Zumutbaren überschritten ist.

Insgesamt lässt sich festhalten, dass Hochschulen bei der Abgabe einer Unterlassungserklärung besondere Vorsicht walten lassen sollten. Dieser Bereich gestaltet sich zum einen als besonders komplex und zum anderen können Fehler hohe Kosten auslösen. Aus diesem Grund sollte vor der Abgabe einer Unterlassungserklärung immer ein Rechtsbeistand zu Rate gezogen werden.

Insbesondere bei Rechtsverletzungen im Internet sollten darüber hinaus alle technischen Möglichkeiten zur Beseitigung ergriffen werden. Die Rechtsprechung zeigt, dass das bloße Entfernen von der eigenen Webseite nicht als ausreichend erachtet wird.

Was lange währt… muss nicht immer gut sein – Teil 1

Rechtliche Probleme bei dem Angebot und der Nutzung einer automatischen E-Mail-Weiterleitung an Hochschulen

von Florian Klein

Die Nutzung einer automatischen E-Mail-Weiterleitung von der universitären E-Mail-Adresse auf eine private E-Mail-Adresse erfreut sich unter Hochschulmitgliedern seit Jahren großer Beliebtheit. Rechtlicher Risiken war man sich dabei meistens überhaupt nicht bewusst, sodass diese Praxis lange bedenkenlos Bestand hatte. Dass dieses Verhalten jedoch keineswegs ohne Weiteres rechtlich zulässig ist, soll in diesem Beitrag aufgezeigt werden, um Hochschulen zu animieren, die Aufrechterhaltung einer solchen Service-Option kritisch zu überdenken.

I. Hintergrund

Zu dem Service-Angebot einer Hochschule gehört es in aller Regel, dass Studierenden und Mitarbeitern ein eigener E-Mail-Dienst mit speziellen Hochschul-Mail-Adressen zur Verfügung gestellt wird, der über hochschuleigene Server betrieben wird. Einigen Hochschulmitgliedern ist die Nutzung eines solchen Dienstes jedoch zu unkomfortabel, weil sie bereits eine eigene private E-Mail-Adresse besitzen und ihre Kommunikation deshalb bevorzugt darüber abwickeln möchten. Um dies zu ermöglichen, bieten Hochschulen zusätzlich meist die Option an, im System eine private E-Mail-Adresse zu hinterlegen, auf die sämtliche E-Mails, die an die Hochschul-Mail-Adresse des jeweiligen Nutzers adressiert sind, automatisch weitergeleitet werden. Zum Teil kann dabei auch ausgewählt werden, ob im Hochschulpostfach zumindest eine Kopie der eingehenden und automatisch weitergeleiteten E-Mails abgelegt werden soll. Ist diese Einstellung einmal aktiviert, endet die Weiterleitung erst, wenn man diese manuell deaktiviert. Bis zu diesem Zeitpunkt werden alle E-Mails ohne jegliche menschliche Kontrolle des Inhalts an einen externen E-Mail-Provider weitergereicht, der dem Nutzer seine private E-Mail-Adresse zur Verfügung stellt. Dies kann in vielen Fällen dazu führen, dass kritische Informationen und Daten die Einflusssphäre der Hochschule verlassen und auf Servern landen, die keiner Kontrolle der Hochschule mehr unterliegen. Führt man sich dies vor Augen, drängen sich in Zeiten einer steigenden Bedeutung des Datenschutzes unweigerlich Zweifel auf, ob dies im Hinblick auf dienstliche Daten tatsächlich mit den geltenden Gesetzen vereinbar ist.

II. Rechtliche Betrachtung

Aus rechtlicher Sicht gibt es bei einer automatischen E-Mail-Weiterleitung in erster Linie vier Problemfelder: das Datenschutzrecht, den strafrechtlichen Geheimnisschutz, das Arbeitsrecht und das Informationsfreiheitsrecht. Vorab ist aber darauf hinzuweisen, dass viele rechtliche Fragen in diesem Zusammenhang kein Spezifikum der automatischen E-Mail-Weiterleitung sind, sondern sich durchaus auch bei einer manuellen, individuellen Weiterleitung stellen können. Eine Besonderheit ergibt sich allerdings aus der fehlenden inhaltlichen Kontrollmöglichkeit bei einer automatischen E-Mail-Weiterleitung, da diese sich ja gerade dadurch auszeichnet, dass jede Mail unterschiedslos weitergeleitet wird. Kann im Einzelfall deshalb überhaupt nicht festgestellt werden, welche Daten und Inhalte weitergeleitet werden, ist für die Beurteilung der rechtlichen Zulässigkeit im Zweifel davon auszugehen, dass darunter auch kritische Inhalte sind, für deren Weitergabe spezielle rechtliche Anforderungen bestehen, zumal E-Mails sehr häufig Daten beinhalten, die

dem Datenschutzrecht unterliegen.
Um den verschiedenen rechtlichen Fragen in hinreichendem Maße gerecht werden zu können, befasst sich dieser Beitrag zunächst nur mit dem Datenschutzrecht. Im kommenden Monat folgt dann der zweite Teil, der sich mit den übrigen drei Rechtsgebieten auseinandersetzt.

1. Rechtliche Beurteilung bei Mitarbeitern

Hochschulen sind in vielen Fällen als Körperschaften des öffentlichen Rechts organisiert. In Nordrhein-Westfalen legt dies beispielsweise § 2 Abs. 1 S. 1 Hochschulgesetz NRW (HG NRW) fest. Insofern ergibt sich, dass die jeweiligen Landesdatenschutzgesetze für staatliche Hochschulen als öffentliche Stellen zur Anwendung kommen und Datenverarbeitungen der Hochschulen deshalb an deren Maßstab zu messen sind. Da jedes Bundesland ein eigenes Landesdatenschutzgesetz erlassen hat, erfolgt die Darstellung hier exemplarisch anhand des nordrhein-westfälischen Datenschutzgesetzes. Die meisten Ausführungen lassen sich jedoch auf die anderen Bundesländer übertragen, da die wesentlichen Grundsätze in allen Bundesländern sehr ähnlich sind.

Die erste Differenzierung, die bei der rechtlichen Betrachtung vorzunehmen ist, ist die zwischen Mitarbeitern der Hochschule und Studierenden, da insofern unterschiedliche Regelungen zu beachten sind. Mitarbeiter sind Teil der Hochschule und ihr Verhalten wird dieser zugerechnet, soweit sie zur Erfüllung ihrer Aufgaben tätig werden und in einem Arbeits- bzw. Beamtenverhältnis zu ihr stehen. Insofern ergeben sich aus dem Status als Beamter oder Angestellter im öffentlichen Dienst keine Unterschiede. Dienstliche Tätigkeiten der Mitarbeiter werden somit nach dem für die Hochschule geltenden Datenschutzrecht beurteilt, wobei die Hochschule nach außen die für diese Datenverarbeitungen verantwortliche Stelle ist.

Relevante Datenverarbeitung

Ausgangspunkt jeder datenschutzrechtlichen Betrachtung ist die Feststellung, ob personenbezogene Daten in einer Weise verarbeitet werden, die vom Datenschutzgesetz erfasst ist. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 DSG NRW). In Bezug auf die Daten, die typischerweise in einer E-Mail enthalten sind, sind dies beispielsweise (personalisierte) E-Mail-Adressen, Namen, Kontaktdaten und Ähnliches. Werden also E-Mails automatisch an eine andere Adresse weitergeleitet, sind in aller Regel auch personenbezogene Daten betroffen.

Problematisch ist dies dann, wenn in der Weiterleitung der E-Mails eine Datenverarbeitung zu sehen ist. Zu denken ist vorrangig an eine Datenübermittlung. Als Übermitteln definiert das Gesetz das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, dass die Daten durch die verantwortliche Stelle weitergegeben oder zur Einsichtnahme bereitgehalten werden […]. Dabei soll eine Übermittlung nicht nur dann vorliegen, wenn der Empfänger die personenbezogenen Daten tatsächlich zur Kenntnis nimmt, sondern auch schon dann, wenn er nur die faktische Möglichkeit hat, die Daten tatsächlich zur Kenntnis zu nehmen. Warum diesem Übermittlungsbegriff ein derart weites Verständnis zugrunde gelegt wird, erschließt sich bei einem Blick auf den Sinn und Zweck der Regelungen zur Datenübermittlung: es geht nämlich primär darum, jegliche gezielte Ausweitung des Personenkreises, dem die personenbezogenen Daten zugänglich sind, zu verhindern und eine solche droht schon dann, wenn nur die faktische Möglichkeit der Kenntnisnahme besteht.
Dritter ist im Fall der automatischen E-Mail-Weiterleitung, bei der ein Mitarbeiter seine eingehenden E-Mails an eine private E-Mail-Adresse weiterleiten lässt, nicht der Mitarbeiter als Inhaber der E-Mail-Adresse, sondern dessen Mail-Provider. Sofern es nicht um hochschulinterne Weiterleitungen geht, bei denen diese Problematik nicht besteht, ist der Anbieter des Mailing-Dienstes weder Teil der Hochschule noch steht er in einem besonderen Verhältnis zu ihr, sodass er sich außerhalb der verantwortlichen Stelle befindet.
Damit eine datenschutzrechtlich relevante Übermittlung vorliegt, müssten die jeweiligen Daten also auch durch die Hochschule an den Mail-Provider weitergegeben werden. Der Begriff der Weitergabe erfasst jede Handlung, durch die die in den Daten enthaltenen Informationen in den Bereich des Empfängers gelangen. Auch wenn der Zweck der E-Mail-Weiterleitung nicht darin liegt, seinem privaten E-Mail-Provider Informationen zu verschaffen, gelangen dadurch die Daten aus allen dienstlichen E-Mails in dessen Machtbereich und können theoretisch von diesem eingesehen werden, solange die Inhalte nicht verschlüsselt sind. Schon auf dem Transportweg werden E-Mails häufig mit Postkarten verglichen, da sie leicht abgefangen und die Inhalte ausgelesen werden können. Sind sie aber erst auf dem fremden Mail-Server eingegangen, kann

der Mail-Provider erst recht faktisch ohne Probleme auf sie zugreifen.
Selbst wenn zum Teil gefordert wird, dass eine tatsächliche Kenntnisnahme der Daten durch den Dritten erfolgt, ist eine solche Kenntnisnahme nicht immer auszuschließen, da beispielsweise Anbieter wie Google tatsächlich E-Mail-Inhalte scannen und – mindestens zu Werbezwecken – automatisiert auswerten. Als Gegenpol dazu stehen unter anderem die deutschen Anbieter, die an das Fernmeldegeheimnis gebunden sind und die deshalb nicht auf die E-Mail-Inhalte zugreifen dürfen. Dies schließt einen Zugriff allerdings nur rechtlich und keineswegs faktisch aus. Auch diese haben also die tatsächliche Möglichkeit einer Kenntnisnahme, sodass im Zweifel selbst bei diesen eine Weitergabe zu bejahen sein dürfte.
Dass diese Weitergabe auch durch die Hochschule als verantwortliche Stelle erfolgt, ergibt sich daraus, dass der jeweilige Hochschulmitarbeiter die automatische E-Mail-Weiterleitung aktiviert und damit die Weitergabe der Daten sämtlicher eingehender E-Mails veranlasst hat. Dieses Verhalten muss sich die Hochschule zurechnen lassen.
Es ist allerdings darauf hinzuweisen, dass diese Konstellation einer automatischen E-Mail-Weiterleitung in der Rechtswissenschaft bisher kaum diskutiert wurde.

Dennoch lässt sich als weiteres Argument für die Einordnung als Datenübermittlung eine Parallele zum Cloud-Computing anführen. Zwar gibt es dieses in verschiedensten Ausprägungen, doch ist eine davon die Bereitstellung von Speicherplatz auf Servern des externen Diensteanbieters für den Cloud-Nutzer. Nimmt jemand einen solchen Dienst in Anspruch und verlagert seine Daten in den Cloud-Speicher, erfolgt dies nicht mit der Intention, dass der Cloud-Anbieter diese zur Kenntnis nehmen soll, sondern dient vorwiegend der Arbeitserleichterung, da die Daten von überall über das Internet abrufbar sind und man sich das Vorhalten eigener großer Speichermedien ersparen kann. Dennoch ist der Cloud-Anbieter faktisch in der Lage, die gespeicherten Daten zur Kenntnis zu nehmen. Hier besteht also eine Konstellation, die der E-Mail-Weiterleitung sehr ähnlich ist, da in beiden Fällen externe Diensteanbieter faktisch Zugriffsmöglichkeiten auf fremde Daten erhalten, auch wenn die Ausnutzung dieser Zugriffsmöglichkeiten vom Nutzer nicht gewollt ist.
Im Hinblick auf das Cloud-Computing mithilfe externer Diensteanbieter besteht weitgehend Einigkeit, dass dieses als sogenannte Auftragsdatenverarbeitung zu qualifizieren ist. Die Auftragsdatenverarbeitung (§ 11 DSG NRW) ist ein rechtliches Konstrukt, das es datenverarbeitenden Stellen erleichtern soll, sich bei der Datenverarbeitung der Unterstützung externer Stellen zu bedienen. Das funktioniert dadurch, dass das Gesetz einen externen Datenverarbeiter nicht als Dritten ansieht, wenn eine wirksame Vereinbarung über die Auftragsdatenverarbeitung geschlossen wurde. Dies führt dazu, dass eine Weitergabe von Daten an ihn im Rechtssinne keine Übermittlung von Daten darstellt und deshalb unter erleichterten Voraussetzungen zulässig ist. Verantwortlich bleibt bei dieser Konstruktion stets der Auftraggeber, der verpflichtet ist, sich im Rahmen der Vereinbarung Kontroll- und Weisungsrechte von dem externen Dienstleister einräumen zu lassen und die Umstände der Datenverarbeitung zu regeln.
Zugleich bedeutet dies aber auch, dass bei einer unwirksamen oder einer nicht vorhandenen Vereinbarung über die Durchführung einer Auftragsdatenverarbeitung die gesetzliche Privilegierung der Datenweitergabe nicht eingreifen kann und dann eine Datenübermittlung vorliegen muss. Denn wenn die Weitergabe der Daten an den Cloud-Anbieter als solche keine Datenübermittlung im Sinne des Datenschutzgesetzes darstellen würde, bräuchte man gar keine Auftragsdatenverarbeitung. Nimmt man also diese Parallele des Cloud-Computings zu Hilfe, ergibt sich auch für die automatische E-Mail-Weiterleitung, dass in der Weiterleitung der E-Mails an eine private E-Mail-Adresse eine Übermittlung der darin enthaltenen Daten an den E-Mail-Provider zu sehen ist.

Doch selbst wenn man dies ungeachtet der oben stehenden Argumente bestreiten möchte, verbleibt immer noch eine datenschutzrechtlich relevante Nutzung von Daten (§ 3 Abs. 2 Nr. 7 DSG NRW), da dies als Auffangtatbestand jede sonstige Verwendung personenbezogener Daten erfasst.

Datenschutzrechtliche Erlaubnistatbestände

Ist also das Vorliegen einer datenschutzrechtlich relevanten Verwendung festgestellt, ist für deren Zulässigkeit erforderlich, dass eine Einwilligung des Betroffenen vorliegt oder eine gesetzliche Vorschrift dieses Verhalten erlaubt (§ 4 DSG NRW).
Von einer Einwilligung des Betroffenen wird man bei einer automatischen E-Mail-Weiterleitung indes nicht ohne Weiteres ausgehen können. Zum einen weiß der Absender überhaupt nicht, dass seine E-Mails, die er an eine Hochschuladresse sendet, an einen anderen Mail-Provider weitergeleitet werden und muss damit auch nicht zwingend rechnen, sodass allein der Versand einer E-Mail, die personenbezogene

Daten enthält, noch nicht als Einwilligung durch schlüssiges Verhalten eingestuft werden kann. Zum anderen könnte der Absender ohnehin nur in die Verwendung der eigenen Daten einwilligen. Im Hinblick auf die Daten Dritter, die potentiell per E-Mail verschickt werden, wäre die Einwilligung des jeweiligen Dritten erforderlich, die naturgemäß nicht vom Absender der E-Mail erteilt werden kann.

Dass das DSG NRW oder eine andere Rechtsvorschrift eine solche Datenverwendung erlaubt, kann ebenfalls nicht pauschal unterstellt werden. Insbesondere ist nicht ersichtlich, inwiefern eine automatische E-Mail-Weiterleitung zur Aufgabenerfüllung der Hochschule erforderlich ist, da in aller Regel auch mit den Hochschul-Mail-Adressen gearbeitet werden kann und ein potentiell geringfügig verringerter Komfort gegenüber privaten Mail-Adressen nicht ausreichend ist, um die strengen Anforderungen des Erforderlichkeitskriteriums zu erfüllen. Da also keineswegs für alle Fälle sichergestellt ist, dass ein Erlaubnistatbestand eingreift, bestehen nicht unerhebliche datenschutzrechtliche Bedenken gegenüber einer automatischen E-Mail-Weiterleitung.
Dies gilt umso mehr, als bei Datenübermittlungen an E-Mail-Provider, die ihren Sitz außerhalb der EU-Mitgliedstaaten haben, wie dies z. B. bei den US-amerikanischen Anbietern der Fall ist, noch höhere Anforderungen gelten. So muss im Normalfall nämlich, zusätzlich zu den üblichen Zulässigkeitsvoraussetzungen, ein angemessenes Datenschutzniveau gewährleistet werden (§ 17 DSG NRW), welches in den meisten Fällen nicht vorliegt und nur durch besondere Vorkehrungen geschaffen werden kann (z. B. durch die Vereinbarung sogenannter Standardvertragsklauseln).

Datenschutz durch technische und organisatorische Maßnahmen

Außerdem ist zu berücksichtigen, dass die Landesdatenschutzgesetze die verantwortlichen Stellen dazu verpflichten, die Ausführung und Einhaltung der datenschutzrechtlichen Vorschriften durch technische und organisatorische Maßnahmen sicherzustellen (z. B. § 10 DSG NRW). Zur Konkretisierung dieser Verpflichtung enthalten die Gesetze eine Auflistung bestimmter Maßnahmen, die der Gewährleistung verschiedener datenschutzrechtlicher Schutzstandards dienen sollen. Dazu gehört beispielsweise, dass die Vertraulichkeit und Verfügbarkeit der Daten sichergestellt werden müssen, indem Maßnahmen getroffen werden, die garantieren, dass die Daten nur von Befugten zur Kenntnis genommen werden können, zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können.
Bei der Nutzung einer automatischen E-Mail-Weiterleitung gelangen geschützte Daten in die Hände eines Dritten, bei dem nicht sichergestellt ist, dass er seinerseits die erforderlichen Schutzmaßnahmen getroffen hat. Dazu kommt, dass die Hochschulen auf die externen Mail-Provider überhaupt keinen Einfluss und deshalb keine Kontroll- oder Steuerungsmöglichkeit zur Einführung der erforderlichen technischen und organisatorischen Maßnahmen haben. Darüber hinaus dürfte man zu den erforderlichen organisatorischen Maßnahmen der Hochschule in einem solchen Fall zählen können, dass sie ihren Mitarbeitern untersagt, solche automatischen E-Mail-Weiterleitungen einzurichten und dies auch technisch verhindert oder zumindest erschwert, indem entsprechende Funktionen gar nicht erst angeboten werden. Die allgemeine Pflicht der Hochschule, ihren Betrieb so zu organisieren, dass geltende Gesetze Beachtung finden und möglichst keine Rechtsverletzungen begangen werden („Compliance“), ist hier im Hinblick auf den Datenschutz spezialgesetzlich konkretisiert. Das Service-Angebot einer automatischen E-Mail-Weiterleitung für dienstliche E-Mail-Konten, welches sich technisch relativ leicht verhindern lässt, wird man deshalb als Verstoß gegen § 10 DSG NRW ansehen müssen.

Pflichten gegenüber der Datenschutzaufsicht

Problematisch ist die automatische E-Mail-Weiterleitung zudem im Hinblick auf die Verpflichtungen, die der Hochschule gegenüber der Datenschutzaufsicht obliegen. Der Landesbeauftragte für Datenschutz und Informationsfreiheit (LDI) hat eine Aufsichtsfunktion gegenüber den öffentlichen Stellen, da das Gesetz vorsieht, dass er die Einhaltung der datenschutzrechtlichen Vorschriften bei diesen überwacht (§ 22 DSG NRW). Um diese Aufgabe erfüllen zu können, sind die Hochschulen als öffentliche Stellen generell verpflichtet, den LDI bei seiner Aufgabe zu unterstützen und erforderlichenfalls Amtshilfe zu leisten. Insbesondere sind ihm Auskünfte über Fragen zur Datenverarbeitung zu erteilen, Einsicht in alle Datenverarbeitungsvorgänge, Dokumentationen und Aufzeichnungen zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, jederzeit Zutritt zu allen Diensträumen und Zugriff auf elektronische Dienste zu ermöglichen und ggf. auch Kopien von Unterlagen zur Verfügung zu stellen. Im Einzelfall kann dies auch bedeuten, dass bestimmte dienst-

liche E-Mails vorzulegen sind. Wenn nun aber die E-Mails nur noch in privaten Postfächern auf fremden Servern liegen, weil sie ohne Speicherung einer Kopie im Postfach der Hochschul-Mail-Adresse automatisch weitergeleitet werden, ist der Hochschule die Erfüllung dieser Verpflichtung faktisch oft nicht mehr möglich. Dieses Problem stellt sich in ähnlicher Hinsicht auch noch unter zwei anderen rechtlichen Aspekten (Arbeitsrecht und Informationsfreiheitsrecht), die allerdings erst im zweiten Teil dieses Beitrags dargelegt werden.

Löschungspflichten

Zu guter Letzt ist noch zu bedenken, dass das Datenschutzrecht Löschungspflichten in Bezug auf solche personenbezogenen Daten vorsieht, deren Speicherung unzulässig ist oder deren Kenntnis nicht mehr zur Aufgabenerfüllung der verarbeitenden Stelle erforderlich ist. Dies ist Ausfluss des Grundsatzes der Datensparsamkeit und der Datenvermeidung, wonach möglichst wenige personenbezogene Daten erhoben und verarbeitet werden sollen und dies auch nur solange wie nötig. Die Einhaltung dieser Löschungspflichten kann nicht mehr effektiv durch die Hochschule kontrolliert werden, wenn die E-Mails mit entsprechenden Daten nicht mehr in ihrem Einflussbereich gespeichert sind, sondern auf den Servern externer Mail-Provider liegen.

Rechtsfolgen

Für datenschutzrechtliche Verstöße bestehen in verschiedenem Maße gesetzliche Sanktionen. So erklärt § 34 DSG NRW die rechtswidrige Weitergabe nicht offenkundiger personenbezogener Daten zur Ordnungswidrigkeit, die mit einer Geldbuße bis zu 50.000 € geahndet werden kann. Diese ordnungsrechtliche Verantwortlichkeit ist zuvorderst eine persönliche und trifft deshalb denjenigen Mitarbeiter, der die automatische E-Mail-Weiterleitung eingestellt und genutzt hat. Im Einzelfall kann jedoch unter den hier nicht näher zu erörternden Voraussetzungen des § 30 Ordnungswidrigkeitengesetz (OWiG) auch eine Geldbuße gegen die Hochschule verhängt werden. Dies kann relevant werden, wenn der Leitungsebene eine Aufsichtspflichtverletzung dergestalt vorzuwerfen ist, dass unzureichende organisatorische Vorkehrungen zur Sicherstellung der Einhaltung datenschutzrechtlicher Regelungen getroffen wurden.

Darüber hinaus kann jeglicher Verstoß gegen datenschutzrechtliche Vorschriften gemäß § 24 DSG NRW zu einer Beanstandung durch den LDI führen, der insofern eine Aufsichtsaufgabe hat. Eine solche Beanstandung müsste gegenüber dem Rektor erfolgen und ist mit einer Aufforderung zur Abgabe einer Stellungnahme verbunden, welcher innerhalb einer bestimmten Frist nachgekommen werden muss. Gleichzeitig unterrichtet der LDI auch die Aufsichtsbehörde. Dies ist unter anderem deshalb notwendig, weil der LDI selbst – zumindest in einigen Bundesländern – keine Durchsetzungsbefugnisse hat. Verweigert die Hochschule trotz Beanstandung durch den LDI eine Anpassung des Verhaltens und teilt die Aufsichtsbehörde die Ansicht des LDI, kann diese (im Fall der nordrhein-westfälischen Hochschulen ist dies das Ministerium für Innovation, Wissenschaft und Forschung des Landes Nordrhein-Westfalen) dann gegebenenfalls die Durchsetzung erzwingen. Im Hinblick auf die konkrete Vorgehensweise in anderen Bundesländern ist auf die entsprechenden Normen der jeweiligen Landesdatenschutzgesetze zu verweisen.

Schließlich ist noch zu beachten, dass § 20 DSG NRW einen Schadensersatzanspruch des Betroffenen vorsieht, wenn dieser einen Schaden durch eine unrichtige oder unzulässige Datenverarbeitung erleidet. In schweren Fällen kann der Betroffene sogar einen Anspruch auf Ersatz seiner immateriellen Schäden haben („Schmerzensgeld“). Das erforderliche Verschulden der verantwortlichen Stelle wird dabei vermutet, kann aber widerlegt werden, sofern es tatsächlich an einem fahrlässigen oder vorsätzlichen Handeln fehlte. Erfolgte die Datenverarbeitung in einer automatisierten Datei, ist der Schadensersatzanspruch sogar verschuldensunabhängig, dafür allerdings in der Höhe auf einen bestimmten Betrag gedeckelt. Anspruchsgegner ist insofern in jedem Fall die Hochschule als Träger der verantwortlichen Stelle.

2. Rechtliche Beurteilung für Studierende

Für Studierende sind gesonderte Erwägungen anzustellen. Selbst wenn diese nach dem jeweiligen Hochschulgesetz als Mitglieder der Hochschule qualifiziert werden (so z. B. für eingeschriebene Studierende § 9 Abs. 1 S. 1 HG NRW) und damit in einem Sonderrechtsverhältnis zur Hochschule stehen, muss die Hochschule sich deren Verhalten nicht ohne Weiteres zurechnen lassen. Sie sind deshalb datenschutzrechtlich nicht Teil der öffentlichen Stelle „Hochschule“, sodass ihr Handeln auch nicht nach dem Landesdatenschutzgesetz zu beurteilen ist. Vielmehr unterliegen sie als Private dem Bundesdatenschutzgesetz (BDSG) und sind dessen Terminologie folgend

sogenannte „nicht-öffentliche Stellen“. Das BDSG wiederum legt in § 1 Abs. 2 Nr. 3 fest, dass es dann nicht anwendbar ist, wenn solche nicht-öffentlichen Stellen eine Datenverarbeitung ausschließlich für persönliche oder familiäre Tätigkeiten vornehmen. Hiermit will der Gesetzgeber Privatleute in einem engen Kreis von den Restriktionen des Datenschutzrechts befreien, um ihr privates Handeln nicht unverhältnismäßig zu erschweren. Zu diesem engen persönlichen Bereich sollen auch Tätigkeiten im Rahmen der Aus- und Fortbildung gehören, wozu man auch das Studium zählen können wird, solange die jeweiligen Tätigkeiten nicht über den üblichen persönlichen Kreis hinausreichen. Richten sich Studierende also eine automatische E-Mail-Weiterleitung von ihrer Hochschul-Mail-Adresse auf eine private E-Mail-Adresse ein und nutzen diese für Zwecke des Studiums und andere private Angelegenheiten, sind die Voraussetzungen dieses speziellen Anwendungsbereichsausschlusses erfüllt und das Datenschutzrecht deshalb nicht anwendbar. Daraus folgt zugleich, dass insoweit anders als bei den Mitarbeitern datenschutzrechtliche Bedenken nicht bestehen und zahlreiche Fälle denkbar sind, in denen die Nutzung einer automatischen E-Mail-Weiterleitung durch Studierende rechtmäßig möglich ist.

Dieser Rahmen einer Datenverarbeitung zu ausschließlich persönlichen Zwecken wird jedoch überschritten, sobald Studierende bestimmte Selbstverwaltungsaufgaben der Hochschule wahrnehmen, indem sie beispielsweise in Gremien, Ausschüssen, Fachschaften oder Ähnlichem tätig werden und dabei personenbezogene Daten verarbeiten. Insoweit kommt das Datenschutzrecht also auch für Studierende zur Anwendung. Das Gleiche gilt für eine sonstige Nutzung der E-Mail-Adresse für Tätigkeiten, die über den persönlichen Bereich hinausgehen. Obwohl dies keine seltenen Konstellationen sind, dürfte es unverhältnismäßig sein, allein deshalb ein pauschales Verbot des Angebots einer automatischen E-Mail-Weiterleitung für alle Studierenden zu fordern. Stattdessen rückt hier die Eigenverantwortung der jeweiligen Studierenden in den Vordergrund, die zunächst selbst dafür Sorge tragen müssen, dass sie gesetzeskonform handeln. Aufgrund der allgemeinen Pflicht der Hochschule zur Organisation des Hochschulbetriebs in der Form, dass gesetzliche Verbote eingehalten werden und insbesondere auch das Datenschutzrecht Beachtung findet, könnte man von ihr aber unter Umständen verlangen, dass sie Studierende, die in Hochschulgremien tätig sind, darauf hinweist, dass die Nutzung einer automatischen E-Mail-Weiterleitung datenschutzrechtlich nicht risikolos und potentiell rechtswidrig ist. Deshalb bietet es sich an, im Rahmen des Aktivierungsprozesses der automatischen E-Mail-Weiterleitung für Studierende einen entsprechenden Warnhinweis aufzunehmen, dessen Kenntnisnahme bestätigt werden muss, sofern dieses Service-Angebot für Studierende überhaupt aufrechterhalten werden soll.

Darüber hinaus verpflichtet § 11 Abs. 3 HG NRW die Mitglieder der Hochschule ohnehin in allen Angelegenheiten zur Verschwiegenheit, die ihnen als Träger eines Amtes oder einer Funktion bekannt geworden sind und deren Vertraulichkeit sich aus Rechtsvorschriften, auf Grund besonderer Beschlussfassung des zuständigen Gremiums oder aus der Natur des Gegenstandes ergibt. Verstöße gegen diese Verschwiegenheitspflicht können durch Maßnahmen zur Wiederherstellung der Ordnung geahndet werden, welche allerdings von der Hochschule entsprechend geregelt sein müssen (§ 11 Abs. 5 HG NRW). Ob diese Verschwiegenheitspflicht bei der Nutzung einer automatischen E-Mail-Weiterleitung eingehalten wird, bei der potentiell solche geheimen Inhalte in den Machtbereich des externen E-Mail-Providers gelangen, ist zumindest zweifelhaft.

III. Fazit

Schon die datenschutzrechtliche Betrachtung hat gezeigt, dass das Service-Angebot einer automatischen E-Mail-Weiterleitung durch Hochschulen jedenfalls für ihre Mitarbeiter rechtliche Risiken mit sich bringt, denen nur durch die Abschaffung dieses Angebots sicher vorgebeugt werden kann. Festzuhalten sind aber auch zwei andere Fakten: zum einen stellen sich diese Probleme in der Regel nicht bei Weiterleitungen an eine andere hochschulinterne E-Mail-Adresse desselben Nutzers, da der Herrschaftsbereich der verantwortlichen Stelle dabei nicht verlassen wird und die Daten nicht in die Hände eines Dritten gelangen. Zum anderen ist darauf hinzuweisen, dass bisher – soweit ersichtlich – weder Gerichtsentscheidungen zu dieser Fragestellung ergangen sind noch sonstige Fälle einer Ahndung eines solchen Angebots bekannt geworden sind. Auch die rechtswissenschaftliche Literatur setzt sich so gut wie gar nicht mit diesem Problem auseinander. Ganz vereinzelt finden sich jedoch ebenfalls kritische Einschätzungen. Dennoch ist zu berücksichtigen, dass die Sensibilität für datenschutzrechtliche Fragestellungen und Standards angesichts fortwährender Diskussionen über Vorratsdatenspeicherung und scheinbar allgegenwärtige Überwachung durch Geheim-

dienste in der Bevölkerung zunimmt. Ferner sind öffentliche Stellen schon durch das Grundgesetz an Gesetz und Recht gebunden und haben eine gewisse Vorbildfunktion. Insofern sollte es nicht zum Maßstab des Handelns gemacht werden, dass dieses Angebot teils schon jahrelang Bestand hatte, ohne dass es Beanstandungen gab. Generell rechtfertigt eine lange Ausübung eines rechtswidrigen Verhaltens keine Fortführung dieser Zustände in der Zukunft. Vielmehr gehört die automatische E-Mail-Weiterleitung auf den Prüfstand der Hochschulen.

Für Studierende dagegen dürfte die automatische E-Mail-Weiterleitung aus datenschutzrechtlicher Perspektive in der Regel deutlich weniger kritisch einzustufen sein. Soweit einige Studierende im Rahmen der Aufgabenerfüllung der Hochschule in Gremien tätig werden und insoweit auch an das Datenschutzrecht gebunden sind, dürfte es unter dem Blickwinkel der Verhältnismäßigkeit vertretbar sein, dieses Service-Angebot für Studierende nicht generell abzuschaffen, sondern dessen Inanspruchnahme nur mit einer Aufklärung und einem entsprechenden Warnhinweis zu versehen. Denn es verbleibt immer noch ein großer Kreis von Studierenden, für die eine Nutzung der automatischen E-Mail-Weiterleitung datenschutzrechtlich zulässig sein dürfte.

Was lange währt… muss nicht immer gut sein – Teil 2

von Florian Klein

Im zweiten Teil des Beitrags soll es um die verbleibenden rechtlichen Fragestellungen gehen, die sich aus den Bereichen des strafrechtlichen Geheimnisschutzes, des Arbeitsrechts und der Informationsfreiheit ergeben.

I. Rechtliche Betrachtung

Aus rechtlicher Sicht gibt es bei einer automatischen E-Mail-Weiterleitung in erster Linie die vier oben genannten Problemfelder. Vorab ist aber erneut darauf hinzuweisen, dass viele rechtliche Fragen in diesem Zusammenhang kein Spezifikum der automatischen E-Mail-Weiterleitung sind, sondern sich durchaus auch bei einer manuellen, individuellen Weiterleitung stellen können. Eine Besonderheit ergibt sich allerdings aus der fehlenden inhaltlichen Kontrollmöglichkeit bei einer automatischen E-Mail-Weiterleitung, da diese sich ja gerade dadurch auszeichnet, dass jede Mail unterschiedslos weitergeleitet wird. Kann im Einzelfall deshalb überhaupt nicht festgestellt werden, welche Daten und Inhalte weitergeleitet werden, ist für die Beurteilung der rechtlichen Zulässigkeit im Zweifel davon auszugehen, dass darunter auch kritische Inhalte sind, für deren Weitergabe spezielle rechtliche Anforderungen bestehen.

Führte schon die datenschutzrechtliche Beurteilung der automatischen E-Mail-Weiterleitung im ersten Teil zur Feststellung zahlreicher rechtlicher Bedenken, können sich insbesondere aufgrund der strafrechtlich flankierten Schweigepflicht bestimmter Geheimnisträger rechtliche Gefahren für die Nutzer dieses Features ergeben.

1. Strafrechtlicher Geheimnisschutz

In einer Reihe von Fällen erkennt die Rechtsordnung die Schutzwürdigkeit von Geheimnissen an und sieht deshalb, wenn dieser Schutz durchbrochen wird, zum Teil sogar strafrechtliche Sanktionen gegen den Täter persönlich vor (Geld- oder Freiheitsstrafe). Im Zusammenhang mit der automatischen E-Mail-Weiterleitung an Hochschulen ist dabei vor allem an die Straftatbestände der Verletzung von Privatgeheimnissen [§ 203 Strafgesetzbuch (StGB)] und der Verletzung des Dienstgeheimnisses (§ 353b StGB) zu denken.

§ 203 StGB – Verletzung von Privatgeheimnissen

§ 203 StGB stellt das unbefugte Offenbaren eines fremden Geheimnisses durch Angehörige bestimmter Berufsgruppen unter Strafe, soweit diesen das Geheimnis auch gerade in dieser Eigenschaft anvertraut worden oder sonst bekannt geworden ist. Zu den geschützten fremden Geheimnissen zählen zum persönlichen Lebensbereich gehörende Geheimnisse sowie Betriebs- und Geschäftsgeheimnisse.
Als Geheimnis in diesem Sinne werden Tatsachen angesehen, die nur einem beschränkten Personenkreis bekannt sind und an deren Geheimhaltung der Betroffene ein sachlich begründetes und damit verständliches Interesse hat oder bei eigener Kenntnis der Tatsache haben würde. Dieses Geheimnis muss für den Täter fremd sein, das heißt, eine andere natürliche oder juristische Person betreffen. Während zum persönlichen Lebensbereich gehörende Geheimnisse solche sind, die sich auf die Lebensverhältnisse des Betroffenen beziehen, stehen Geschäfts- oder Betriebsgeheimnisse im Zusammenhang mit einem Geschäftsbetrieb, wobei insofern der jeweilige Unternehmer ein wirtschaftliches Interesse an deren Geheimhaltung haben muss.
Die Strafandrohung nach § 203 StGB gilt allerdings nicht für jeden, der fremde Geheimnisse offenbart. Taugliche Täter sind stattdessen nur Angehörige bestimmter Berufs- und Personengruppen, die in dieser Strafnorm einzeln aufgezählt sind. Aus dieser Auflistung sollen hier exemplarisch die für den Hoch-

schulbereich wichtigsten Gruppen herausgegriffen werden:

- Ärzte, Zahnärzte, Apotheker, Angehörige sonstiger Heilberufe, deren Ausübung oder Berufsbezeichnung eine staatlich geregelte Ausbildung erfordern (§ 203 Abs. 1 Nr. 1 StGB), und Berufspsychologen (§ 203 Abs. 1 Nr. 2 StGB), welche allesamt zahlreich in den Universitätskliniken zu finden sind
- Amtsträger (§ 203 Abs. 2 Nr. 1 StGB; insb. Beamte)
- Personen, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnehmen (§ 203 Abs. 2 Nr. 3 StGB), also primär die Mitglieder der Personalräte
- für den öffentlichen Dienst besonders Verpflichtete (§ 203 Abs. 2 Nr. 2 StGB)

Zur letzten Gruppe gehören alle, die an der Hochschule beschäftigt oder für sie tätig sind und auf die gewissenhafte Erfüllung ihrer Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet sind, sofern sie nicht ohnehin schon Amtsträger sind. Trotz der umständlichen Formulierung trifft dies auf viele Hochschulmitarbeiter zu, da es häufig vorgesehen ist, dass sogar schon studentische Hilfskräfte und erst recht wissenschaftliche Mitarbeiter förmlich nach dem Verpflichtungsgesetz auf die gewissenhafte Erfüllung ihrer Obliegenheiten und damit zur Geheimhaltung verpflichtet werden. Der Kreis der potentiellen Täter ist an Hochschulen daher nicht zu unterschätzen. Wichtig ist für die Strafbarkeit nach § 203 StGB allerdings, dass das Geheimnis dem jeweiligen Täter auch gerade in dieser Eigenschaft anvertraut oder bekannt geworden ist.

Im Hochschulbereich fallen in den von § 203 StGB geschützten Bereich insbesondere die Daten von Patienten, die in den Universitätskliniken behandelt werden. Aber auch darüber hinaus sind zahlreiche Konstellationen denkbar, in denen Angehörige der Hochschule zu einer der in § 203 StGB genannten Personengruppen gehören und in dieser Eigenschaft Kenntnis von Geheimnissen erlangen. Zu denken ist dabei beispielsweise an Forschungs- oder Geschäftsdaten von Kooperationspartnern im Rahmen von Forschungsprojekten. Als weiteres Beispiel können die sogenannten „Law Clinics“ dienen, die an einigen juristischen Fakultäten eingerichtet worden sind. In diesen können Studierende der Rechtswissenschaft unter Anleitung und Aufsicht eines Professors oder Anwalts schon während des Studiums ehrenamtlich echte Rechtsberatung erbringen und damit über die Theorie hinaus für den Anwaltsberuf üben. Die Informationen aus dem Mandatsverhältnis sind insoweit geschützte Geheimnisse. Dass auch Studierende, deren Ausbildung noch gar nicht abgeschlossen ist, schon taugliche Täter sein können, ergibt sich daraus, dass § 203 StGB nicht nur die Angehörigen der einzeln aufgezählten Berufsgruppen erfasst, sondern auch deren berufsmäßig tätigen Gehilfen sowie die Personen, die bei ihnen zur Vorbereitung auf den Beruf tätig sind. Dies betrifft daher auch Medizinstudenten in der klinischen Ausbildung und sonstige Studierende, die unterstützend im Bereich von Berufsgeheimnisträgern (nach § 203 Abs. 1 StGB) agieren.

So ist also leicht nachvollziehbar, dass durch die Nutzung einer automatischen E-Mail-Weiterleitung durch Angehörige der oben benannten Personengruppen hin und wieder auch E-Mails an einen externen Mail-Provider weitergeleitet werden, die möglicherweise Informationen enthalten, die als geschützte Geheimnisse zu qualifizieren sind. Deshalb bleibt noch zu klären, ob in einer solchen Weiterleitung ein Offenbaren im Sinne des § 203 StGB zu sehen ist.

Unter Offenbaren versteht man jede Mitteilung eines zur Zeit der Tat noch bestehenden Geheimnisses oder einer Einzelangabe an einen Dritten, der dieses zumindest in dieser Form noch nicht sicher kennt. Hierfür reicht es schon aus, dass das Geheimnis in irgendeiner Weise an einen anderen gelangt ist. Eine Offenbarung kann bereits die Ermöglichung des Zugangs zu den geheimen Daten sein. Insofern ist zwar umstritten, ob eine Strafbarkeit nur dann besteht, wenn der Dritte tatsächlich Kenntnis von dem Geheimnis genommen hat, allerdings gibt es zahlreiche Stimmen in der juristischen Fachliteratur, die schon die bloße Möglichkeit einer Kenntnisnahme ausreichen lassen. Im Übrigen kann auch eine Offenbarung durch Unterlassen stattfinden, indem ein zur Geheimniswahrung Verpflichteter beispielsweise geschützte Schriftstücke herumliegen lässt oder seinen Computer nicht hinreichend vor fremden Zugriffen schützt.

Hier zeigen sich deutliche Parallelen zu dem Merkmal der Datenübermittlung im Datenschutzrecht. Dies bedeutet, dass die automatische Weiterleitung von unverschlüsselten E-Mails, die potentiell geschützte Informationen beinhalten können und die von einem zur Geheimhaltung Verpflichteten eingesetzt wird, dazu führt, dass geheime Daten in den Herrschaftsbereich des externen E-Mail-Providers gelangen, der faktische Zugriffsmöglichkeiten hat. Selbst wenn man den Begriff des Offenbarens enger auslegt und die tatsächliche Kenntnisnahme durch den Dritten fordert, könnten sogar diese strengeren Anforderungen erfüllt werden, wenn der

externe E-Mail-Provider sämtliche E-Mail-Inhalte automatisiert scannt und auswertet (wie zum Beispiel Gmail). Mithin kann die Nutzung einer automatischen E-Mail-Weiterleitung an Hochschulen in einigen Fällen zu einer Offenbarung von Privatgeheimnissen führen.

Da die Strafbarkeit aber nur eingreift, wenn die Offenbarung unbefugt erfolgt, darf es keine Rechtfertigungsgründe geben. Eine Einwilligung des Betroffenen hat insoweit rechtfertigende Wirkung, allerdings wird diese sicher nicht in allen Fällen vorliegen. Auch der Informationsaustausch innerhalb einer Behörde sowie mit den Aufsichtsbehörden erfolgt grundsätzlich nicht unbefugt, allerdings rechtfertigt dies nicht die Weitergabe der Informationen an externe Dritte. Deshalb dürfte auch das Merkmal des Fehlens einer Befugnis zur Offenbarung regelmäßig erfüllt sein.

Schließlich muss der jeweilige Täter noch vorsätzlich handeln, was bedeutet, dass er Kenntnis von den Umständen haben muss, die die Tatbestandsmäßigkeit ausmachen, und diese billigend in Kauf genommen haben muss. Dies anzunehmen erscheint ebenfalls nicht abwegig, wenn jemand weiß, dass er zur Geheimhaltung verpflichtet ist und die automatische E-Mail-Weiterleitung dazu führt, dass E-Mails mit geschützten Inhalten, die ihn gelegentlich erreichen, in die Hände eines externen E-Mail-Providers gelangen.

Praktisch bedeutsam ist allerdings, dass die Verletzung von Privatgeheimnissen nur dann verfolgt wird, wenn der Verletzte einen Strafantrag stellt (§ 205 StGB). Verletzter ist derjenige, dessen Geheimnis offenbart wurde. Dieses Strafantragserfordernis dürfte zumindest das Risiko einer tatsächlichen Strafverfolgung erheblich minimieren, da der Verletzte bei einer automatischen E-Mail-Weiterleitung überhaupt erst einmal Kenntnis davon erlangen müsste und selbst dann fraglich ist, ob er dies als strafwürdiges Unrecht erkennen und anzeigen würde. Dennoch ist es gerade für Mitarbeiter einer öffentlichen Stelle nicht ratsam, solchen Normen zuwiderzuhandeln.

Festzuhalten ist also, dass eine Verwirklichung des Straftatbestandes der Verletzung von Privatgeheimnissen bei Nutzung einer automatischen E-Mail-Weiterleitung durch zahlreiche Hochschulangehörige droht, wobei praktisch das Strafantragserfordernis einer tatsächlichen Strafverfolgung häufig entgegensteht.

§ 353b StGB – Verletzung des Dienstgeheimnisses

§ 353b StGB ist ihm Rahmen des Geheimnisschutzes ein spezieller Tatbestand für Dienstgeheimnisse und Amtsträger, der mit einem höheren Strafrahmen ausgestattet ist als § 203 StGB, aber viele tatbestandliche Parallelen zu diesem aufweist, sodass die obigen Ausführungen zum Teil auch hier gelten. Zunächst gibt es Überschneidungen bei den betroffenen Personengruppen, denn § 353b Abs. 1 StGB gilt ebenfalls für Amtsträger, für Personen, die für den öffentlichen Dienst besonders verpflichtet sind, und für Personen, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnehmen. Im Gegensatz zu § 203 StGB geht es hier allerdings nicht zwingend um fremde Geheimnisse, sondern um Dienstgeheimnisse, für die auch kein Personenbezug erforderlich ist. Dazu können beispielsweise Prüfungsaufgaben gehören. Außerdem verlangt § 353b Abs. 1 StGB in gleicher Weise, dass jemand, der zu dem soeben benannten Personenkreis gehört, ein Geheimnis unbefugt offenbart, das ihm in dieser Eigenschaft anvertraut worden oder sonst bekannt geworden ist. Eine solche Geheimnisoffenbarung kann im Einzelfall wiederum in der Weiterleitung einer E-Mail, die ein geschütztes Geheimnis enthält, an eine externe private E-Mail-Adresse gesehen werden. Kann also nicht sicher ausgeschlossen werden, dass man E-Mails mit solchen kritischen Inhalten erhält und hat man eine Funktion inne, die eine Zugehörigkeit zum potentiellen Täterkreis begründet, sollte von der Einrichtung einer automatischen E-Mail-Weiterleitung Abstand genommen werden.

Allerdings ist hier noch zu erwähnen, dass die Verletzung von Dienstgeheimnissen gem. § 353b Abs. 1 StGB nur strafbar ist, wenn dadurch wichtige öffentliche Interessen gefährdet werden. Nach wohl herrschender Meinung soll hierfür schon eine mittelbare Gefährdung ausreichen, die darin bestehen kann, dass das Vertrauen der Allgemeinheit in die Unparteilichkeit, Unbestechlichkeit und Funktionsfähigkeit der öffentlichen Verwaltung erschüttert wird. Zwar wird man davon ausgehen können, dass eine solche Gefährdung nicht standardmäßig vorliegt, sondern vielmehr eine Ausnahme darstellt. Dennoch kann gerade angesichts der undifferenzierten und automatisierten Weiterleitung aller E-Mails nicht unbedingt ausgeschlossen werden, dass in seltenen Fällen Geheimnisse erfasst sind, deren Offenbarung mit entsprechendem Gefährdungspotential verbunden ist. Ob die Interessengefährdung vorsätzlich oder fahrlässig erfolgt, ist dabei primär für die

Höhe des gesetzlichen Strafrahmens relevant. Im Hinblick auf die übrigen Tatbestandsmerkmale ist allerdings auch hier ein vorsätzliches Handeln erforderlich. Praktisch von Bedeutung ist zudem, dass die Verletzung von Dienstgeheimnissen nur mit Ermächtigung verfolgt wird, welche im Falle der Hochschulen von den obersten Landesbehörden zu erteilen wäre (§ 353b Abs. 4 S. 2 Nr. 3 StGB).
Obwohl sich also das Risiko einer strafrechtlichen Verfolgung noch in einem überschaubaren Rahmen bewegt, kann es keinesfalls gänzlich ausgeschlossen werden, wenn eine automatische E-Mail-Weiterleitung genutzt wird.

2. Arbeitsrecht

Unter arbeitsrechtlichen Gesichtspunkten ist zu beachten, dass der Arbeitnehmer dem Arbeitgeber und der Beamte seinem Dienstherrn in dienstlichen beziehungsweise geschäftlichen Angelegenheiten grundsätzlich Rechenschaft schuldig und weisungsgebunden ist, wobei diesbezüglich gerade im Forschungsbereich häufig Ausnahmen bestehen können. Vorbehaltlich dieser Ausnahmen gehört es zu den arbeitsvertraglichen und beamtenrechtlichen Pflichten, dass dem Arbeitgeber oder Dienstherrn auf Verlangen dienstliche E-Mails vorgelegt werden. Insoweit werden E-Mails in der Regel mit Schriftstücken und dienstlicher Post verglichen. Mit dieser Pflicht korrespondiert aber aufgrund des Fernmeldegeheimnisses nicht das Recht des Arbeitgebers/Dienstherrn, eigenmächtig das Postfach des Arbeitnehmers/Beamten einzusehen, sofern eine (partielle) Privatnutzung erlaubt oder geduldet ist.
Werden E-Mails auf private E-Mail-Accounts weitergeleitet, ist es nicht nur viel schwieriger, dienstliche Vorgänge zu kontrollieren, sondern die E-Mails verlassen auch generell die Einflusssphäre der Hochschule, sodass diese nicht steuern kann, wie weiter mit den E-Mails verfahren wird und dass gegebenenfalls wichtige Verwaltungsunterlagen stets verfügbar sind. Im Einzelfall kann die Nutzung einer automatischen E-Mail-Weiterleitung daher eine Pflichtverletzung des Mitarbeiters darstellen. Auch wenn sich eine Vorlage der betreffenden E-Mails bei Verweigerung der Mitwirkung des Arbeitnehmers möglicherweise gerichtlich durchsetzen lässt, werden die faktischen Zugriffsmöglichkeiten deutlich geschmälert und es droht eine Vereitelung dieses Anspruchs. Dazu kommt noch, dass sich auch der Schutz gegen unbefugte Löschungen von Daten mangels arbeitgeberseitiger Backups der privaten E-Mail-Konten kaum bewerkstelligen lässt.
Hier könnte man allenfalls dadurch Abhilfe schaffen, dass stets Kopien der weitergeleiteten E-Mails im dienstlichen E-Mail-Account abgelegt werden.

3. Informationsfreiheitsrecht

Ähnliche Probleme wie unter dem Punkt Arbeitsrecht ergeben sich im Hinblick auf das Informationsfreiheitsrecht. Zurzeit gibt es in elf der 16 Bundesländer Informationsfreiheitsgesetze, die den Zweck verfolgen, den Bürgern den freien Zugang zu Informationen, die bei öffentlichen Stellen vorhanden sind, zu gewährleisten und die grundlegenden Voraussetzungen festzulegen, unter denen derartige Informationen zugänglich gemacht werden müssen. Nur in Bayern, Baden-Württemberg, Hessen, Niedersachsen und Sachsen sind bisher keine entsprechenden Gesetze erlassen worden. Tatbestandlich gilt das Informationsfreiheitsrecht für die Verwaltungstätigkeit der öffentlichen Stellen. Für Hochschulen ist der Anwendungsbereich jedoch in der Regel eingeschränkt. So sieht zum Beispiel § 2 Abs. 3 Informationsfreiheitsgesetz NRW (IFG NRW) vor, dass dieses Gesetz für sie nur gilt, soweit sie nicht im Bereich von Forschung, Lehre, Leistungsbeurteilungen und Prüfungen tätig werden. Für die originäre Verwaltungstätigkeit bleibt jedoch auch bei Hochschulen noch ein Bereich übrig, in dem das IFG NRW zur Anwendung kommen kann. Ohne die einzelnen Voraussetzungen des Zugangsanspruchs nach dem Informationsfreiheitsgesetz hier im Detail zu erörtern, kann festgehalten werden, dass Informationen über die Verwaltungstätigkeit, die in dienstlichen E-Mails enthalten sind, grundsätzlich Gegenstand des Zugangsanspruchs nach § 4 Abs. 1 DSG NRW sein können. Nutzen also Hochschulmitarbeiter, die – zumindest teilweise – Verwaltungstätigkeiten ausüben, eine automatische E-Mail-Weiterleitung, ist nicht auszuschließen, dass vom IFG NRW erfasste Informationen an einen externen Mail-Provider weitergeleitet werden und deshalb der Kontrolle der Hochschule entzogen sind. Auch hier droht also faktisch eine unzulässige Vereitelung des Zugangsanspruchs, der aber ebenfalls durch die Ablage von Kopien der eingehenden Mails begegnet werden kann.

II. Fazit

Neben dem Datenschutzrecht gibt es noch andere rechtliche Aspekte, die zu einer kritischen Einschätzung des Angebots einer E-Mail-Weiterleitung – jedenfalls für Hochschulmitarbeiter – führen. Deshalb sollte überprüft werden, ob der

Mehrwert eines solchen Angebots tatsächlich die Eingehung dieser rechtlichen Risiken rechtfertigen kann. Nicht nur die Tatsache, dass Hochschulen als Körperschaften des öffentlichen Rechts an Recht und Gesetz gebunden sind und deshalb für solche wirtschaftlichen Kosten-Nutzen-Rechnungen an sich wenig Raum bleibt, muss dabei berücksichtigt werden, sondern auch die Tatsache, dass E-Mail-Weiterleitungen ein Relikt der 90er-Jahre darstellen und heutzutage meist entbehrlich sind. War es früher noch umständlich, verschiedene E-Mail-Konten abzurufen, ist es nunmehr sehr einfach, in seinem E-Mail-Programm verschiedene E-Mail-Adressen anzugeben, die dann allesamt abgerufen und die eingehenden E-Mails komfortabel in einem Programm angezeigt werden können.

Die einfachste technische Lösung dürfte insofern die Abschaffung der automatischen E-Mail-Weiterleitung für Mitarbeiter und Studierende darstellen, obwohl für letztere die aufgezeigten rechtlichen Probleme nur vereinzelt auftauchen. Insbesondere sind arbeits- und informationsfreiheitsrechtliche Aspekte im Hinblick auf den E-Mail-Verkehr der Studierenden belanglos. In gleicher Weise dürfte die Zugehörigkeit von Studierenden zu einer der in §§ 203, 353b StGB genannten Personengruppen der Ausnahmefall sein, sodass auch strafrechtliche Aspekte normalerweise außer Acht gelassen werden können. Für das Datenschutzrecht wurden entsprechende Schlüsse bereits in Teil 1 dieses Beitrags gezogen.

Nur aus der Macht der Gewohnheit heraus verbietet sich ein Festhalten an der bisher gelebten Praxis. Stattdessen dürfte eine kritische Diskussion des Problems durch die zuständigen Stellen der Hochschulen angezeigt sein. Bei allen Umständen, die damit verbunden sind, sollte nicht verkannt werden, dass es auch für die Außenwirkung der Hochschule positiv sein dürfte, wenn sie von sich behaupten kann, dass sensible Daten bei ihr in guten Händen sind und nicht in der ganzen Welt verteilt werden, wo eine verlässliche Kontrolle der Verwendung der Daten nicht möglich ist.

Ein Auskunftsverlangen, das man nicht ablehnen kann

Zum Auskunftsanspruch gegen Host-Provider bei Urheberrechtsverletzungen durch Dritte

von Lennart Sydow

Das Landgericht Hamburg hatte in einem Verfahren im einstweiligen Rechtsschutz vom 12.01.2015 (Az.: 310 O 11/15) über die Verpflichtung eines Webhosting-Anbieters zur Erteilung von Auskünften über seine Nutzer zu entscheiden. Solche Auskunftsansprüche gegen Dritte, die selbst nicht für die eigentliche Urheberrechtsverletzung verantwortlich sind, bestehen nur in wenigen gesetzlich geregelten Fällen. Die gewerbliche Erbringung von Dienstleistungen, die für rechtsverletzende Tätigkeiten genutzt werden, ist einer davon. Hochschulen und Forschungseinrichtungen müssen sich daher mit dem möglichen Eingang etwaiger Auskunftsersuchen beschäftigen, wenn sie als Internetzugangsanbieter auftreten oder Dritten Speicherkapazitäten zur Verfügung stellen.

I. Hintergrund

Die rechtswidrige Verbreitung von Software und Medieninhalten, wie Foto-, Film- und Musikdateien, über das Internet, ist vor deutschen Gerichten seit Jahren ein ständig aktuelles Thema. Aus rechtlicher Sicht steht dem Urheber allein das Recht zu, sein Werk über das Internet öffentlich zugänglich zu machen. Diese Inhalte können nur zulässigerweise im Internet zugänglich gemacht werden, wenn entweder eine der gesetzlichen Schrankenregelungen dies erlaubt oder der Urheber Nutzungsrechte daran eingeräumt hat. Anderenfalls stellt die Zugänglichmachung durch Dritte eine Urheberrechtsverletzung dar. Für die Rechteinhaber ist es aber oft mit erheblichen Schwierigkeiten verbunden, gegen die Verantwortlichen vorzugehen. Zwar besteht gegen die Täter und Teilnehmer einer Urheberrechtsverletzung ein Anspruch auf Unterlassung der verletzenden Handlung und im Falle einer vorsätzlichen oder fahrlässigen Verletzung auch ein Anspruch auf Schadensersatz aus § 97 Urheberrechtsgesetz (UrhG). Um diese Rechte aber durchzusetzen, ist zunächst einmal erforderlich, dass dem Rechteinhaber die Identität der handelnden Personen bekannt ist. Dies ist bei Rechtsverletzungen im Internet für die Rechteinhaber nur schwer festzustellen. Damit sie an die nötigen Informationen gelangen können, hat der Gesetzgeber in § 101 Abs. 2 UrhG unter gewissen Voraussetzungen einen Auskunftsanspruch gegen Personen vorgesehen, die nicht selbst eine Urheberrechtsverletzung vornehmen oder daran teilnehmen, sondern nur eine (technische) Hilfstätigkeit ausüben.

Nach dieser Vorschrift kann die Herausgabe verschiedener Informationen, wie beispielsweise der Name und die Anschrift der Nutzer einer Dienstleistung, verlangt werden. Der Auskunftsanspruch richtet sich unter anderem gegen denjenigen, der in gewerblichem Ausmaß Dienstleistungen erbracht hat, die für rechtsverletzende Tätigkeiten genutzt wurden. Erforderlich ist darüber hinaus, dass eine offensichtliche Urheberrechtsverletzung vorliegt und dass das Auskunftsverlangen im Einzelfall nicht unverhältnismäßig ist. Soweit Verkehrsdaten – also solche Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden (siehe § 3 Nr. 30 Telekommunikationsgesetz) – verwendet werden müssen, um die Auskunft erteilen zu können, ist zudem eine richterliche Anordnung über die Zulässigkeit der Auskunftserteilung erforderlich.

Immer wieder haben sich Gerichte diesbezüglich damit zu beschäftigen, dass Accessprovider, als gewerbliche Anbieter von Dienstleistungen, zur Erteilung von Auskünften über ihre Nutzer verpflichtet werden sollen (siehe hierzu: Klein, „Verfolgung von Urheberrechtsverletzungen im Internet erleichtert“, DFN-Infobrief Recht 5/2012).

Anfang dieses Jahres hatte das Landgericht Hamburg (LG Hamburg) nun in einem Verfahren über einen solchen Auskunftsanspruch gegen einen Webhosting-Anbieter zu entscheiden, der dem Betreiber eines BitTorrent-Trackers nicht den Netzzugang aber Serverkapazitäten zur Verfügung stellte. BitTorrent ist eines der größten Filesharing-Netzwerke, bei dem eine Inhaltsdatei in Datenpakete aufgeteilt und dann direkt zwischen Nutzern weiterverteilt wird.

II. Sachverhalt und Entscheidung des Gerichts

In dem Beschluss des LG Hamburg vom 12.01.2015 (Az.: 310 O 11/15) ging es um einen Fall, in dem die Anwälte der Rechteinhaber zunächst die Betreiber dreier großer BitTorrent-Tracker aufgefordert hatten, Inhalte ihrer Mandanten zu sperren. Tracker sind spezielle Server, die den Kontakt zwischen Teilnehmern des BitTorrent-Netzwerkes herstellen und diesen so ermöglichen, einzelne Datenpakete auszutauschen, die dann wieder zu der Inhaltsdatei zusammengesetzt werden. Sie vermitteln die Kontaktaufnahme zwischen den Nutzern des Netzwerkes, indem sie die IP-Adressen der anbietenden Rechner an den suchenden Rechner senden. Als diese nicht auf die Aufforderung reagierten, wendeten die Rechteinhaber sich an den Webhosting-Anbieter der Tracker-Server und wiesen ihn auf die rechtsverletzenden Inhalte hin. Als Hostprovider ist ein solcher Webhosting-Anbieter grundsätzlich nicht Täter oder Teilnehmer einer Rechtsverletzung, die von seinen Kunden unter Nutzung der von ihm zur Verfügung gestellten Speicherkapazitäten begangen wird. Möglich ist aber eine Verpflichtung zur Unterlassung nach den Grundsätzen der Störerhaftung, wenn der Anbieter in irgendeiner Weise willentlich und adäquat kausal zur Verletzung eines geschützten Rechtsgutes beiträgt und zumutbare Prüfpflichten verletzt hat. Um eine solche Verantwortlichkeit als Störer zu vermeiden, schaltete der Provider die Server der betroffenen Seiten auf den Hinweis der Rechteinhaber ab, nachdem er zunächst die Betreiber der Tracker-Server aufgefordert hatte, die rechtsverletzenden Inhalte zu sperren, diese aber darauf nicht reagiert hatten.

Da der Webhosting-Anbieter seinen Pflichten unverzüglich nachkam, war eine gerichtliche Geltendmachung eines Unterlassungsanspruchs gegen diesen nicht erforderlich. Sein Beitrag an der Rechtsverletzung des Tacker-Servers wurde beseitigt. Vor das LG Hamburg gelangte der Fall erst, weil die Rechteinhaber noch zusätzlich Auskunft über Namen, Anschrift und E-Mail-Adresse der Kunden des Providers verlangten, die die Tracker-Server bis zu diesem Zeitpunkt betrieben hatten. Der Anspruch zur Erteilung von Auskünften ist unabhängig von der Verpflichtung zur Unterlassung der störenden Handlung, die zu der Rechtsverletzung beiträgt. Da der Anbieter diese Auskünfte verweigerte, beantragten die Rechteinhaber vor dem LG Hamburg, dem Hostprovider die Erteilung der Auskünfte aufzugeben. Das Gericht folgte dem Antrag und stellte die Verpflichtung des Webhosting-Anbieters zur Auskunftserteilung fest, weil alle Voraussetzungen des § 101 Abs. 2 UrhG erfüllt seien: Die Rechteinhaber hatten aus Sicht der Richter glaubhaft gemacht, dass MP3-Dateien von Musikstücken, an denen sie die ausschließlichen Nutzungsrechte halten, im Internet unerlaubterweise öffentlich zugänglich gemacht worden waren. Dies sei unter Verwendung der fraglichen Tracker-Server geschehen, die die Verbindung zu den Nutzern herstellten. Sobald die Verbindung hergestellt worden war, wurden die Inhalte von verschiedenen Nutzern heruntergeladen. Der Zugriff sei somit unter Verwendung der Tracker-Server ermöglicht worden, auch wenn die Inhalte selbst nicht auf diesen hinterlegt waren. Dies wertete das Gericht als ausreichend für die erforderliche offensichtliche Rechtsverletzung. Auch habe der Webhosting-Dienst mit der Zurverfügungstellung der Serverkapazitäten in gewerblichem Ausmaß eine Dienstleistung erbracht, welche für die rechtsverletzenden Tätigkeit der Tracker-Server-Betreiber genutzt wurde.

III. Fazit und Auswirkungen für Hochschulen und Forschungseinrichtungen

Diese Einordnung zeigt, dass nicht nur die Internetzugangsanbieter von Nutzern, die Inhalte im Internet verfügbar machen, in Form einer Auskunftsverpflichtung zur Verantwortung gezogen werden können, sondern auch Serverbetreiber, die den rechtsverletzenden Inhalten ähnlich nahe stehen. Leider nicht ganz eindeutig sind die Ausführungen bezüglich der offensichtlichen Rechtsverletzung, die Voraussetzung für den Auskunftsanspruch ist. Hier ist wohl davon auszugehen, dass den Betreibern der Tracker-Server nicht selbst eine

Täterschaft oder Teilnahme an den jeweiligen Rechtsverletzungen vorgeworfen wird, denn die Inhaltsdateien werden ausschließlich von den jeweiligen Nutzern geteilt. Die Tracker-Server stellen lediglich die Verbindung zwischen Nutzern her, die dann untereinander die Datenpakete austauschen. Von daher ist anzunehmen, dass hier eine Verantwortlichkeit der Tracker ebenfalls nur nach den Grundsätzen der Störerhaftung bestehen kann, wenn diese willentlich einen kausalen Beitrag zur Verletzung leisten. Wann genau der Betreiber eines solchen Tracker-Servers aber verantwortlich ist, kann an dieser Stelle offen bleiben. Für Hochschulen und Forschungseinrichtungen spielt dies praktisch wohl kaum eine Rolle, da sie keine solchen Server betreiben.

Viel relevanter kann für Hochschulen und Forschungseinrichtungen die oben geschilderte Verpflichtung eines Webhosting-Anbieters zur Auskunftserteilung über seine Nutzer sein, auf die diese Entscheidung aufmerksam macht. Dass diese Einrichtungen Speicherkapazitäten für Dritte anbieten, ist in verschiedenen Situationen denkbar und in der Hochschulpraxis stellenweise bereits umgesetzt (zum Beispiel bei Cloud-Diensten für Studenten), wenn auch noch nicht so verbreitet wie das Angebot eines Internetzugangs. Es ist folglich damit zu rechnen, dass im Einzelfall auch gegen Hochschulen in ihrer Funktion als Access- und Hostprovider diese Auskunftsansprüche geltend gemacht werden können. Soweit im Einzelfall solche Auskunftsersuchen gestellt werden, ist zu beachten, dass diese möglichst erst nach einer Prüfung der Voraussetzungen erfüllt werden sollten. Dies gilt zumindest dann, wenn – wie im vorliegenden Fall – keine Verkehrsdaten verwendet werden müssen, um die Auskunft zu erteilen, und daher auch keine richterliche Anordnung erforderlich ist. Besonderes Augenmerk dürfte dabei auf die Frage zu legen sein, ob die Speicherung bestimmter Inhalte durch die Nutzer tatsächlich eine offensichtliche Rechtsverletzung darstellt. Es ist dann jedenfalls zu empfehlen, den Datenschutzbeauftragten und die jeweilige Rechtsabteilung einzubinden.

Dienst ist Dienst und Spaß ist Spaß

Bayerischer Verwaltungsgerichtshof über Beweisverwertungsverbote bei Zufallsfunden

von Lennart Sydow

Das oberste bayerische Verwaltungsgericht befasste sich am 01.12.2014 (Az.: 16a DZ 11.2411) mit dem Fall eines Polizeibeamten, der in einem Disziplinarverfahren wegen wiederholter verbotener Privatnutzung seines Dienstcomputers mit einer Geldbuße von 500,- Euro belegt worden war. Streitgegenstand war ein mögliches Verwertungsverbot von zufällig bei einer zulässigen Überprüfung von Dienstcomputern erlangten Beweismitteln. Dabei kam es zunächst darauf an, ob es sich um eine gezielte verdeckte Durchsuchung des Dienstcomputers handelte und dann auf die Auswirkungen des zufällig entdeckten Beweismittels.

I. Hintergrund und rechtlicher Rahmen

Besonders in Strafverfahren kann die Frage nach der Zulässigkeit von Beweisen bedeutenden Einfluss auf den Ausgang eines Verfahrens haben. Zumindest seit Beginn des 20. Jahrhunderts wird daher in Fachkreisen über die Behandlung von Beweismitteln diskutiert, die unter Verstoß gegen Verfahrensvorschriften gewonnen wurden. Grundlage dieser Diskussion ist der notwendige Ausgleich zwischen dem Bedürfnis der Wahrheitserforschung vor Gericht und dem Recht auf ein faires Verfahren. Verstöße bei der Beweiserhebung können beispielsweise die Durchsuchung einer Wohnung unter bewusster Umgehung des Erfordernisses einer richterlichen Anordnung oder das Unterlassen einer Belehrung (z. B. über ein Aussageverweigerungsrecht) eines Zeugen oder Angeklagten darstellen. Diese gesetzeswidrige Beweiserhebung muss allerdings nicht automatisch dazu führen, dass auch die Verwertung der Beweismittel vor Gericht unzulässig ist. Aber nur wenn auch die Verwertung unzulässig ist, sind die fraglichen Beweismittel durch das Gericht von vornherein abzulehnen. Sofern solche Beweismittel bereits eingebracht wurden, dürfen sie jedenfalls nicht bei der Entscheidung berücksichtigt werden. Wurde eine Entscheidung unter Berücksichtigung von Beweismitteln, deren Verwertung unzulässig ist, gefällt, kann diese mit Rechtsmitteln angegriffen werden.

Dass eine rechtswidrige Beweiserhebung zu einem Verwertungsverbot führt, ist nur in wenigen Fällen gesetzlich geregelt. Besteht eine solche ausdrückliche Regelung nicht, kann sich dennoch nach Abwägung der entgegenstehenden Interessen ergeben, dass die Verwertung der rechtswidrig erlangten Beweise Grundrechte verletzen würde und daher unzulässig ist. Selbst wenn die Beweiserhebung nicht gegen gesetzlich normierte Verfahrensvorschriften verstößt, kann sich ausnahmsweise ein Beweisverwertungsverbot ergeben, soweit Grundrechte des Betroffenen oder Dritter verletzt werden.

Auch wenn der Ursprung der Diskussion über Beweisverwertungsverbote im Strafprozessrecht liegt, stellt sich die Problematik ebenso im Disziplinar- und Zivilprozessrecht (bei letzterem insbesondere in arbeitsrechtlichen Streitigkeiten). Wie im Strafprozess kann es in solchen Verfahren darauf ankommen, welche Beweismittel zur Klärung eines Sachverhaltes verwertet werden dürfen. Verhältnismäßig bekannt sind hierbei Fälle, in denen eine unzulässige Videoüberwachung zu Informationen führt, die die Kündigung von Angestellten rechtfertigen würden. Auch hier zieht aber nicht jede rechtswidrige Erlangung von Beweismitteln ein Verwertungsverbot nach sich. Entscheidend ist vielmehr, ob eine Verletzung verfassungsrechtlich garantierter Rechte des Betroffenen vorliegt, über die im Einzelfall nach Abwägung der schutzwürdigen entgegenstehenden Interessen zu entscheiden ist. Dabei kommt es darauf an, wie schwer der Vorwurf gegen den Betroffenen wiegt und wie stark durch die Erhebung und/oder Verwertung der Beweise in seine Rechte eingegriffen wird. Zu beachten sind die Ausprägungen des Allgemeinen Persönlich-

keitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz (GG), insbesondere das Recht auf informationelle Selbstbestimmung und das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme, sowie das Fernmeldegeheimnis (§ 88 Telekommunikationsgesetz und Art. 10 GG).
Abseits der im Arbeitsrecht vieldiskutierten Problematik von Beweisverwertungsverboten bei Videoaufnahmen sind noch zahlreiche andere Konstellationen denkbar, in denen Verwertungsverbote eine Rolle spielen können. Ende letzten Jahres wurde in diesem Zusammenhang die Verwertbarkeit von Informationen, die bei einer Überprüfung eines Dienstcomputers zufällig erlangt wurden, thematisiert.

II. Sachverhalt

Im konkreten Fall ging es um ein Disziplinarverfahren gegen einen Polizeibeamten. In dem Verfahren war gegen den Beamten eine Geldbuße in Höhe von 500 € ausgesprochen worden. Grund dafür war, dass bei einer Überprüfung durch den Datenschutzbeauftragten aufgefallen war, dass der Beamte über seinen Dienstcomputer, entgegen des ausdrücklichen Verbots der privaten Nutzung, „Spaß-E-Mails“ mit privatem Inhalt über einen Verteiler an mehr als 40 Kollegen versendet hatte. Die Überprüfung bezog sich dabei auf die Dienstcomputer mehrerer anderer Kollegen und war nicht aus disziplinarrechtlichen, sondern lediglich aus datenschutzrechtlichen Gründen erfolgt. Anlass war der Eingang von Meldungen über Viren und Wurmangriffe beim Firewall-Administrator des Landeskriminalamtes. Nachdem derselbe Beamte schon zwei Jahre zuvor private Dateien mit sexuellem Inhalt über seinen dienstlichen E-Mail-Account verschickt hatte und ihm dafür ein Verweis ausgesprochen worden war, sah sich die Disziplinarbehörde zu diesem Schritt veranlasst. Hiergegen klagte der Betroffene vor dem Verwaltungsgericht München, um zu erreichen, dass das Disziplinarverfahren gegen ihn aufgehoben wird. Er war der Meinung, dass die Information, dass er die E-Mails versandt hatte, nicht hätte verwendet werden dürfen, da dies durch eine unzulässige Durchsuchung in Erfahrung gebracht worden sei. Diese Klage wurde durch das Gericht abgewiesen, woraufhin der Kläger die Zulassung der Berufung vor dem Bayerischen Verwaltungsgerichtshof beantragte.

III. Rechtliche Betrachtung

Der Bayerische Verwaltungsgerichtshof lehnte die Zulassung der Berufung mit Beschluss vom 01.12.2014 ab. Das Gericht hatte keine ernstlichen Zweifel an der Richtigkeit des Urteils der Vorinstanz. Ein Beweisverwertungsverbot bezüglich Informationen, die durch eine heimliche Durchsuchung erlangt worden sind, sei schon deswegen ausgeschlossen, weil gerade keine gezielte Durchsuchung zu den Informationen geführt habe. Eine gezielte disziplinarrechtliche Durchsuchung, die nur unter den Voraussetzungen des Art. 29 des Bayerischen Disziplinargesetzes (BayDG) erfolgen darf und daher grundsätzlich einer Anordnung der Disziplinarkammer bedarf, lag hier nach Meinung des Gerichts nicht vor. Stattdessen habe es sich lediglich um eine datenschutzrechtliche Überprüfung gehandelt, bei der zufällig die Verstöße des Beamten aufgedeckt wurden. Ob eine Durchsuchung rechtmäßig gewesen wäre, wurde folgerichtig offen gelassen.

Aber auch sonst unterlagen die Informationen, die zufällig bei der Überprüfung der Datensicherheit erlangt wurden, nach Ansicht des Gerichts keinem Beweisverwertungsverbot. Die Höhe der Anforderungen an die Zulässigkeit solcher Überprüfungen hängt erheblich davon ab, ob die private Nutzung der Dienstrechner durch den Dienstherrn oder Arbeitgeber gestattet ist. Da die EDV-Rahmenrichtlinie der Behörde den Beamten die private Nutzung der Dienstcomputer ausdrücklich untersagte, könne der Dienstherr die E-Mails der Beschäftigten in demselben Maße wie den dienstlichen Schriftverkehr einsehen. Dies umfasse auch die Möglichkeit zu überprüfen, ob eine private Nutzung trotz Verbotes stattfindet, solange der Grundsatz der Verhältnismäßigkeit beachtet wird.

Aus der Urteilsbegründung wird deutlich, dass das Gericht davon ausgeht, dass die Verwertung von Beweismitteln, die durch eine zulässige Überprüfung gefunden wurden, nur einen schwachen Eingriff in die Persönlichkeitsrechte des Betroffenen darstellt, soweit die private Nutzung des Dienstcomputers nicht gestattet ist. Das Interesse des Dienstherren, die Dienstvergehen zu ahnden, wird in diesem Fall höher bewertet. Dies ist gut nachvollziehbar, wenn man bedenkt, dass die Beweismittel bei einer zulässigen datenschutzrechtlichen Überprüfung erlangt wurden. Auch die gezielte Überprüfung der Nutzung ist, zur Aufklärung von Verstößen gegen Nutzungsverbote, im Rahmen des Verhältnismäßigkeitsgrundsatzes regelmäßig zulässig. Es erscheint daher konsequent,

wenn auch zufällig erlangte Informationen nicht anders bewertet werden, solange diese bei einer zulässigen Überprüfung erlangt wurden. Wie oben gesagt ist aber zu beachten, dass die Entscheidung über ein Verwertungsverbot immer im Einzelfall, nach einer individuellen Interessenabwägung durch das Gericht, zu treffen ist. Die Entscheidung im vorliegenden Fall kann daher lediglich als Tendenz gewertet werden und eine genaue Abwägung und rechtliche Beratung (zum Beispiel durch den Datenschutzbeauftragten) im Einzelfall nicht entbehrlich machen.

IV. Auswirkungen für Hochschulen

Für Hochschulen bedeutet dieses Urteil, dass jedenfalls in Disziplinarverfahren gegen Beamte eine Verwertung zufällig erlangter Beweismittel regelmäßig möglich sein wird, wenn diese bei einer zulässigen Überprüfung der Dienstcomputer entdeckt wurden. Aber auch für eventuelle Kündigungsstreitigkeiten von angestellten Mitarbeitern könnte man aus dem vorliegenden Urteil wertvolle Schlüsse ziehen. Die Ausführungen des Gerichts dürften zu großen Teilen auf die Verwertbarkeit von Beweismitteln in Streitigkeiten vor Arbeitsgerichten übertragbar sein. Auch dort kommt es bei der Frage nach Beweisverwertungsverboten darauf an, ob Grundrechte des Betroffenen in einer Weise betroffen sind, dass diese durch die Verwertung verletzt würden. Soweit die private Nutzung der Dienstcomputer nicht gestattet ist und dieses Verbot durchgesetzt wird, wird auch hier regelmäßig davon auszugehen sein, dass eine Verletzung der Persönlichkeitsrechte ausbleibt.

Es ist aber zu beachten, dass diese Tendenz nur für den Fall gilt, dass die private Nutzung ausdrücklich verboten ist. Ist diese gestattet, stellt sich gar nicht erst die Frage nach der Zulässigkeit der Überprüfung auf Verstöße gegen das Privatnutzungsverbot. Auch eine Überprüfung auf andere Verstöße hin ist dann zudem nicht so leicht möglich. Sobald nämlich die private Nutzung gestattet ist, gelten die strengen Anforderungen an Eingriffe in das Fernmeldegeheimnis und die Eingriffsintensität in die Persönlichkeitsrechte des Betroffenen ist deutlich größer. Um dem Verhältnismäßigkeitsgrundsatz zu entsprechen, sind daher in diesem Fall höhere Anforderungen an das hinter der Überprüfung stehende Interesse zu stellen.

Alles hat ein Ende, nur XP hat zwei!?

Forderung nach Abschaltung von behördlichen PCs mit Windows XP

von Kevin Kuta

Auf vielen privaten Rechnern wird man selbst heute noch das Betriebssystem Windows XP vorfinden. Auf das gleiche Szenario wird man auch in der öffentlichen Verwaltung treffen. Vielen Einrichtungen fällt der Umstieg auf ein neues Betriebssystem aus den unterschiedlichsten Gründen (etwa anfallende Kosten, hoher Aufwand, Zuständigkeitsprobleme) schwer. Dies kann mit Blick auf die Praxis der Aufsichtsbehörden aber gravierende Folgen haben.

I. Hintergrund

Bis zum Jahr 2011 soll Windows XP das am meisten genutzte Betriebssystem weltweit gewesen sein, bis es im Laufe desselben Jahres von Windows 7 abgelöst wurde. Neben Privathaushalten waren auch behördliche PCs mit diesem Betriebssystem ausgestattet. Zumindest mit Blick auf die behördlichen PCs ist jedoch die Vergangenheitsform falsch. Anscheinend läuft auf einer Vielzahl der PCs öffentlicher Einrichtungen zum gegenwärtigen Zeitpunkt immer noch Windows XP. Auf den ersten Blick scheint daran nichts unverständlich. Die Mitarbeiter sind an den Umgang mit diesem Betriebssystem gewöhnt und auch die Rechenzentren sind in Support-Fragen versiert. Der „Support“ ist mittlerweile jedoch der entscheidende Problempunkt an Windows XP. Dieser wurde seitens des Herstellers Microsoft für dieses Betriebssystem zum Beginn des zweiten Quartals im Jahre 2014 nach einer langen Vorlaufphase eingestellt. Bereits im Jahre 2002, also kurz nach Veröffentlichung des Produkts, wurden der weitere Fahrplan sowie das Supportende angekündigt. Dementsprechend kann von einer „Überraschung“ keine Rede sein.

Das Supportende birgt die große Gefahr der Anfälligkeit der betagten Systeme für Cyberangriffe in sich. Bisher konnten Sicherheitslücken seitens des Herstellers durch „Service Packs“ oder Sicherheitsupdates behoben und ein sicherer Umgang gewährleistet werden. Mit der Beendigung des Supports können derartige Lücken nicht mehr geschlossen und damit die Sicherheit nicht mehr garantiert werden. Dies gilt vor allem im Hinblick auf Hacker-Angriffe oder die Infektion des Systems, etwa mit Viren oder Schadprogrammen. Zwar werden von bestimmten Nutzergruppen inoffizielle Systemaktualisierungen, insbesondere weitere „Service Packs“ und Sicherheitsupdates, öffentlich zugänglich gemacht. Hierbei besteht aber keine Unterstützung von Seiten Microsofts. Demgemäß bergen diese Aktualisierungen als solche schon die Gefahr einer Infektion mit Schadprogrammen oder Viren.

II. Forderung des Berliner Datenschutzbeauftragten

Auch in der Berliner Verwaltung konnten die PCs mit Windows XP nicht rechtzeitig ausgetauscht bzw. aktualisiert werden. Aus diesem Grund musste seitens des IT-Dienstleistungszentrums Berlin (ITDZ) ein verlängerter Support mit Microsoft vereinbart werden, der mehrere hunderttausend Euro verschlungen hat. Jedoch ist selbst dieser Support im April 2015 ausgelaufen. Die Anzahl der betroffenen PCs lag zum damaligen Zeitpunkt im unteren fünfstelligen Bereich. Zwar verwies die Berliner Innenbehörde auf die dezentrale Organisation des IT-Einsatzes in der Berliner Verwaltung, sodass die notwendige Aktualisierung von Hard- und Software aufgrund der Organisations- und Verantwortungsstruktur im Aufgaben- und Verantwortungsbereich der jeweiligen Senats- bzw. Bezirksverwaltung stehe. Dies änderte aber nichts an dem Umstand, dass Handlungsbedarf bestand und nach wie vor besteht.

Nach Ansicht des Berliner Datenschutzbeauftragten seien die persönlichen Daten der Bürger einem unverantwortlichen Risiko möglicher Hacker-Angriffe ausgesetzt. Dementspre-

chend ging seine Forderung so weit, in der Berliner Verwaltung alle PCs abzuschalten, die mit dem Betriebssystem Windows XP ausgestattet waren. Es ist jedoch anzumerken, dass inzwischen eine Vielzahl der betagten PCs mit neuen Betriebssystemen ausgestattet worden sein sollen.

Rechtlicher Hintergrund dieser Forderung ist die Aufsichtsfunktion der Bundes-/Landesdatenschutzbeauftragten. Sofern der Bundesbeauftragte für den Datenschutz einen Verstoß gegen die Vorschriften des Bundesdatenschutzgesetzes (BDSG) oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten bzw. die jeweiligen Landesdatenschutzbeauftragten einen solchen gegen das entsprechende Landesdatenschutzgesetz feststellen, findet eine Beanstandung bei den in der jeweiligen Norm genau aufgeführten Stellen statt und diese werden gleichzeitig zur Stellungnahme aufgefordert (vgl. § 25 Abs. 1 BDSG sowie die entsprechenden Vorschriften der Landesdatenschutzgesetze). Dabei kann aber auch von einer Beanstandung abgesehen oder auf eine Stellungnahme der betroffenen Stelle verzichtet werden, insbesondere dann, wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt (vgl. § 25 Abs. 2 BDSG sowie die entsprechenden Vorschriften der Landesdatenschutzgesetze). Außerdem soll die Stellungnahme der betroffenen Stelle auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung des Bundesbeauftragten getroffen worden sind (vgl. § 25 Abs. 3 BDSG sowie die entsprechenden Vorschriften der Landesdatenschutzgesetze). Einige Landesdatenschutzgesetze sehen zusätzlich noch die Möglichkeit vor, dass der Landesbeauftragte für Datenschutz mit der Beanstandung auch Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden kann.

III. Fazit und Auswirkungen für die Hochschulen

Viele Hochschulen haben schon auf neuere Betriebssysteme umgestellt, sodass sich das Szenario aus der Berliner Verwaltung hier nicht wiederholen wird. Sofern aber noch PCs mit dem Betriebssystem Windows XP in Betrieb sind, sollte aus Gründen der Sicherheit sowie im Hinblick auf eine mögliche Verfügung der Datenschutzaufsicht dieser Umstand umgehend geändert und die betagten PCs ausgetauscht oder aktualisiert werden. Zwar kann der jeweils zuständige Landesdatenschutzbeauftragte im Falle von unerheblichen oder bereits beseitigten Mängeln von einer Beanstandung absehen. Nichtsdestotrotz besteht mit Hinblick auf den Schutz der Nutzer- sowie Hochschuldaten Handlungsbedarf beim Betrieb von PCs mit veralteten Betriebssystemen, für die seitens des Herstellers kein Support mehr angeboten wird.

Letztlich können die Vorkommnisse in Berlin als mahnendes Beispiel gesehen werden. Die Rechenzentren der Hochschulen sollten dementsprechend ihr IT-Management derart ausgestalten, dass angekündigte Supportlücken seitens der Hersteller nicht unbeachtet bleiben und somit stets bestmöglicher Schutz gewährleistet werden kann. Durch eine gute und vorausschauende Managementplattform können die Gefahren von Infektionen minimiert sowie ein mögliches Einschreiten der Aufsichtsbehörden verhindert werden. Dass dies in Zeiten knapper Kassen häufig nicht leicht umzusetzen ist, kann insofern nicht als Rechtfertigung gewertet werden.

Second Hand Software im Paket

Bundesgerichtshof geht weiteren Schritt zur Liberalisierung des Handels mit „Gebrauchtsoftware“

von Clara Ochsenfeld

Mit der Frage der Zulässigkeit des Handels mit sogenannten „Gebrauchtlizenzen“ von Software haben sich die Gerichte in der Vergangenheit bereits mehrfach befassen müssen (vgl. Försterling in DFN-Infobrief Recht 5/2012, S. 8 ff.). In einem Urteil des Bundesgerichtshofs (BGH) vom 11. Dezember 2014, dessen Begründung seit dem 16. Juni 2015 vorliegt (BGH, I ZR 8/13 - UsedSoft III), führt der BGH seine bisherige Rechtsprechung fort und erweitert die Voraussetzung zugunsten eines wirksamen Erwerbs gebrauchter Software. Er bejaht eine Erschöpfung des Verbreitungsrechts nunmehr nicht nur hinsichtlich der heruntergeladenen Kopie des Ersterwerbers, sondern darüber hinaus – und das war bislang ungeklärt – auch hinsichtlich derjenigen Kopie, die der Ersterwerber selbst zum Zwecke der Weitergabe an einen Zweiterwerber anfertigt. Die Entscheidung öffnet damit dem Gebrauchtsoftwarehandel die Türen für die Aufspaltung sog. Volumenlizenzen – dies sind Lizenzen, die als gebündeltes Paket veräußert werden und die die Nutzung einer bestimmten Anzahl eigenständiger Kopien des Computerprogramms erlauben.

Einordnung der Problematik

Das deutsche und europäische Recht schützt die Erfinder und Hersteller von Computerprogrammen grundsätzlich dahingehend, dass dem Rechtsinhaber gem. § 69c Nr. 3 S. 1 Urheberrechtsgesetz (UrhG) das ausschließliche Recht der Verbreitung und Vervielfältigung seines Computerprogramms zusteht. Der Schutz findet jedoch seine Grenzen, wenn ein Vervielfältigungsstück des Programmes mit Zustimmung des Rechtsinhabers im Gebiet der Europäischen Union […] im Wege der Veräußerung in den Verkehr gebracht worden ist (sog. Erschöpfungsgrundsatz). In diesem Fall erschöpft sich gem. § 69c Nr. 3 S. 2 UrhG das Verbreitungsrecht in Bezug auf dieses Vervielfältigungsstück. Das bedeutet, dass in diesem Fall der urheberrechtliche Schutz zugunsten eines der Allgemeinheit dienenden freien Warenverkehrs zurücktreten muss, soweit der Rechtsinhaber eine entsprechende Vergütung für das Vervielfältigungsstück erhalten hat. Sinn und Zweck dieser Regelung ist es demnach, die Verbreitung rechtmäßig veräußerter Werkstücke zu erleichtern, diese nicht durch daran fortbestehende Rechte zu beschränken und letztlich klare und übersichtliche Verhältnisse im Rechtsverkehr zu schaffen. Die Wirkung der Erschöpfung entfaltet sich grundsätzlich gegenüber jedermann und führt dazu, dass die in Verkehr gebrachten Werkstücke im Interesse der Verwerter und der Allgemeinheit an einem freien Warenverkehr für jede Weiterverbreitung frei werden.

Durch die Rechtsprechung des EuGH (Urteil vom 03.07.2012 – C-128/11 – Oracle/UsedSoft) und anschließend des BGH (Urteil vom 17.07.2013 - I ZR 129/08 - UsedSoft II) war die grundsätzliche Problematik der sog. „Onlineerschöpfung“ gebrauchter Software bereits gelöst worden (vgl. Försterling in DFN-Infobrief Recht 5/2012 S. 8 ff.). Der EuGH stellte in seiner Entscheidung die Online-Übermittlung (z. B. durch einen Download) der körperlichen Weitergabe (z. B. auf einem Datenträger) unter der Voraussetzung gleich, dass dem Ersterwerber ein unbegrenztes Nutzungsrecht eingeräumt wurde und dieser seine eigene Programmkopie löscht. Die Löschung der eigenen Programmkopie ist insoweit erforderlich, als die sog. „Online-Erschöpfung“ gerade nicht dazu führen soll, dass sich die Anzahl der berechtigten Nutzer erhöht, sondern lediglich sichergestellt werden soll, dass ebenso wie im analogen Bereich die Verkehrsfähigkeit und damit die Weitergabe eines geschützten Werkes ermöglicht wird. Lediglich am Rande

ging der BGH hier auf die Frage ein, wann ein ausreichender Nachweis für das Löschen der eigenen Programmkopie vorliegt und ließ sie letztlich offen. Allerdings ließ er durchdringen, dass eine notarielle Bestätigung über die Erklärung des Ersterwerbers darüber, die Kopien entfernt zu haben, nicht genüge.

Bislang durch die höchstrichterliche Rechtsprechung noch ungeklärt war die Frage, ob das Verbreitungsrecht sich auch hinsichtlich einer Zweitkopie, also einer Kopie, die durch den Ersterwerber für den Zweiterwerber angefertigt wird, erschöpft. Dies hat der BGH mit seiner Entscheidung nun bejaht und damit den Weg für den Handel mit Gebrauchtsoftware, die durch den Ersterwerber im Rahmen von Volumenlizenzverträgen erworben wurde, geebnet.

Sachverhalt der Entscheidung

In dem der Entscheidung zugrundeliegenden Sachverhalt erwarb eine Bildungseinrichtung 40 zeitlich unbegrenzte Softwarelizenzen von einem Softwareunternehmen, welches die ausschließlichen urheberrechtlichen Nutzungsrechte an der veräußerten Software hält. Die Einrichtung erhielt die Software aufgrund der Teilnahme an einem Vertragslizenzprogramm für Bildungseinrichtungen vom veräußernden Unternehmen zu vergünstigten Konditionen. Eine Vertragsklausel bestimmte, dass die erworbenen Lizenzen nicht übertragbar sind und ausschließlich zum Zweck der internen Verteilung innerhalb der Bildungseinrichtung genutzt werden dürfen. Die Bildungseinrichtung erhielt das für die Installation der Software notwendige sog. Enduser-License-Agreement (EULA) sowie eine Seriennummer, mittels derer sie sich die entsprechende Software im Internet vom Kundenportal des Herstellers herunterlud und auf Installationsdatenträgern (sog. „Media-Kit-Datenträgern“) speicherte. Im Anschluss an den Erwerb veräußerte die Einrichtung die Software – ohne diese zuvor auf ihren Rechnern installiert zu haben – dann zu einem höheren Preis an einen Händler für sog. „Gebrauchtsoftware“, der zwei der Lizenzen nebst einem Media-Kit-Datenträger mit dem darauf gespeicherten EULA seinerseits an einen Dritten weiterveräußerte. Das Softwareunternehmen sah in der Weiterveräußerung eine Verletzung seines urheberrechtlichen Verbreitungsrechts und verklagte den Händler für Gebrauchtsoftware auf Unterlassung und Schadensersatz.

Entscheidung des BGH

Der BGH hat die Revision des Softwareunternehmens als unbegründet zurückgewiesen. Begründet wurde dies damit, dass das klagende Softwareunternehmen dem Herunterladen einer Kopie des Computerprogramms zugestimmt hatte und der erwerbenden Bildungseinrichtung 40 Lizenzen einräumte. Somit gestattete es die Herstellung von insgesamt 40 einzelnen Kopien zur Installation an 40 eigenständigen Arbeitsplätzen. Die Zustimmung des klagenden Softwareunternehmens belief sich somit nicht nur auf das Herunterladen einer Kopie der Computerprogramme, sondern erstreckte sich auch darauf, 40 eigenständige Kopien herzustellen. Der BGH bejaht eine Erschöpfung nunmehr auch hinsichtlich dieser weiteren vom Ersterwerber angefertigten Kopien. Dies begründet er vornehmlich damit, dass eine wirtschaftliche Betrachtungsweise, aufgrund der aufgestellten Grundsätze des EuGH zur Online-Erschöpfung, geboten sei. Der BGH geht davon aus, dass der Fall, indem der Rechtsinhaber dem Herunterladen des Computerprogramms und der Anfertigung einer weiteren Kopie zustimmt, hinsichtlich der Erschöpfung des Verbreitungsrechts nicht anders zu beurteilen sei als der Fall, dass der Rechtsinhaber der Veräußerung in einer entsprechenden Anzahl körperlichen Datenträger zustimmt. Die Erschöpfung trete unabhängig davon ein, dass sich das Softwareunternehmen nur mit einer Nutzung des Programms durch Bildungseinrichtungen einverstanden erklärt hat. Der Erschöpfungsgrundsatz könne nicht vertraglich abbedungen werden, sodass sich das Softwareunternehmen gerade nicht auf eine vertragliche Vereinbarung mit dem Ersterwerber berufen könne, die die Zustimmung der Nutzung durch Bildungseinrichtungen begrenzt. Der weitere Vertrieb eines Werkstücks, das mit Zustimmung des Rechteinhabers im Wege der Veräußerung in den Verkehr gebracht wurde, ist vom Berechtigten im Anschluss laut BGH nämlich nicht mehr kontrollierbar. Eine wirksame Beschränkung gegenüber dem Ersterwerber wirke demnach nicht dahingehend, dass auch der weitere Vertrieb auf diese Beschränkung hin überprüft werden könne.

Das klagende Softwareunternehmen konnte darüber hinaus nicht mit dem Argument durchdringen, das durch die Bildungseinrichtung gezahlte Entgelt für die Softwarelizenzen sei allein zur Nutzung nichtkommerzieller Zwecke angemessen gewesen. Denn bereits der EuGH hatte in seiner Entscheidung festgelegt, dass es grundsätzlich ausreicht, wenn der Rechtsinhaber die Möglichkeit hatte beim Erstverkauf der betreffenden Kopie eine angemessene Vergütung zu erzielen. Das

Softwareunternehmen habe hier die Möglichkeit gehabt, die Zustimmung zum Herunterladen der Kopie von der Zahlung eines Entgeltes abhängig zu machen und eine angemessene Vergütung zu erzielen. Es komme demnach nicht darauf an, ob dieses Entgelt lediglich unter der Voraussetzung einer beschränkten Nutzergruppe für angemessen gehalten wurde.
Der BGH hat in seiner Entscheidung jedoch darüber hinaus klargestellt, dass eine Aufspaltung nur dann möglich ist, wenn es sich um sog. Volumenlizenzen über Einzelplatzsoftware handelt und die Kopien in entsprechender Anzahl der Veräußerung beim Ersterwerber unbrauchbar gemacht wurden. Bei den einzelnen Lizenzen handele es sich demnach um eigenständige Nutzungsrechte, die eigenständig übertragen werden können. Dies gilt jedoch nicht im Falle sog. Client-Server-Lizenzen, also Software, die auf einem Server gespeichert wird und die Nutzung des Programms durch mehrere Personen gestattet wird, ohne dass einzelne Kopien angefertigt werden. In diesem Fall liegt die Voraussetzung der Löschung insofern nicht vor, als diese nach wie vor auf dem Server des Ersterwerbers liegt. Der Nacherwerber kann sich folglich nur dann auf den Erschöpfungsgrundsatz berufen, wenn die Kopien in entsprechender Anzahl seines Erwerbs beim Ersterwerber unbrauchbar gemacht wurden.

Fazit und Hinweise für die Hochschulen

Für die Hochschulen und Bildungseinrichtungen kann die Entscheidung des BGH sowohl positive als auch negative Auswirkungen hervorrufen. Positiv insoweit, als die weitere Öffnung eines Gebrauchtmarktes für Software auch ihnen die Möglichkeit gibt, Software vergünstigt aus zweiter Hand zu beziehen. Hierbei sollte jedoch beachtet werden, dass die Anforderungen an die Darlegungs- und Beweislast des Zweiterwerbers, der sich auf die Löschung der Kopie beim Ersterwerber beruft, noch nicht abschließend geklärt sind. Im Falle des Erwerbes von Gebrauchtsoftware sollten die Hochschulen demnach insbesondere auf geeignete Nachweise bezüglich des Entfernens der jeweiligen Kopien beim Ersterwerber achten und insoweit ihre Rechtsabteilung in den Erwerbsvorgang miteinbeziehen. Negative Auswirkung kann die Entscheidung insoweit haben, als die Softwareunternehmen die finanzielle Begünstigung und Gewährung von Rabatten beim Erwerb von Volumenlizenzen in Zukunft einschränken könnten, da für sie nicht gewährleistet werden kann, dass die Software nur für die vereinbarten Zwecke von einem bestimmten Nutzerkreis verwendet wird.

Darüber hinaus ist insbesondere bei der Veräußerung von Software durch die Hochschulen und Forschungsinstitute an einen Gebrauchthändler äußerste Vorsicht geboten. Bei der Veräußerung von Software ist nämlich stets zwischen der schuldrechtlichen und urheberrechtlichen Ebene zu unterscheiden. Schuldrechtliche Absprachen bestehen und wirken grundsätzlich nur zwischen den jeweiligen Vertragsparteien. Das Urheberrecht hingegen beinhaltet dingliche Rechte, die gegenüber jedermann wirken. Das dargestellte Urteil betrifft nur das Verhältnis Softwarehersteller (bzw. Rechtsinhaber) und Zweiterwerber (Gebrauchtsoftwarehändler). Zu unterscheiden ist demnach das Verhältnis zwischen Softwarehersteller und Ersterwerber. Die Softwareüberlassungsverträge zwischen Hersteller und Ersterwerber enthalten nämlich oftmals schuldrechtliche Klauseln, die einer Weiterveräußerung an Dritte entgegenstehen und Schadensersatz- sowie Unterlassungsansprüche des Softwareunternehmens nach sich ziehen können, soweit sie Wirksamkeit entfalten. Im Falle einer Veräußerung der Software ist demnach ebenfalls immer die Rechtsabteilung der Institution miteinzubeziehen, die die entsprechenden Klauseln genau prüfen kann.

Drum prüfe, wer im Netz was findet …

Bundesgerichtshof zur Verjährungsfrist von Ansprüchen aus unerlaubter Online-Nutzung urheberrechtlich geschützter Werke

von Jan Heuer

Mit seiner Entscheidung vom 15.01.2015 (Az.: I ZR 148/13) hat der Bundesgerichtshof (BGH) zur Frage der Dauer der Verjährungsfrist bei unerlaubter Online-Nutzung urheberrechtlich geschützter Werke Stellung bezogen. Ansprüche aus unerlaubter Online-Nutzung auf Zahlung einer fiktiven Lizenzgebühr unterliegen danach einer 10-jährigen Verjährungsfrist. Um den Beginn der Verjährungsfrist bestimmen zu können, sind rechtsverletzende Dauerhandlungen gedanklich in Einzelhandlungen aufzuspalten. Für diese Einzelhandlungen läuft jeweils eine gesonderte Verjährungsfrist.

I. Hintergrund

Das Betreiben eigener Websites und die Zurverfügungstellung urheberrechtlich relevanter Inhalte sind in- und außerhalb des Hochschulbereichs zum täglichen Geschäft geworden. Auf vielen Websites werden Eigen- und Fremdinhalte verbreitet und der Öffentlichkeit zugänglich gemacht. Jedoch besteht für jeden Urheber ein besonderes Interesse daran, diese Verbreitung bzw. Nutzung der von ihm geschaffenen Werke zu kontrollieren. Soweit keine Nutzungsrechte (§ 31 Urheberrechtsgesetz (UrhG)) eingeräumt worden sind und auch keine besondere gesetzliche Erlaubnis (sog. Schrankenregelung) eingreift, ist die Verwendung solcher Werke nicht zulässig. Als Gegenleistung für die Einräumung von Nutzungsrechten besteht ein Anspruch des Urhebers auf eine angemessene Vergütung. Werden die Inhalte ohne bestehendes Nutzungsrecht oder gesetzliche Erlaubnis verwendet, besteht zum einen ein Anspruch des Urhebers auf Unterlassung (§ 97 Abs. 1 UrhG), zum anderen ein Anspruch auf Schadensersatz (§ 97 Abs. 2 UrhG), wenn die urheberrechtsverletzende Nutzung vorsätzlich oder fahrlässig erfolgte.

Betreibt man eine Website, so kann es dazu kommen, dass eigene Ansprüche aus unerlaubter Online-Nutzung urheberrechtlich geschützter Werke bestehen, wenn andere Personen eigene Werke von der Seite übernehmen und diese der Öffentlichkeit zugänglich machen. In gleicher Weise kann man sich aber auch selbst solchen Ansprüchen ausgesetzt sehen, wenn man Werke von fremden Seiten übernimmt.

Sind Ansprüche gegen eine Partei entstanden, können diese zeitlich nicht unbegrenzt geltend gemacht werden. Unter dem Gesichtspunkt von Rechtssicherheit und Rechtsfrieden, kann nach Ablauf der Verjährungsfrist ein Anspruch nicht mehr durchgesetzt werden. Die deshalb fehlende Durchsetzbarkeit des Anspruchs muss indes vom Anspruchsgegner geltend gemacht werden (sog. Einrede). Das heißt, dass die Verjährung eines Anspruchs nur dann berücksichtigt wird, wenn der Anspruchsgegner geltend macht, dass dem Anspruch die Verjährung entgegensteht.

II. Das Urteil des BGH

Im vom BGH zu entscheidenden Fall stritten die Parteien um das Bestehen bzw. die mögliche Verjährung von Schadensersatzansprüchen aus der unerlaubten Nutzung urheberrechtlich geschützter Fotografien.

Sachverhalt

Der Beklagte betrieb bis zum Jahr 2008 einen Handel mit Motorradteilen und hatte dazu Fotografien dieser Teile auf seiner Internetseite in den Jahren 2006, 2007 und 2008 eingestellt.

An den Fotografien bestanden Urheberrechte des Klägers, der den Beklagten wegen der unerlaubten Verwendung seiner

Fotos auf Schadensersatz in Anspruch nahm. Im Januar 2012 wurde Klage beim zuständigen Landgericht eingereicht und der Kläger begründete seinen Anspruch in Höhe von 184.440 € wie folgt:
Der Beklagte habe 106 Fotos ohne Nutzungsberechtigung und unter Verletzung der Pflicht zur Urheberbenennung auf seiner Internetseite in der Zeit von 2006 bis 2008 eingestellt (ein tatsächlicher Nachweis für die Nutzung wurde im weiteren Verlauf jedoch nur für die Jahre 2006 und 2007 dargelegt). Als Schadensersatz sei als angemessene Vergütung eine fiktive Lizenzgebühr geschuldet. Die Verletzung des Rechts auf Anerkennung der Urheberschaft durch das Unterlassen der Urheberbezeichnung rechtfertige darüber hinaus einen pauschalen Aufschlag von 100 % auf die übliche Vergütung (fiktive Lizenzgebühr).
Der Beklagte trat der Klage entgegen und erhob die Einrede der Verjährung. Darauf bezugnehmend hat das Landgericht die Klage abgewiesen und auch die Berufung beim Oberlandesgericht blieb ohne Erfolg.
Im Zuge der Revision gab der BGH aber dem Kläger nun zum Teil Recht und verurteilte den Beklagten zu einer anteiligen Zahlung eines Schadensersatzes in Höhe von 122.960 €.

Verjährung des Anspruchs

Im Fokus stand die besondere Regelung der Verjährung urheberrechtlicher Schadensersatzansprüche. Entscheidend für die Frage, ob ein Anspruch verjährt ist, ist neben der Länge der Verjährungsfrist die Frage ihres Beginns. Dabei ist für Urheberrechtsverletzungen zu beachten, dass diese als Dauerhandlungen eingestuft werden können. Dies war vorliegend das unbefugte, längere Zeit andauernde Zugänglichmachen von Fotografien im Internet. Eine solche an sich andauernde Verletzungshandlung ist laut BGH gedanklich in Einzelhandlungen (also in Tage) aufzuspalten. Insofern ergibt sich jeweils ein separater Beginn der Verjährung und daraus folgend auch eine separate Verjährungsfrist für jede gedankliche Einzelhandlung.
Für den Verjährungsbeginn ist neben dem Zeitpunkt der Handlung, die den Anspruch begründet (hier das Einstellen der Fotos), die Kenntnis des Klägers von dieser Handlung maßgeblich (§ 199 Abs. 1 Bürgerliches Gesetzbuch (BGB)). Der Lauf der Verjährungsfrist beginnt am Ende des Jahres, in dem der Anspruch entstanden ist und der Kläger von den Umständen Kenntnis erlangt hat, die den Anspruch begründen. Bei der Frage, wie lange diese Frist läuft, ist bei Ansprüchen aus Urheberrechtsverletzungen zu differenzieren:
Vom BGH wurde insoweit festgehalten, dass für die Ansprüche aus einer Urheberrechtsverletzung grundsätzlich die regelmäßige Verjährungsfrist von 3 Jahren gilt (§ 102 Satz 1 UrhG).
Daneben ist vom BGH aber die Regelung des § 102 Satz 2 UrhG besonders betont worden. Nach § 102 Satz 2 UrhG ist § 852 BGB unter bestimmten Voraussetzungen auch auf Ansprüche aus Urheberrechtsverletzungen anzuwenden. Nach der Regelung des § 852 BGB kann, obwohl der Schadensersatzanspruch des Opfers einer unerlaubten Handlung verjährt ist, das, was der Schädiger durch die unerlaubte Handlung erlangt hat herausverlangt werden. Insofern sollen dem Schädiger, der Schadensersatzansprüchen nicht mehr ausgesetzt ist, die Vorteile seines rechtswidrigen Verhaltens nicht erhalten bleiben. Auf Ansprüche aus Urheberrechtsverletzungen findet die Rechtsfolge dieser Vorschrift dann Anwendung, wenn der Verpflichtete (also der Rechtsverletzer) durch diese Urheberrechtsverletzung etwas auf Kosten des Berechtigten (grundsätzlich des Urhebers selbst) erlangt hat. Für diesen Anspruch (sog. „Restschadensersatzanspruch“) gilt eine 10-jährige Verjährungsfrist.
Der Verpflichtete – also der Schädiger – hat im zugrundeliegenden Fall durch das Einstellen der Fotografien ins Internet in das Urheberrecht (hier das Recht der öffentlichen Zugänglichmachung) des Klägers eingegriffen. Durch die fehlende Urheberbenennung wurde auch dessen Recht auf Anerkennung der Urheberschaft berührt. Er hat also den Gebrauch der Fotografien mangels eigener Nutzungsrechte ohne rechtlichen Grund auf Kosten des Antragstellers erlangt. Nach ständiger Rechtsprechung des BGH besteht der Gegenwert für den Gebrauch des Urheberrechts in einer angemessenen Lizenzgebühr. Der Vermögensvorteil des Verletzers, also das was er als Folge seines rechtswidrigen Verhaltens erlangt hat, liegt dabei im Gebrauchsvorteil, z. B. einem Werbe- oder Illustrationseffekt. Er hat also die Nutzung der Fotografien ohne Nutzungsrecht erhalten. Deshalb besteht nach den Grundsätzen des Bereicherungsrechts, auf die § 852 BGB verweist, ein Anspruch darauf, dass dieser Gebrauchsvorteil herausgegeben wird, was durch Zahlung einer fiktiven Lizenzgebühr erfolgt. Eben dieser Anspruch des Klägers verjährt aber erst – so der BGH – in 10 Jahren.
Hat der Verletzer also durch die unerlaubte Verwendung urheberrechtlich geschützter Werke einen Gebrauchsvorteil erlangt, gilt eine Verjährungsfrist von 10 Jahren für Ansprüche auf Ausgleich dieses Vorteils. Geht es dagegen um einen Anspruch, bei dem eine Vorteilserlangung nicht relevant ist

(z. B. Anspruch auf Beseitigung, Unterlassung, Vernichtung), gilt die regelmäßige Verjährungsfrist von 3 Jahren. Vorliegend war der Anspruch des Klägers nicht verjährt, denn mit der Klageerhebung im Januar 2012 war ein Ablauf der 10-jährigen Verjährungsfrist nicht gegeben.

Höhe des Anspruchs

Neben der Frage, ob Verjährung eingetreten war, galt es für den BGH festzustellen, wie hoch der Schadensersatzanspruch des Klägers war. Unproblematisch war ein Schaden in Höhe einer fiktiven Lizenzgebühr entstanden (s.o.). Diese wäre in jedem Fall für die Nutzung der Lichtbilder zu entrichten gewesen. Der Kläger verlangte jedoch daneben für die fehlende Nennung als Urheber Schadensersatz.

Ein solcher steht dem Urheber bei fehlender Nennung grundsätzlich zu (§ 97 UrhG). Als Vermögensschaden kann dieser dann geltend gemacht werden, wenn dem Betroffenen durch die fehlende Nennung z. B. Folgeaufträge entgehen. Die entsprechende Forderung des Klägers wurde vom BGH – auch der Höhe in Form eines 100% Aufschlages nach – nicht beanstandet.

Jedoch sahen die Richter im vorliegenden Fall die Höhe des gesamten Schadens anders als der Kläger. Dieser stützte seine Berechnung auf die Urheberrechtsverletzungen in den Jahren 2006, 2007 und 2008. Indes hatte er den konkreten Nachweis dafür, dass der Beklagte das in Rede stehende Urheberrecht verletzt hat, nur für die Jahre 2006 und 2007 erbracht. Deshalb wurde dem Kläger ein anteiliger Betrag in Höhe von 122.960 € nebst Zinsen als Schadensersatz nur für die in den Jahren 2006 und 2007 erfolgten Urheberrechtsverletzungen zugesprochen.

III. Fazit und Konsequenzen für die Hochschulpraxis

Wie oben bereits festgehalten, sind Hochschulen in der Praxis durch ihren Online-Auftritt in Bezug auf die Verletzung von Urheberrechten besonders gefährdet. Jedoch können Hochschulen auf beiden Seiten der urheberrechtlichen Verletzung stehen. Gerade die Nutzung von urheberrechtlich geschützten Lichtbildern für den eigenen Webauftritt oder für die Nutzung von Broschüren birgt das Risiko, sich schadensersatzpflichtig zu machen. Andererseits können auch Werke, an denen Urheberrechte der Hochschulen bestehen, von Dritten ohne die notwendige Einräumung von Nutzungsrechten verwendet werden. Entscheidend sind im Ergebnis zwei Punkte:

Die Verjährung von Schadensersatzansprüchen, die darauf beruhen, dass urheberrechtlich geschützte Werke ohne Berechtigung genutzt werden, liegt, der Entscheidung folgend, grundsätzlich bei 10 Jahren. Damit ist sowohl der längere Schutz des Berechtigten – dem Opfer der Urheberrechtsverletzung – gesichert als auch die Gefahr, für eine solche Verletzung längere Zeit haftbar gemacht zu werden, gegeben. Unter diesem Gesichtspunkt ist in Bezug auf bestehende Urheberrechte gerade – aber nicht ausschließlich – an Lichtbildern erhöhte Aufmerksamkeit geboten. Man denke hier an die Verwendung von im Internet massenhaft kursierenden Bildern. Geht es dagegen um Unterlassungsansprüche, die häufig im Wege der Abmahnung geltend gemacht werden, bleibt es bei der üblichen 3-jährigen Verjährungsfrist.

Dem Urteil ist darüber hinaus etwas grundsätzlich Relevantes zu entnehmen. Der Kläger hat den Nachweis über die in Rede stehende Verletzung zu führen. Er muss also darlegen, welche urheberrechtlich geschützten Werke ohne Einräumung eines Nutzungsrechts zu welchem Zeitpunkt bzw. für welchen Zeitraum und in welcher Form verwendet wurden. Hochschulen, die urheberrechtlich relevante Inhalte zugänglich machen, ist insofern zu einer guten Dokumentation etwaiger Verletzungen durch Dritte (beispielsweise durch Screenshots oder Ausdrucke) zu raten.

Es bleibt festzuhalten, dass die erhöhte Verjährungsfrist aus § 102 Satz 2 UrhG, 852 BGB eine im Verhältnis zur regelmäßigen Verjährungsfrist enorme Verlängerung birgt. Mit der Entscheidung des BGH und der darin liegenden Einordnung urheberrechtlicher Schadensersatzansprüche aus unerlaubter Online-Nutzung werden diese wohl in Zukunft selten durch eine Verjährung „ausgebremst". Insbesondere bei Bildmaterial sollte deshalb zur Sicherheit nur auf selbst gefertigtes oder solches, an dem die eigene Rechtsposition unzweifelhaft ist, zurückgegriffen werden.

Anmerkung:

Zur Verwendung fremder Fotos: Altemark, in: DFN-Infobrief 05/2010

Zu Auskunftsansprüchen bei Urheberrechtsverletzungen: Klein, in: DFN-Infobrief 09/2012

Zur Prüfungspflicht bei der Nutzung fremder Fotos: Overbeck, in: DFN-Infobrief 12/2014

Wer schreibt, der bleibt

Bundesarbeitsgericht verlangt im Arbeitsverhältnis Schriftform für Einwilligungen in Bildnisveröffentlichungen

von Florian Klein

Personenbilder und Imagevideos mit Angestellten gehören seit einiger Zeit zu den gängigen Mitteln der Öffentlichkeitsarbeit nicht nur von Unternehmen, sondern auch von Hochschulen. Sind dabei jedoch einzelne Personen in erkennbarer Weise abgebildet, ist bei jeder Veröffentlichung das Recht am eigenen Bild zu beachten. Dies führt in der Regel dazu, dass die Veröffentlichung der Einwilligung der abgebildeten Person bedarf. Im Hinblick auf die Formerfordernisse, die bei der Einholung einer solchen Einwilligung zu beachten sind, hat das Bundesarbeitsgericht nun mit Urteil vom 11.12.2014 (Az. 8 AZR 1010/13) entschieden, dass eine entsprechende Einwilligung im Arbeitsverhältnis aufgrund der Bedeutung des Rechts auf informationelle Selbstbestimmung der Arbeitnehmer nur wirksam ist, wenn sie schriftlich erteilt wurde. Außerdem äußerte sich das Gericht zu den Anforderungen, die für einen Widerruf der Einwilligung bestehen.

I. Hintergrund

Das Recht am eigenen Bild ist ein besonderes Persönlichkeitsrecht, das jeder natürlichen Person zusteht und sie davor schützt, dass ohne oder gegen ihren Willen Bilder von ihr in die Öffentlichkeit getragen werden. Besondere Bekanntheit erlangt es meistens dann, wenn Prominente gerichtlich gegen die Veröffentlichung von Paparazzi-Fotos in den einschlägigen Zeitungen oder Zeitschriften vorgehen. Dies darf aber nicht darüber hinweg täuschen, dass jedem dieses Recht zusteht. Niedergelegt ist das Recht am eigenen Bild seit dem Jahr 1907 in § 22 Kunsturhebergesetz (KUG), welcher bestimmt, dass Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden dürfen. Diese Norm ist auch für Hochschulen von Relevanz, da es dort im Bereich der Außendarstellung häufig zu Veröffentlichungen von Personenbildern kommt. Dies betrifft nicht nur Konstellationen, in denen der Hochschule durch die Veröffentlichung von Mitarbeiterfotos oder Imagevideos mit Angestellten und Studierenden ein Gesicht gegeben werden soll, sondern auch Vorlesungsaufzeichnungen, in denen Dozenten oder Zuhörer zu sehen sind, und Bilder anderer Veranstaltungen, die Menschen zeigen. Ein geschütztes Bildnis liegt schon dann vor, wenn das äußere Erscheinungsbild einer Person in einer für Dritte erkennbaren Weise wiedergegeben wird, ohne dass es dabei auf eine besondere Form oder ein besonderes Medium der Wiedergabe ankommt. Neben klassischen Foto- oder Videoaufnahmen erfasst dies etwa Zeichnungen, solange die abgebildete Person erkennbar bleibt. Primäres Identifizierungsmerkmal im Rahmen der Erkennbarkeit sind die Gesichtszüge einer Person, allerdings können auch sonstige individuelle Merkmale wie beispielsweise Haarfarbe, Figur, Größe oder Statur im Einzelfall zu einer Erkennbarkeit führen. Die Rechtsprechung lässt es dabei ausreichen, wenn die Erkennbarkeit für einen mehr oder minder großen Bekanntenkreis des Abgebildeten besteht.

Der Einwilligung bedarf nach § 22 KUG allerdings nur die Verbreitung und die öffentliche Zurschaustellung eines Bildnisses. Die Herstellung einer Aufnahme ist dagegen zumindest vom KUG nicht erfasst. Da das Recht am eigenen Bild noch einen verfassungsrechtlichen Kern besitzt, der zudem über die allgemeinen zivilrechtlichen Regelungen abgesichert ist, kann durchaus schon die Herstellung eines Bildnisses rechtswidrig sein, was zum Beispiel häufig bei heimlichen Aufnahmen der Fall ist.

Für eine Verbreitung im Sinne des § 22 KUG kommt es darauf

an, dass eine körperliche Weitergabe des Originals oder von Kopien des Bildnisses erfolgt, die das Risiko einer nicht mehr zu kontrollierenden Kenntnisnahme birgt. Eine Weitergabe in der Öffentlichkeit ist dabei aber nicht erforderlich.

Der Tatbestand der öffentlichen Zurschaustellung erfasst dagegen jede Art der (unkörperlichen) Sichtbarmachung eines Bildnisses, bei der das Publikum keine Verfügungsgewalt darüber erhält. Öffentlich ist die Zurschaustellung, wenn sie gegenüber einer Mehrzahl von Personen (d. h. mindestens 2 Personen) erfolgt, die nicht durch gegenseitige Beziehungen oder durch Beziehung zum Schausteller persönlich untereinander verbunden sind. Klassische Beispiele sind hierfür die Ausstrahlung in einem Film oder im Fernsehen.

Die Veröffentlichung von Mitarbeiterfotos oder Imagevideos im Internet oder auch im Intranet wird in der Regel als öffentliche Zurschaustellung anzusehen sein, sodass die Beschränkungen des Rechts am eigenen Bild zu beachten sind.

Zulässig sind solche Handlungen deshalb nur, wenn eine Einwilligung des Betroffenen vorliegt. Dass diese im Normalfall auch formlos, also beispielsweise mündlich oder durch schlüssiges Verhalten, erteilt werden kann und dass ein Widerruf der Einwilligung nur bei Vorliegen eines wichtigen Grundes und nach Abwägung der widerstreitenden Interessen möglich sein soll, war in Fachkreisen bislang weitgehend anerkannt. Eine detailliertere Darstellung der Fragestellungen rund um Einwilligung, Widerruf und Ausnahmen vom Einwilligungserfordernis mit besonderem Augenmerk auf den Hochschulbereich findet sich bereits in einer früheren Ausgabe des DFN-Infobriefs Recht, weshalb an dieser Stelle ausdrücklich auf diesen Artikel verwiesen werden soll (s. Klein, „Das haben wir auf Band“ in: DFN-Infobrief Recht 3/2015).

Werden Personenbilder ohne die erforderliche Einwilligung veröffentlicht, stellt dies eine Verletzung des Rechts am eigenen Bild dar, die zu Unterlassungs- und Beseitigungsansprüchen des Betroffenen führen kann. Außerdem kann dies gegebenenfalls Schadensersatzansprüche auslösen, die bei schwerwiegenden Persönlichkeitsrechtsverletzungen insbesondere die Zahlung eines Ausgleichs für immaterielle Schäden (sog. Schmerzensgeld) umfassen können. Darüber hinaus ist noch zu beachten, dass die Verletzung des Rechts am eigenen Bild nach dem Kunsturhebergesetz eine Straftat darstellt (§ 33 KUG), die mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe sanktioniert ist. Eine Strafverfolgung kann jedoch ausschließlich auf Antrag des Verletzten erfolgen.

II. Die Entscheidung des Gerichts

Besonders eingängig wurden das Recht am eigenen Bild und seine Auswirkungen im Arbeitsverhältnis kürzlich in einem Urteil des Bundesarbeitsgerichts (BAG) behandelt. Das BAG hatte im Hinblick auf die Veröffentlichung eines Imagefilms eines Unternehmens zu entscheiden, welche Anforderungen an die Einwilligung in eine Bildnisveröffentlichung im Arbeitsverhältnis bestehen und unter welchen Voraussetzungen ein Widerruf erklärt werden kann. Dabei stellte das Gericht nicht nur den Vorrang des KUG vor dem Bundesdatenschutzgesetz (BDSG) fest, sondern statuierte auch ein Schriftformerfordernis für die Einwilligung von Arbeitnehmern.

1. Sachverhalt

Kläger war ein Monteur, der bei der Beklagten, einem Unternehmen für Kälte- und Klimatechnik, seit Juli 2007 angestellt war. Im Oktober 2008 unterschrieb der Kläger zusammen mit ca. 25 Kollegen eine Namensliste, die die Erklärung enthielt, dass Filmaufnahmen von seiner Person zur freien Nutzung im Rahmen der Öffentlichkeitsarbeit der Beklagten verwendet und ausgestrahlt werden dürfen. Daraufhin produzierte das beklagte Unternehmen einen Werbefilm, in dem der Kläger in zwei Sequenzen kurz zu sehen war. Die erste Szene befand sich am Anfang des Videos und zeigte einen vom Kläger gesteuerten Pkw, wobei zwischen den Parteien streitig war, ob der Kläger in dieser Szene überhaupt erkennbar war. In der zweiten beanstandeten Szene am Ende des Videos war dagegen ein Gruppenbild der Angestellten zu sehen, auf dem der Kläger mit ca. 30 Kollegen für knapp 2 Sekunden erkennbar abgebildet war. Nach Abschluss der Produktion wurde dieser Imagefilm von dem beklagten Unternehmen wie geplant im Rahmen eines neuen Internetauftritts online gestellt und konnte fortan über dessen Homepage angeschaut werden, was längere Zeit unbeanstandet blieb. Gut zwei Jahre später, Ende Januar 2011, endete dann das Arbeitsverhältnis zwischen dem Kläger und der Beklagten. Im November 2011 wiederum, nachdem weitere zehn Monate vergangen waren, ließ der klägerische Monteur per Anwaltsschreiben gegenüber dem beklagten Unternehmen erklären, dass er seine „möglicherweise“ erteilte Einwilligung zur Verwendung seiner Bilder widerrufe und verlange, dass das Video bis spätestens zum 08.12.2011 von der Homepage entfernt werde. Nach fruchtlosem Fristablauf reichte er eine Unterlassungsklage beim zuständigen Arbeitsgericht ein, die verbunden war mit der Forderung nach Zahlung eines Schmer-

zensgeldes. Daraufhin löschte die Beklagte das Video Ende Januar 2012 von ihrer Homepage, behielt sich allerdings vor, es in Zukunft wieder dort zu veröffentlichen.

2. Urteil

Nach dem Gang durch die Instanzen landete das Verfahren schließlich beim Bundesarbeitsgericht, welches die Klage im Ganzen für unbegründet hielt und sie deshalb vollumfänglich abwies. Eine Verletzung des Rechts am eigenen Bild des Klägers konnten die Richter nämlich aufgrund der Einwilligung des Klägers nicht erkennen.

Zunächst entschied das BAG, dass sich die Zulässigkeit der Veröffentlichung des Werbefilms nach den §§ 22, 23 KUG richte und nicht nach dem Datenschutzrecht. Dies ist beachtlich, weil Abbildungen von erkennbaren Personen meistens auch als personenbezogene Daten einzustufen sind, für die grundsätzlich das Datenschutzrecht (BDSG bzw. die Landesdatenschutzgesetze) gilt. Insofern wäre gegebenenfalls die Bejahung eines Löschungsanspruchs nach den Vorschriften des BDSG in Betracht gekommen. In welchem Verhältnis BDSG und KUG bei solchen Bildnisveröffentlichungen zueinander stehen, wurde bisher in der Rechtsprechung jedoch kaum erörtert. Vielmehr wurde in der Regel stillschweigend allein das KUG als Maßstab der rechtlichen Beurteilung herangezogen. Da das BDSG und das KUG in ihren Regelungen aber keinesfalls deckungsgleich sind und teilweise sich widersprechende Anforderungen stellen, muss das Verhältnis der beiden Gesetze zueinander geklärt werden.

Das BAG setzte sich nun erstmals höchstrichterlich mit dieser Frage auseinander und stellte fest, dass das KUG als Spezialgesetz für Fragen der Veröffentlichung von Bildnissen vorrangig vor dem BDSG sei. Dabei stützte es sich insbesondere auf § 1 Abs. 3 BDSG, welcher eine Subsidiarität des BDSG vorsieht, soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind. Im Hinblick auf die teilweise strengeren Voraussetzungen der Datenschutzgesetze war das Gericht nur zu dem Zugeständnis bereit, dass die dem Datenschutzrecht zugrunde liegenden Verfassungsgrundsätze bei der Anwendung des KUG zu beachten und zu wahren seien. Dazu gehört vor allem das Recht auf informationelle Selbstbestimmung, welches gewährleistet, dass der Einzelne grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen kann.

Nach Klärung des anzuwendenden Gesetzes stellte das BAG fest, dass der Werbefilm jedenfalls aufgrund des enthaltenen Gruppenfotos ein Bildnis im Sinne des § 22 KUG darstelle. Im Hinblick auf die umstrittene Anfangssequenz wurde dagegen offengelassen, ob eine Erkennbarkeit tatsächlich vorlag, da zumindest eine erkennbare Abbildung bereits vorhanden war, die den Schutzbereich des § 22 KUG eröffnete. Auch die Frage, ob eine Ausnahme des § 23 KUG einschlägig war, welche die Veröffentlichung ohne Einwilligung des Klägers hätte rechtfertigen können, beantwortete das BAG aufgrund der Einwilligung des Klägers nicht.

Im Folgenden erläuterte das BAG dann, warum hier eine Einwilligung vorlag und welche Anforderungen an deren Wirksamkeit zu stellen sind.

Grundsätzlich bestünden für die Einwilligung nach dem KUG keine Formerfordernisse, sodass sie auch formlos oder konkludent erteilt werden könne. Dass darin ein Wertungswiderspruch zum Datenschutzrecht liege, welches ein Schriftformerfordernis für die Einwilligung aufstellt, sei jedoch hinzunehmen, weil das KUG eine bereichsspezifische Spezialregelung darstelle, die insofern Vorrang habe.

Allerdings hielten die Richter eine verfassungskonforme Auslegung des § 22 KUG für erforderlich, in deren Rahmen eine Abwägung zwischen dem Verwendungsinteresse des Arbeitgebers und dem Recht auf informationelle Selbstbestimmung des Arbeitnehmers vorgenommen werden müsse. Aus dieser Abwägung soll sich dann ableiten lassen, ob im konkreten Fall eine Erlaubnis erforderlich ist und in welcher Form diese zu erteilen ist. Da die Ausübung des Rechts auf informationelle Selbstbestimmung im Arbeitsverhältnis von hoher Bedeutung sei, ergebe sich aus der Abwägung, dass die Einwilligung der Arbeitnehmer auch und gerade im Arbeitsverhältnis der Schriftform bedürfe. Denn nur bei einer schriftlichen Einwilligung könne dem Arbeitnehmer hinreichend verdeutlicht werden, dass die Einwilligung zur Veröffentlichung von Bildern nicht zu den arbeitsvertraglichen Verpflichtungen gehört und dass ihre Erteilung oder Verweigerung keine Folgen für das Arbeitsverhältnis haben dürfen.

Hier hatte der Kläger die Namensliste unterschrieben und damit seine Einwilligung erteilt. Diese Erklärung erfolgte anlassbezogen, weil es bei der Liste um ein konkretes Filmprojekt zu Werbezwecken ging, sie wurde im Einzelfall eingeholt, klar bezeichnet und separat von anderen Erklärungen schriftlich abgegeben. Dies erfüllte daher die Anforderungen, die an eine informierte Einwilligung zu stellen sind. Insbesondere handelte es sich auch nicht nur um eine allgemeine Einwilli-

gung in nicht näher bezeichnete Veröffentlichungen, die vorab generalisierend im Arbeitsvertrag erteilt wurde.

Zuletzt setzt eine wirksame Einwilligung voraus, dass sie freiwillig erteilt wurde. Daran könnte man zweifeln, weil der Arbeitnehmer gegenüber dem Arbeitgeber weisungsgebunden ist und dadurch ein Über-/Unterordnungsverhältnis besteht. In dieser Hinsicht positionierte sich das BAG allerdings sehr klar und stellte fest, dass eine freiwillige Erklärung selbst im Arbeitsverhältnis möglich ist, weil ein Arbeitnehmer mit Eingehung des Arbeitsverhältnisses und Eingliederung in einen Betrieb nicht seine Grund- und Persönlichkeitsrechte abgebe.

Auch im konkreten Fall hatte das Gericht keine Zweifel an der Freiwilligkeit der Einwilligung, da keine Anhaltspunkte für besonderen Druck oder Zwang vorlagen. Im Übrigen hatten sechs andere Beschäftigte der Beklagten die Namensliste nicht unterschrieben, wobei bei einem sogar der Abwesenheitsvermerk „Urlaub, Krank oder Schule“ fehlte. Daraus ließ sich schließen, dass dieser Arbeitnehmer schlicht keine Einwilligung erteilen wollte, was ohne arbeitsrechtliche Konsequenzen für ihn blieb.

War damit also geklärt, dass ursprünglich eine wirksame Einwilligung zur Veröffentlichung des Imagevideos bestand, musste sich das BAG noch mit der Frage befassen, ob diese Einwilligung mittlerweile wieder erloschen war. Dazu diskutierte es drei potentielle Erlöschungsgründe.

Zunächst wäre ein Erlöschen der Einwilligung möglich gewesen, wenn sie zeitlich befristet erteilt worden und diese Frist abgelaufen wäre. Insbesondere wäre es zulässig gewesen, seine Einwilligung ausdrücklich auf die Dauer des Arbeitsverhältnisses zu beschränken. Eine solche Beschränkung oder Befristung lag hier jedoch nicht vor.

Danach stellten die Richter fest, dass jedenfalls bei Bildern oder Filmen, die reinen Illustrationszwecken dienen und die keinen spezifischen Bezug zu der individuellen Person des Arbeitnehmers aufweisen, die Einwilligung nicht automatisch mit Beendigung des Arbeitsverhältnisses erlischt. Stattdessen müsste der abgebildete Arbeitnehmer ausdrücklich erklären, dass er an seiner Einwilligung nicht mehr festhalten möchte. Ein solcher automatischer Wegfall der Einwilligung mit Beendigung des Arbeitsverhältnisses war zuvor gelegentlich in der Rechtsprechung angenommen worden, dürfte nun aber als überholt angesehen werden. Dass es sich im konkreten Fall nur um einen Film handelte, der allein Illustrationszwecken diente und nicht von der individuellen Person des Klägers lebte, bejahte das Gericht, weil die beiden beanstandeten Szenen nur allgemein die Arbeitsabläufe im Betrieb der Beklagten darstellen sollten und auch das Gruppenbild nur eine „typische“ Belegschaft abbilden sollte, ohne sich genauer auf die einzelnen Individuen zu beziehen.

Schließlich hatte sich das BAG noch mit einem potentiellen Erlöschen der Einwilligung durch den ausdrücklich per Anwaltsschreiben erklärten Widerruf des Klägers zu beschäftigen. Eine Einwilligung im Sinne des KUG sei weder frei widerruflich noch zwingend unwiderruflich. Vielmehr sei erneut eine Interessenabwägung im Einzelfall erforderlich, um bestimmen zu können, ob die Einwilligung widerrufen werden könne. Dabei müsste auf Seiten des Arbeitgebers nicht nur sein Veröffentlichungsinteresse berücksichtigt werden, sondern vor allem auch sein wirtschaftliches Interesse daran, die entstandenen Produktionskosten für das Imagevideo durch werbliche Verwendung kompensieren zu können. Für den Arbeitnehmer streite dagegen das Recht auf informationelle Selbstbestimmung, welches mit Beendigung des Arbeitsverhältnisses möglicherweise neue Impulse erhalten könne, was aber nicht zwangsläufig der Fall sein müsse. Insofern könne ein Arbeitnehmer grundsätzlich vorbringen, dass sein ehemaliger Arbeitgeber nach seinem Ausscheiden nicht mehr weiter mit Abbildungen von ihm werben soll. Dies stehe allerdings unter der Prämisse, dass die werbliche Verwendung ohne gesonderte Vergütung erfolgte. Darüber hinaus könne der Einwand der Unterlassung einer weiteren werblichen Verwendung nur berücksichtigt werden, wenn speziell mit der Person des Arbeitnehmers oder seiner Funktion im Unternehmen geworben wird. Werde das Bild des Arbeitnehmers dagegen nur für eine allgemeine Darstellung des Unternehmens genutzt, ohne dass die Person des AN besonders hervorgehoben, sein Name genannt oder seine Identität in sonstiger Weise herausgestellt werde und vermittle die Abbildung auch nicht zwingend den Eindruck, es handle sich um die aktuelle Belegschaft, soll dies gerade keine wirtschaftliche und insbesondere persönlichkeitsrelevante Weiterverwertung der Abbildung des Arbeitnehmers darstellen. Da hier ausschließlich eine solche illustrative Verwendung der Abbildung des Klägers vorlag, ohne dass seine individuelle Persönlichkeit für Werbezwecke ausgenutzt wurde, konnte der Kläger diesen Einwand nicht erheben. Dementsprechend konnte er darauf auch keinen Widerruf stützen.

Vielmehr hielt es das BAG in einer solchen Konstellation im Hinblick auf einen Widerruf für erforderlich, dass der Arbeitnehmer einen Grund im Sinne einer plausiblen Erklärung angebe, warum er die Einwilligung jetzt widerrufen wolle,

obwohl er sie früher doch noch erteilt habe. An einer solchen plausiblen Erklärung fehlte es hier, sodass das Gericht den erklärten Widerruf für unwirksam hielt. Dabei berücksichtigte es zusätzlich noch, dass der Widerruf erst zehn Monate nach Beendigung des Arbeitsverhältnisses erklärt wurde, was noch größeren Erklärungsbedarf mit sich brachte.
Im Ergebnis hatte die ursprünglich per Unterschrift auf der Namensliste erteilte Einwilligung Bestand, sodass eine Verletzung des KUG nicht vorlag und die Klage auf Unterlassung und Schmerzensgeld deshalb abzuweisen war.

III. Fazit und Konsequenzen für die Hochschulpraxis

Das Urteil des BAG klärt für die arbeitsrechtliche Praxis und darüber hinaus allgemein einige wichtige Fragen. Zunächst wird im Verhältnis von Datenschutzrecht (BDSG, Landesdatenschutzgesetze) und Recht am eigenen Bild (KUG) ein Vorrang des spezialgesetzlichen Bildnisschutzes des KUG festgelegt. Bei der Beurteilung der Rechtmäßigkeit der Veröffentlichung von Mitarbeiterfotos oder ähnlichem sind deshalb zukünftig nur noch die Maßstäbe des KUG zu beachten. Diese hat das BAG aber jedenfalls für Arbeitsverhältnisse verschärft und fordert aufgrund einer verfassungskonformen Auslegung, dass Einwilligungen von Arbeitnehmern schriftlich erfolgen. Dies wird wohl weitgehend auf den Hochschulbereich übertragen werden können, zumal die Einholung schriftlicher Einwilligungen zuvor schon aus Beweisgründen sinnvoll war. Ob dieses vom BAG aufgestellte Schriftformerfordernis allerdings im Verhältnis zwischen den Studierenden und der Hochschule anzuwenden ist, kann nicht mit Sicherheit prognostiziert werden. Ausgehend von der Argumentation des Gerichts wird man aber im Studierendenverhältnis wohl umso eher ein Schriftformerfordernis aus dem Recht auf informationelle Selbstbestimmung ableiten können, je mehr für den Studierenden in der konkreten Situation eine besondere Abhängigkeit von der Hochschule besteht, da ein solches Abhängigkeitsverhältnis für das Arbeitsverhältnis typisch ist und somit zu einer vergleichbaren Interessenlage führen kann. Entscheidend ist dabei, inwiefern gerade die Schriftform erforderlich ist, um den Studierenden zu vermitteln, dass die Verweigerung oder Erteilung einer Einwilligung zur Bildnisveröffentlichung keinerlei Auswirkungen auf ihr Studium und das Verhalten der Hochschule hat. Dies dürfte vor allem in Prüfungen, Pflichtveranstaltungen oder sonstigen Situationen der Fall sein, in denen die Studierenden auf die Mitwirkung der Hochschule in besonderer Weise angewiesen oder einem besonderen Druck ausgesetzt sind. Im Übrigen können jedoch weiterhin formlose Einwilligungen ausreichend sein, sofern sich aus einer Interessenabwägung nichts anderes ergibt, wobei auch hier schriftliche Einwilligungen aus Beweisgründen stets vorzugswürdig sind.

Wichtig ist zudem die Feststellung, dass Willenserklärungen von Arbeitnehmern durchaus freiwillig sein können. Was zunächst unspektakulär klingt, bringt in der Praxis weitreichende Folgen mit sich, da dadurch das Instrument der Einwilligung auch im Arbeitsverhältnis zur Rechtfertigung von Eingriffen in Rechte der Arbeitnehmer herangezogen werden kann. Hier schafft das Urteil des BAG Rechtssicherheit und gebietet den vielen zweifelnden Ansichten in der juristischen Fachliteratur Schweigen. Trotz der Weisungsgebundenheit und der faktischen Abhängigkeit des Arbeitnehmers vom Arbeitgeber bleiben autonome und freie Entscheidungen möglich. Dies eröffnet neuen Spielraum für Arbeitgeber, der für Hochschulen in vielerlei Hinsicht interessant sein kann, beispielsweise wenn man sich von seinen Angestellten die Befugnis einräumen lassen möchte, E-Mail-Konten, die zumindest zum Teil auch privat genutzt werden, stichprobenartig zu kontrollieren. Unbedingt zu beachten ist aber weiterhin, dass eine freie Entscheidung gerade im Arbeitsverhältnis voraussetzt, dass auf den Arbeitnehmer in keiner Weise Druck oder Zwang ausgeübt wird. Denn nur weil freiwillige Entscheidungen auch von Arbeitnehmern möglich sein sollen, ist dies nicht automatisch immer der Fall. Insofern sollte schon der Anschein vermieden werden, dass der Arbeitnehmer in eine bestimmte Richtung gedrängt wird, selbst wenn das nur durch das mittelbare In-Aussicht-Stellen von Nachteilen erfolgt. Über das Arbeitsverhältnis hinaus wird man diese Aussage wohl auf das Studierendenverhältnis übertragen können, da hier häufig eine deutlich geringere Abhängigkeit besteht als im Arbeitsverhältnis. Insofern können Willenserklärungen von Studierenden ebenfalls das Kriterium der Freiwilligkeit erfüllen.

Zu guter Letzt verdienen die aufschlussreichen Ausführungen des BAG zur Problematik des Erlöschens einer vormals erteilten Einwilligung Beachtung.
Klargestellt ist nunmehr nämlich, dass die Beendigung des Arbeitsverhältnisses – vorbehaltlich spezieller individueller Regelungen – nicht dazu führt, dass eine früher erteilte Einwilligung eines Arbeitnehmers ohne Weiteres, insbesondere ohne ausdrückliche Erklärung des Betroffenen, erlischt. Dies gilt

jedenfalls für solche Abbildungen, auf denen der Betroffene nur zu reinen Illustrationszwecken zu sehen und seine individuelle Person nicht von Belang für die Aussage des Bildes ist. Neben den Beschäftigten der Hochschulen wird man diese Überlegung wohl auch auf Studierende und das Ende ihres Studiums übertragen können, da insofern eine ähnliche Interessenlage besteht.

Beruht die Bedeutung der bildlichen Darstellung einer Person dagegen gerade auf ihrer individuellen Persönlichkeit oder Funktion und verfolgt die Abbildung deshalb nicht nur Illustrationszwecke, ist die Lage weniger eindeutig. Mit diesem Fall musste sich das BAG nicht auseinandersetzen, allerdings wird man hier davon ausgehen können, dass deutlich strengere Maßstäbe angelegt werden müssen, da das Persönlichkeitsrecht des Abgebildeten in dieser Konstellation deutlich stärker betroffen ist. Aus diesem Grund ist eine sorgfältige Auslegung der Einwilligungserklärung unter Berücksichtigung der widerstreitenden Interessen erforderlich, um zu klären, ob die Einwilligung von vornherein darauf angelegt war, die Veröffentlichung nur während der Dauer des Arbeits- bzw. Studierendenverhältnisses oder auch darüber hinaus zu legitimieren.

Geht es um Bildnisse, bei denen die Einwilligung nicht automatisch erlischt, besteht die letzte Möglichkeit zur Beseitigung der Einwilligung nur noch in der Erklärung eines Widerrufs. Auch das BAG sieht allerdings keine unbeschränkte Widerrufsmöglichkeit des Betroffenen, sondern stellt bestimmte Anforderungen. Insofern lässt sich festhalten, dass bei Bildnissen, für die der Betroffene eine gesonderte Vergütung erhalten hat, ein Widerruf auch nach Beendigung des Arbeitsverhältnisses nur in seltenen Ausnahmefällen zulässig sein dürfte. Bei Bildnissen dagegen, die die Person und Persönlichkeit des Abgebildeten ohne Vergütung besonders hervorheben oder ausnutzen, reicht die darin liegende weitere Verwertung der Persönlichkeit zumindest bei einer werblichen Verwendung in der Regel aus, um einen Widerruf eines ausgeschiedenen Mitarbeiters begründen zu können. In solchen Fällen sollte einem ausdrücklich erklärten Löschungsverlangen deshalb im Zweifel stattgegeben werden, sofern nicht auf Seiten der Hochschule im Einzelfall so gewichtige Gründe für eine Beibehaltung der Veröffentlichung vorliegen, dass diese das Persönlichkeitsrecht des Abgebildeten überwiegen.

Schließlich bleiben noch die Bildnisse, die allein Illustrationszwecken dienen. Hier verlangt das BAG eine plausible Erklärung für den Widerruf als gegenläufige Ausübung des Rechts auf informationelle Selbstbestimmung im Vergleich zum Zeitpunkt der früheren Erteilung der Einwilligung. Was genau sich dahinter verbirgt, lässt das Urteil leider offen. Dennoch wird man hier erneut auf das Ergebnis einer Interessenabwägung abstellen können. Gibt der ehemalige Arbeitnehmer eine Erklärung für den Widerruf an, aus der sich ergibt, dass besondere Umstände vorliegen, aufgrund derer sein Persönlichkeitsrecht zusätzliches Gewicht erlangt, kann dies zur Legitimation des Widerrufs ausreichen. Ein willkürlicher und unbegründeter Widerruf kann in dieser Situation dagegen im Regelfall unberücksichtigt bleiben, da er die Bindungswirkung der Einwilligung insoweit nicht erschüttern kann. Tendenziell werden die Anforderungen an die „plausible Erklärung“ aber etwas geringer sein, als dies bei einem „wichtigen Grund“ der Fall ist, sodass die für einen Widerruf zu überwindenden Hürden nach den Maßstäben des BAG niedriger sind als bisher vielfach von der Rechtsprechung angenommen.

Orientieren sich die Hochschulen bei der Veröffentlichung von Fotos und Videos, die Abbildungen von Personen enthalten, an diesen Kategorien, sollte dem Recht am eigenen Bild in hinreichendem Maße Rechnung getragen werden können.

Big Brother „LIKES“ watching you

Landesarbeitsgericht Düsseldorf entscheidet über Mitbestimmungsrecht des Betriebsrats an Facebook-Auftritt des Arbeitgebers

von Hagen Sporleder

Nach einer Entscheidung des Landesarbeitsgerichts (LAG) Düsseldorf stellt der Betrieb einer Facebook-Seite durch einen Arbeitgeber, die die Möglichkeit zum Kommentieren und „Liken“ von Mitarbeiterverhalten durch Dritte bietet, grundsätzlich keine Überwachung durch eine technische Einrichtung im Sinne von § 87 Abs. 1 Ziffer 6 Betriebsverfassungsgesetz (BetrVG) dar. Daher kommt dem Betriebsrat in der Regel kein Mitbestimmungsrecht hinsichtlich des Seitenbetriebs zu. Kritische Kommentare von Facebook-Nutzern verletzen das Persönlichkeitsrecht des betroffenen Mitarbeiters grundsätzlich nicht, soweit sie durch die Meinungsfreiheit gedeckt sind und ihrerseits kommentiert oder nötigenfalls gelöscht werden können.

I. Hintergrund

Bedingt durch ihre weit verbreitete Nutzung ermöglichen Plattformen wie Facebook einem riesigen potentiellen Publikum den Zugriff auf persönliche Daten. Hochgeladene Bilder, Kommentare, Informationen zur eigenen Person, zu Familie und Freunden lassen je nach Freigiebigkeit des Nutzers einen mehr oder weniger genauen Schluss auf dessen Persönlichkeit zu.

Die Daten dürften dabei nicht nur für Unternehmen von Interesse sein, welche die Nutzer als potentielle Kunden und Marktforschungssubjekte sehen. Auch Arbeitgeber können zu den regelmäßigen Besuchern eines Facebook-Profils gehören, da sie sich anhand der Nutzer-Aktivitäten ohne besondere Mühe ein ungeschöntes Bild von Bewerbern und Mitarbeitern machen können.

Dabei bergen die eingestellten Informationen nicht nur für sich genommen mögliche Gefahren beispielsweise für die Reputation des Nutzers. Indem Posts, Angaben und Bilder zeitlich und systematisch geordnet werden, erlauben sie unter Umständen die Erstellung eines relativ exakten Persönlichkeitsprofils, das Auskunft über Leistungsbereitschaft, Gewissenhaftigkeit, Loyalität und Sozialkompetenz einer Person geben kann.

Spätestens dieser Punkt dürfte Arbeitgeber aufmerken lassen. Schließlich wirken sich die aufgezählten Aspekte unmittelbar auf ihr Ansehen, die Zufriedenheit ihrer Kunden und den Betriebsfrieden aus.

Insofern überrascht es wenig, dass Facebook immer wieder Ausgangpunkt für arbeitsgerichtliche Entscheidungen ist. Das Spektrum der Rechtsstreitigkeiten ist groß und geht von geschäftsschädigenden Posts des Arbeitnehmers über Beleidigung von Kollegen und Vorgesetzten bis hin zur Kündigung wegen Veröffentlichung anstößiger Bilder.

Im Gegensatz zu der Problematik, die im Folgenden dargestellt wird, haben die bisher entschiedenen Fälle eine Gemeinsamkeit. Sie gehen von einem aktiven Verhalten des Arbeitnehmers aus, da dieser selbst entscheidet, etwas auf Facebook zu posten, hochzuladen, zu „liken“ oder zu kommentieren.

Fälle, in denen Dritte, etwa Kunden, das Verhalten eines Mitarbeiters kommentieren, sind der Kontrolle des Betroffenen hingegen meistens entzogen. Dennoch kann der Arbeitgeber auch aus diesen Informationen seine Schlüsse insbesondere hinsichtlich der Qualität der Arbeitsleistung und dem Verhalten am Arbeitsplatz ziehen.

II. Entscheidung des LAG Düsseldorf

Ein Arbeitgeber, der mehrere Bluttransfusionszentren betreibt, eröffnete bei Facebook ein Profil, auf welches er bei Blutspendeterminen mittels ausgelegter Flugblätter hinwies.

Zudem informierte er seine Mitarbeiter über das Bestehen des Auftritts und übergab ihnen zugleich einen Leitfaden zum Umgang mit sozialen Medien, in welchem sie unter anderem zu einem stets freundlichen Umgangston angehalten wurden.
Auf der Facebook-Seite konnten unter anderem Spenderpersonen die Kommentarfunktion und die „Like"-Funktion nutzen. Im Verlauf des Seitenbetriebs entstanden jedenfalls zwei Kommentare, die die Professionalität der in den Transfusionszentren arbeitenden Mitarbeiter betrafen. So wurde etwa gepostet, dass eine an einem bestimmten Tag für die Blutentnahme zuständige Mitarbeiterin „noch lernen muss, die Nadel zu setzen".
Die Pflege des Facebook-Auftritts oblag einer Gruppe von zehn Mitarbeitern des Arbeitgebers, welche Informationen einzustellen oder Posts von Spendern zu kommentieren hatten. Jeder dieser Mitarbeiter verfügte über einen individuellen Administratorenzugang, anhand dessen nachvollzogen werden konnte, wann und welcher der zehn Mitarbeiter Eingaben auf der Facebook-Seite vorgenommen hatte. Der Arbeitgeber verfügte zudem über einen allgemeinen Zugang, der diese Möglichkeit nicht bot.
Bedenken mehrerer Mitarbeiter an dem Betrieb des Facebook-Auftritts veranlassten den Betriebsrat dessen gerichtliche Einstellung zu erwirken. Das in erster Instanz zuständige Arbeitsgericht (ArbG) Düsseldorf gab dem Betriebsrat Recht, der seine Mitbestimmungsrechte nach § 87 Abs. 1 Ziffer 6 BetrVG verletzt sah. Danach darf der Arbeitgeber eine technische Einrichtung, die die Leistungen und das Verhalten der Arbeitnehmer überwacht, nur betreiben, wenn der Betriebsrat vor der Inbetriebnahme der Einrichtung sein Mitbestimmungsrecht ausgeübt hat. Der Betriebsrat meint, dass es sich bei der Facebook-Seite um eine solche Überwachungseinrichtung handele.
Erstens sei eine Leistungs- und Verhaltenskontrolle aller Mitarbeiter möglich, die in den Transfusionszentren arbeiten. Diese Mitarbeiter würden durch die Kommentare öffentlich kritisiert, woraus wiederum der Arbeitgeber Schlüsse hinsichtlich der Arbeitsleistung ziehen könne.
Zweitens könne der Arbeitgeber Leistung und Verhalten der zehn Mitarbeiter überwachen, die mit der Pflege der Seite betraut sind, da Facebook deren Log-in-Daten und die Eingabezeitpunkte speichert. Auf diesem Weg konnte tatsächlich nachvollzogen werden, wann und in welcher Form einer der zehn Mitarbeiter beispielsweise auf den Post eines Spenders geantwortet hatte.
Zu der Entscheidung des LAGs Düsseldorf ist anzumerken, dass es in beiden Fällen problematisch ist, dass eine technische Überwachung im Sinne von § 87 Abs. 1 Ziffer 6 BetrVG nur besteht, wenn selbsttätig Informationen aufgezeichnet werden.
Dies trifft aber zumindest auf das Kommentieren und „Liken" gerade nicht zu. Nicht Facebook generiert beispielsweise den erwähnten Kommentar zum „Geschick mit der Nadel", sondern der jeweilige Facebook-Nutzer. Die Datenaufzeichnung geht damit auf menschliches Verhalten zurück und ist demnach nicht selbsttätig erfolgt.
Die Auswirkung der Überwachung durch einen Menschen und der, die von einer technischen Einrichtung ausgeht, sind aber nicht ohne Weiteres vergleichbar.
Eine technische Überwachung ist zum einen oft nicht direkt wahrnehmbar. Zum anderen kann sich der Betroffene ihr auch nicht entziehen. Beides trifft zum Beispiel auf die Aufzeichnung des Fahrverhaltens mittels eines Fahrtenschreibers, nicht aber auf einen mitfahrenden Vorgesetzten zu.
Das Bundesarbeitsgerichts (BAG) sieht nach gefestigter Rechtsprechung in den Fällen technischer Überwachung eine Gefahr für die freie Persönlichkeitsentfaltung des Arbeitnehmers gegeben, wenn er in einen von ihm nicht beeinflussbaren Überwachungsprozess eingebunden wird. Ein nicht überwachter Mitarbeiter verhält sich nämlich anders als einer, dessen Verhalten aufgezeichnet wird.
Das in zweiter Instanz zuständige LAG Düsseldorf lehnt in seinem Beschluss vom 12.01.2015 (Az. 9 TaBV 51/14) ein Mitbestimmungsrecht für die oben beschriebene Konstellation ab.
Nach seiner Entscheidung liegt hinsichtlich der durch Kommentare und „Likes" kritisierten Mitarbeiter gerade keine selbsttätige Datenerfassung vor. Einerseits gäben die Spender in ihren Kommentaren lediglich ihre Beobachtungen wieder, wie sie es auch in einer E-Mail oder einem Brief tun könnten. Andererseits seien die Spender auch nicht vom Arbeitgeber dazu instruiert oder beauftragt worden. Eine Einrichtung zur Überwachung bestünde nur, wenn Facebook selbst Kommentare über die Mitarbeiter posten würde. Das ist aber hinsichtlich der kritisierten Mitarbeiter offensichtlich nicht der Fall.
Auch eine Beeinträchtigung der freien Persönlichkeitsentfaltung erkennt das LAG nicht an. Der Sinn und Zweck des Mitbestimmungsrechts nach § 87 Abs. 1 Ziffer 6 BetrVG, nämlich der Schutz der Persönlichkeit vor anonymer Kontrolle durch technische Aufzeichnungen, wie etwa dem erwähnten Fahrtenschreiber, sei hier nicht berührt. Der jeweilige Mitarbeiter sehe sich nämlich nur dem menschlich kontrollierten Verhalten der Spender gegenüber, die sich im Rahmen ihrer Meinungsfrei-

heit auf der Seite äußern würden.

Anders beurteilte das LAG die Rechtslage hinsichtlich der zehn Mitarbeiter, die den Facebook-Auftritt betreuen. Mittels der insgesamt zehn individuellen Administratorenkennungen konnte nachvollzogen werden, welcher Mitarbeiter wann welche Informationen auf der Seite veröffentlicht hatte. Im Gegensatz zu der oben beschriebenen Problematik erfolgte diese Datenerfassung auch direkt durch Facebook und demnach selbsttätig, wobei sich durch die so gewonnenen Daten ein Rückschluss auf das Arbeitsverhalten des betroffenen Mitarbeiters ziehen ließ. Allerdings hatte der Arbeitgeber die in Rede stehenden zehn Mitarbeiter noch während des laufenden Verfahrens angewiesen, nur noch die allgemeine Administratorkennung und nicht mehr die individuellen Kennungen zu benutzen, so dass eine Identifizierung des Einzelnen nicht mehr ohne Weiteres möglich war. Die Identifizierung des Einzelnen ist aber gerade Voraussetzung für ein Mitbestimmungsrecht nach § 87 Abs. 1 Ziffer 6 BetrVG, da Arbeitnehmer nicht vor einer Überwachung schlechthin, sondern nur vor einer nicht wahrnehmbaren, technischen Überwachung geschützt werden sollen. Diese Gefahr war durch Benutzung ein und derselben allgemeinen Kennung gebannt.

Die Benutzung einer gemeinsamen Kennung eröffnet aber ein anderes Problem. Auch wenn der einzelne Mitarbeiter nicht (mehr) identifizierbar ist, erfasst Facebook dennoch Daten bei der Anmeldung mit der allgemeinen Kennung. Aus diesem Grund können die Mitarbeiter zwar nicht einzeln, aber als Gruppe überwacht werden.

Aus der Überwachung von in der Regel kleinen Gruppen kann sich nach ständiger Rechtsprechung des BAG indes auch ein Mitbestimmungsrecht ergeben. Ist eine Gruppe nämlich gemeinsam für einen bestimmten Leistungserfolg verantwortlich, kann ein Gruppendruck entstehen, der wiederum die Persönlichkeitsentfaltung des einzelnen Gruppenmitglieds beeinträchtigen kann. Bei der Beurteilung, ob dies der Fall ist, spielen die Gruppengröße, die Organisation der Gruppe, die Art der Tätigkeit und der Anpassungszwang innerhalb der Gruppe eine Rolle.

Dies berücksichtigend hat das LAG vorliegend eine Gefährdung der Persönlichkeitsentfaltung des einzelnen Gruppenmitglieds aber dennoch verneint und daher auch ein Mitbestimmungsrecht des Betriebsrats abgelehnt. Die Gruppe sei mit zehn Mitgliedern groß genug, um auch bei urlaubs- oder krankheitsbedingter Abwesenheit einiger Mitglieder keine Rückschlüsse auf die Facebook-Tätigkeit des Einzelnen zuzulassen. Anders wäre dies nur, wenn durch zusätzliche (nicht nur technische) Möglichkeiten eine Identifizierung erfolge könnte. Bei einem Fahrtenschreiber kann etwa anhand einer Einsatzliste nachvollzogen werden, wer welches Fahrzeug benutzt hat, so dass dem jeweiligen Mitarbeiter ein entsprechendes Fahrtenschreiberprotokoll zugeordnet werden kann.

Auch aus der Art der Tätigkeit ergäbe sich keine Gefährdung, da alle zehn Mitarbeiter die Betreuung der Seite nicht als Hauptaufgabe, sondern neben anderen Tätigkeiten ausüben. Bei Zusammenschau der Größe, der Organisation und der Art der Tätigkeit, seien somit vorliegend auch keine Anpassungszwänge gegeben.

Anders wäre dies zum Beispiel, so das Gericht, bei einer Gruppe von sechs Mitgliedern, die im Akkord arbeiten. Hier wäre nämlich der einzelne Mitarbeiter gezwungen, sein eigenes Verhalten unter einem Gruppendruck an dem Verhalten der Gruppe auszurichten.

Das LAG sieht auch aus anderen Gründen kein Mitbestimmungsrecht gegeben. Insbesondere stellte es fest, dass der Arbeitgeber durch den Seitenbetrieb keine personenbezogenen Daten im Sinne des Bundesdatenschutzgesetzes (BDSG) erhebt und auch keine Verletzung des Persönlichkeitsrechts wegen der auf Facebook geäußerten Kritik angenommen werden kann. Die Meinungsfreiheit der Spender überwiege grundsätzlich die Persönlichkeitsentfaltung der Mitarbeiter, soweit keine beleidigenden Kommentare erfolgten. Diese könnten wiederum gelöscht werden.

III. Fazit und Konsequenzen für die Hochschulpraxis

Die Relevanz der Entscheidung ist insbesondere für Universitätskliniken als hoch einzuschätzen, da sich die Problematik deckungsgleich auf sie übertragen lässt, soweit sie einen Facebook-Auftritt als Informationsforum für Blutspenden betreiben. Aber auch für alle anderen Hochschulbereiche ist die Problematik eröffnet, soweit ein Facebook-Auftritt besteht und von Mitarbeitern betreut wird.

Eine Einschränkung ergibt sich daraus, dass das BetrVG und damit das Mitbestimmungsrecht nur für privatrechtliche Rechtsträger (z. B. GmbH) gilt, so dass Körperschaften öffentlichen Rechts, zu denen Hochschulen in der Regel zählen, nicht dem BetrVG unterliegen (§ 130 BetrVG). Allerdings gilt das BetrVG auch für privatrechtliche Gesellschaften, die der öffentlichen Hand gehören, denn es kommt allein auf den formell-rechtlichen Charakter der Gesellschaft an. Zudem

enthalten die Personalvertretungsgesetze der Bundesländer, die die Mitbestimmungsrechte der Beschäftigten des öffentlichen Dienstes regeln und die für die dort ansässigen Hochschulen in der Regel gelten, übereinstimmende oder jedenfalls vergleichbare Regelungen wie das BetrVG. So findet insbesondere der die Mitbestimmung bei technischer Überwachung anordnende § 87 Abs. 1 Ziffer 6 BetrVG neben § 75 Abs. 3 Nr. 17 Bundespersonalvertretungsgesetz Entsprechungen zum Beispiel in § 72 Landespersonalvertretungsgesetz NRW, § 85 Personalvertretungsgesetz Berlin und Artikel 75a Bayrisches Personalvertretungsgesetz.

Sofern ein Personalrat vorhanden oder falls eine wissenschaftliche Einrichtung rechtlich beispielsweise als GmbH organisiert und ein Betriebsrat gewählt ist, kann sich aus den oben genannten Gründen eine Mitbestimmung an einem Facebook-Seitenbetrieb jedenfalls hinsichtlich der Mitarbeiter ergeben, denen die Betreuung der Seite zukommt. Das gilt wiederum nur, wenn nicht bereits tarifvertraglich abschließend eine Regelung zum jeweiligen Mitbestimmungsrecht geschlossen wurde. Dann ist nämlich ein weitergehender Schutz der Arbeitnehmer laut ständiger Rechtsprechung des BAG nicht mehr erforderlich. Abschließend ist eine tarifvertragliche Regelung, wenn sie alle denkbaren Fälle abdeckt und dem Schutzzweck (also vorliegend der Wahrung der freien Persönlichkeitsentfaltung) Genüge tut. Es wäre demnach zu prüfen, ob eine tarifvertragliche Vereinbarung zur technischen Überwachung auch die in Rede stehende Facebook-Problematik erfasst und zum Schutz der Mitarbeiter regelt. Sofern dies der Fall ist, findet das Mitbestimmungsrecht keine Anwendung. Das Mitbestimmungsrecht besteht aber überhaupt nur dann, wenn die Anonymität des einzelnen Mitarbeiters nicht gewährleistet ist. Stellt der Arbeitgeber Anonymität her, besteht es nicht.

Zusammenfassend lässt sich sagen, dass bei der folgenden modellhaften Konstellation ein Mitbestimmungsrecht zu verneinen sein dürfte: Es besteht eine Gruppe von etwa zehn Mitarbeitern, die die Seitenbetreuung als Teilaspekt neben vielen anderen Tätigkeiten ausüben, weder als Gruppe noch einzeln für ein bestimmtes Leistungsergebnis verantwortlich sind und bei der alle Mitglieder denselben allgemeinen Administratorenzugang nutzen und auch mittels anderer Möglichkeiten nicht identifizierbar sind. Hingegen könnte ein Mitbestimmungsrecht zu beachten sein, wenn es sich um eine Gruppe handelt, die aus nur sechs oder weniger Mitarbeitern besteht, denen die Seitenbetreuung als Haupt- oder gar Alleinaufgabe zukommt, denen vorgegeben wird, wie viele Kommentare in einem bestimmten Zeitraum zu beantworten sind oder in welcher Zeit Kommentare beantwortet werden müssen und die jeweils über einen individuellen Zugang oder unterschiedliche IP-Adressen verfügen oder anhand anderer Mittel (wie z. B. eines Dienstplans) identifiziert werden können. Zu beachten ist ferner, dass diese Kriterien nicht kumulativ vorliegen müssen. Für die Bejahung eines Mitbestimmungsrechts könnte das Vorliegen eines Merkmals ausreichen.

Vertrauen ist gut, Kontrolle ist besser?

Das LAG Rheinland-Pfalz zu Arbeitszeitbetrug und Verwertbarkeit von Erkenntnissen bei rechtswidriger Einsichtnahme in den elektronischen Kalender des Arbeitnehmers

von Jan Heuer

Das Landesarbeitsgericht Rheinland-Pfalz (LAG Rheinland Pfalz, Urteil vom 25.11.2014, Az.: 8 Sa 363/14) bestätigt eine außerordentliche Kündigung wegen Falschdeklarationen im Arbeitszeitkonto. Gegenstand des Verfahrens war zum einen, ob die heimliche Einsichtnahme des Arbeitgebers in einen elektronischen Kalender des Arbeitnehmers rechtmäßig ist, und zum anderen, unter welchen Voraussetzungen dadurch gewonnene Erkenntnisse im Prozess verwertbar sind. Laut LAG sind trotz Rechtswidrigkeit der Einsichtnahme die aus ihr gewonnenen Erkenntnisse bei unstrittigem Sachvortrag im Prozess verwertbar. Die außerordentliche Kündigung wegen Falschangabe einer ganztätigen Dienstreise war damit im zugrundeliegenden Fall rechtmäßig.

I. Hintergrund

Auf dem betrieblich genutzten Computer geführte elektronische Kalender sind im heutigen Arbeitsalltag nicht mehr wegzudenken. Sie dienen der täglichen Optimierung von Arbeitsabläufen und sind damit zu einem unerlässlichen Bestandteil der modernen Arbeitswelt geworden. Viele Arbeitnehmer nutzen ihren dienstlichen Kalender auch, um die Planung privater Termine kenntlich zu machen. Die Überprüfung der Kalender durch den Arbeitgeber kann damit schnell zu einem Eingriff in die Privatsphäre des Arbeitnehmers führen.

Oftmals besteht jedoch das Interesse des Arbeitgebers, die Terminierungen seiner Mitarbeiter zu überprüfen. Die Ursache dieses Interesses kann vielfältiger Natur sein. Insbesondere kann ein erhöhtes Bedürfnis des Arbeitsgebers bestehen, den Kalender mit den Angaben in etwaigen Arbeitszeitkonten abzugleichen, um so mögliche Betrugsversuche aufzuklären bzw. den möglichen Verdacht eines solchen Verhaltens zu bestätigen. Fraglich ist dabei, ob ein unbegrenzter Zugriff des Arbeitgebers auf den Kalender zulässig sein kann und wie mögliche Erkenntnisse, die aus einer Einsichtnahme gewonnen werden, gegen den Arbeitnehmer verwendet werden können.

II. Urteil des LAG Rheinland-Pfalz

1. Sachverhalt

Kern der Streitigkeit, die dem LAG Rheinland-Pfalz vorlag, war die Frage der Rechtmäßigkeit einer außerordentlichen Kündigung des Arbeitgebers ggü. einer seiner Arbeitnehmerinnen. Die betroffene Arbeitnehmerin war Angestellte bei der Beklagten. Als Leiterin eines analytischen Labors trug Sie zuletzt Verantwortung für 38 Beschäftigte. Sie war arbeitsvertraglich verpflichtet, ein Zeitkonto zum Nachweis erbrachter Arbeitsleistungen zu führen.

Am 12.09.2013 erhielt der Personalleiter der Beklagten einen Hinweis darauf, dass bestimmte, im Zeitkonto durch die Klägerin geltend gemachte Zeiteinträge, nicht den wahren Begebenheiten entsprachen. So soll die Beklagte einen Privattermin wahrgenommen haben, obwohl Sie für den gesamten Tag einen beruflichen Messebesuch in ihr Arbeitszeitkonto eintrug. Der Personalleiter ging dem Hinweis nach und konnte dessen Richtigkeit feststellen. Danach wurde der Betriebsrat zur beabsichtigten außerordentlichen Kündigung angehört. Ebenso wurde dem Betriebsrat mitgeteilt, dass der Personalleiter beabsichtige den elektronischen Terminkalender der Klägerin, welcher sich auf ihrem (rein) betrieblich

genutzten Notebook befand, zu überprüfen. Der Betriebsrat erhob dagegen keine Einwände. Der Kalender wurde sodann überprüft und mehrere Privattermine, welche im Arbeitszeitkonto als Dienstzeit geltend gemacht worden waren, wurden entdeckt. Am 30.09.2013 wurde gegenüber der Klägerin die außerordentliche Kündigung des Arbeitsverhältnisses mitgeteilt. Die Klägerin erhob dagegen eine Kündigungsschutzklage vor dem Arbeitsgericht Mainz (ArbG). Die von der Beklagten (Arbeitgeberin) geltend gemachten Verstöße, die durch die Einsichtnahme bekannt wurden (also die Deklaration privater Termine als Arbeitszeit), blieben im Verlauf des Verfahrens von der Klägerin unbestritten. Die Klage wurde abgewiesen.
Mit dem Begehren, das Urteil des ArbG Mainz abzuändern und festzustellen, dass das Beschäftigungsverhältnis nicht durch die außerordentliche Kündigung beendet wurde, wandte sich die Klägerin mit Ihrer Berufung an das LAG Rheinland-Pfalz. Das LAG erhielt die Entscheidung des ArbG Mainz aufrecht und bestätigte die Wirksamkeit der fristlose Kündigung und die Beendigung des Arbeitsverhältnisses zum 30.09.2013.

2. Entscheidungsgründe

In seiner Entscheidung hatte das LAG dabei sowohl materiell-rechtliche, als auch prozessuale Aspekte zu bewerten.

Grund der außerordentlichen Kündigung

Aus materiell-rechtlicher Sicht wurde dabei dem falsch geführten Arbeitszeitkonto durch das LAG besondere Bedeutung zugemessen. Um eine fristlose Kündigung zu rechtfertigen, muss gem. § 626 Absatz 1 des Bürgerlichen Gesetzbuches (BGB) ein wichtiger Grund vorliegen. Die Frage, ob ein wichtiger Grund vorliegt, wird dabei in zwei Stufen geprüft. So muss der zugrunde liegende Sachverhalt grundsätzlich geeignet sein, einen wichtigen Grund darzustellen (1. Stufe) und darüber hinaus auch im vorliegenden Einzelfall einen solchen wichtigen Grund darstellen (2. Stufe). Das Arbeitsrecht wird dabei vom Prognoseprinzip beherrscht. Eine Kündigung soll nie für die Sanktion von Fehlverhalten in der Vergangenheit ausgesprochen werden, sondern den Parteien die Möglichkeit eröffnen die vertragliche Beziehung zu beenden, wenn ein vertragskonformes Zusammenwirken für die Zukunft nicht mehr möglich erscheint.
Dem zugrundeliegenden Fall war insoweit zu entnehmen, dass die Klägerin in Ihrem Zeitkonto falsche Angaben gemacht hatte. Durch die Falschdeklaration hat die Klägerin eine Gutschrift vergütungspflichtiger Stunden erhalten, ohne die notwendige Arbeitsleistung erbracht zu haben. Der Beklagten war dadurch ein erheblicher Schaden entstanden.
Dieser sog. Arbeitszeitbetrug ist insoweit generell als wichtiger Grund durch die Rechtsprechung anerkannt. Laut LAG stellt der Arbeitszeitbetrug der Klägerin auch im konkreten Einzelfall (2. Stufe) unter Anwendung des Prognoseprinzips einen wichtigen Grund nach § 626 Absatz 1 BGB dar.
Insbesondere wurden durch das Gericht die Führungsposition und die damit einhergehende Vorbildfunktion der Klägerin thematisiert. Auf Grund der Schwere des Verstoßes hielt das Gericht eine vorherige Abmahnung, die als milderes Mittel der fristlosen Beendigung des Arbeitsverhältnisses grundsätzlich vorgeht, für nicht erforderlich. Die zweiwöchige Frist, innerhalb derer eine außerordentliche Kündigung ausgesprochen werden muss (§ 626 Absatz 2 Satz 1 BGB), wurde, ebenso wie die erforderliche Schriftform (§ 623 BGB), gewahrt.

Einsichtnahme in den Kalender und Wirksamkeit der Kündigung

Im Zivilprozess geht es daneben immer auch darum, dass über streitige Tatsachen Beweis erhoben werden muss. Der Grundsatz der Beweislast ist dabei so gelegen, dass jede Partei, über die für sie günstigen Umstände Beweis erbringen muss. Wird der Tatsachenvortrag einer Partei nicht bestritten, gilt er als zugestanden und ist damit entscheidungsrelevanter Sachverhalt des Prozesses (§ 138 Absatz 3 Zivilprozessordnung). Nur solche Vorträge, die als bewiesener oder unstrittiger Sachverhalt gegeben sind, können die Grundlage für die Anwendung materiellen Rechts im Prozess bilden.
In dem vom LAG zu entscheidenden Fall war insofern dem Umstand Rechnung zu tragen, dass der Arbeitgeber den elektronischen Kalender der Klägerin ohne deren Mitwirken durchsucht hatte und nur so die Fehldeklaration des Zeitkontos vollumfänglich entdecken konnte. Dies bildete dann u. a. die Grundlage der Kündigung. Das Gericht beschäftigte sich daran anknüpfend mit der Frage, ob auf Grund dieser, möglicherweise rechtswidrigen, Einsichtnahme, eine Unwirksamkeit der Kündigung bestehen könnte.
Bezüglich der Einsichtnahme war unter rechtlichen Gesichtspunkten nach zwei Aspekten zu trennen. Zum einen galt es der Frage nachzugehen, ob die Einsichtnahme in den Kalender selbst rechtmäßig war, zum andern, ob die möglicherweise rechtswidrig erlangten Informationen im Prozess verwertet werden konnten, also der durch sie begründete Streitstoff

berücksichtigt werden durfte.

Die Rechtmäßigkeit der Einsichtnahme war auf der Grundlage des Bundesdatenschutzgesetzes (BDSG) zu ermitteln. Gegenstand des BDSG sind personenbezogene Daten (§ 3 Absatz 1 BDSG). Dass Terminplanungen im Ergebnis Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person darstellen und damit solche personenbezogenen Daten sind, war insoweit unproblematisch. Das Erheben solcher Daten kann nach dem BDSG ohne Mitwirken des Betroffenen nur erfolgen, wenn eine Rechtsvorschrift dies vorsieht (vgl. § 4 Absatz 2 Nr. 1 BDSG).

Für die Erhebung personenbezogener Daten in Arbeitsverhältnissen gilt die Regelung des § 32 BDSG. So ist u.a. vorgesehen, dass Daten dann erhoben werden dürfen, wenn diese für die Beendigung des Arbeitsverhältnisses erforderlich sind. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat. Die Erhebung, Verarbeitung oder Nutzung muss zur Aufdeckung erforderlich sein und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung darf nicht überwiegen, insbesondere dürfen Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sein (vgl. § 32 Absatz 1 Satz 2 BDSG). An die Erforderlichkeit sind dabei erhöhte Anforderungen zu stellen. Indes sah das LAG in dem bereits vor der Sichtung bestätigten Fall der Fehldeklaration einen, für den Arbeitgeber ausreichenden, Verdacht des Arbeitszeitbetrugs und stellte zudem fest, dass die Einsichtnahme für die Beklagte das einzige Mittel war, etwaige Unregelmäßigkeiten in Bezug auf die Arbeitszeiterfassung der Klägerin aufzuklären. Es ist dennoch auch klargestellt worden, dass mögliche mildere Mittel genutzt werden müssen, um den Anforderungen an die Verhältnismäßigkeit gerecht zu werden. Ein milderes Mittel als die geheime Einsichtnahme stellt dabei die Einsichtnahme unter Anwesenheit der Klägerin dar. Nach ständiger Rechtsprechung des Bundesarbeitsgerichts (BAG) erhöht die Heimlichkeit einer solchen Maßnahme nämlich typischerweise das Gewicht der aus ihr resultierenden Freiheitsbeeinträchtigung.

Dass eine Einsichtnahme grundsätzlich erfolgte („Ob“ der Maßnahme), wurde dabei durch das LAG nicht beanstandet. Vielmehr fußte die Rechtswidrigkeit der Einsichtnahme im konkreten Fall auf der heimlichen Durchführung („Wie“ der Maßnahme). Die heimliche Einsichtnahme des Arbeitgebers in den Kalender war damit nicht durch § 32 BDSG gedeckt und folglich rechtswidrig.

Die Frage der Rechtmäßigkeit der Einsichtnahme war, so das LAG, von der Frage der Verwertung der gewonnen Erkenntnisse zu trennen. So mag die Erlangung der Erkenntnisse auf rechtswidrige Weise erfolgt sein, jedoch führt dies nach der ständigen Rechtsprechung des BAG nicht zwingend zu einem Verbot der prozessualen Verwertung. Eine Unverwertbarkeit im Prozess ist bei unbestrittenem Sachvortrag nur dann gegeben, wenn es der Schutz des Arbeitnehmers erfordert. Dies ist dann der Fall, wenn durch die gerichtliche Entscheidung der Eingriff in die Privatsphäre des Arbeitnehmers vertieft würde. Unstreitige Tatsachen werden also nur dann nicht verwertet, wenn der Schutzzweck derjenigen Norm, die eine mögliche Informationsgewinnung regelt (im Fall § 32 BDSG), einer gerichtlichen Verwertung entgegensteht.

Da im vorliegenden Fall nicht die Berechtigung der Beklagten an sich in Rede stand („Ob“), sondern die Rechtswidrigkeit aus dem „Wie“ der Maßnahme folgte, sah das LAG die Eingriffsintensität nicht als zu hoch an. Daneben wurde herausgestellt, dass mit der Einsichtnahme nur ein relativ geschützter Bereich des Persönlichkeitsrechts der Beklagten berührt wurde. Der Eingriff bezog sich nur auf den Dienstkalender der Betroffenen, sodass ihr Privatleben nur geringfügig betroffen war. Daneben wurde durch das LAG herausgestellt, dass der Klägerin auch die Möglichkeit der Einsichtnahme selbst bewusst gewesen sein muss. Dass z. B. im Falle von Erkrankung oder Verhinderung eine Einsichtnahme erfolgen würde, um Schäden durch die Versäumung von Terminen abzuwenden, sei dabei vorhersehbar gewesen. Eine Vertiefung des Verstoßes des Arbeitgebers durch die gerichtliche Verwertung des unbestrittenen Tatsachenvortrags wurde damit vom LAG abgelehnt. Trotz rechtswidriger Einsichtnahme war damit eine Verwertung der erlangten Erkenntnisse (also, dass der sich aus der Einsichtnahme gebildete Sachverhalt voll berücksichtigt wird) möglich.

III. Fazit und Relevanz für die Hochschulen

Bei der Einsichtnahme in Accounts von Mitarbeitern, um deren Kalender zu prüfen und so dem Verdacht eines Arbeitszeitbetruges nachzugehen, sind die datenschutzrechtlichen Anforderungen zu beachten. Für Hochschulen relevant ist dabei, dass das BDSG auf Sie nicht anwendbar ist. Hochschulen sind öffentliche Stellen der Länder. Auf Hochschulen findet damit

das jeweils einschlägige Landesdatenschutzgesetz (LDSG) Anwendung. Der Maßstab ist insofern dort zu suchen. Die LDSGe enthalten jedoch im Regelfall eine dem § 32 BDSG vergleichbare Regelung (z. B. § 29 DSG NRW oder § 36 BaWÜDSG). Die Aussagen des LAG sind im Ergebnis im Rahmen dieser Übereinstimmung der Vorschriften, also im Wesentlichen, zu übertragen.

Grundlegend ist ein Arbeitszeitbetrug geeignet eine fristlose Kündigung zu rechtfertigen. Die mögliche Rechtswidrigkeit der Einsichtnahme hindert eine prozessuale Verwertung der gewonnen Erkenntnisse dabei nur, wenn ein schwerer Verstoß vorliegt, der durch die Verwertung die Verletzung der Rechte des Betroffenen vertiefen würde.

Obwohl das LAG eine zulässige Verwertung annahm, wird durch die Entscheidung auch verdeutlicht, dass die Möglichkeit besteht, dass eine rechtswidrige Einsichtnahme in elektronische Kalender einer prozessualen Verwertung, der durch sie gewonnen Erkenntnisse, entgegenstehen kann. Umso mehr sollten Hochschulen vor Einsichtnahme in entsprechende elektronische Kalender den betroffenen Arbeitnehmer informieren und die Einsichtnahme selbst möglichst nicht heimlich vornehmen. In jedem Fall sollte zuvor Rücksprache mit der Rechtsabteilung gehalten werden. Vorsicht in Bezug auf Einsichtnahmen ist dann geboten, wenn der betriebliche Computer nicht rein betrieblich, sondern auch privat genutzt wird. Ist dies der Fall, können sich andere, erhöhte datenschutzrechtliche Anforderungen im Rahmen einer Erforderlichkeitsprüfung ergeben.

Es ist hervorzuheben, dass sich die Entscheidung des LAG explizit auf den elektronisch geführten Kalender der Arbeitnehmerin bezieht und sich nicht pauschal auf z. B. die Einsichtnahme in E-Mailkonten übertragen lässt.

Werden die oben dargestellten Grundsätze beachtet, können die damit gewonnen Erkenntnisse aus der Einsichtnahme in den elektronischen Kalender eines rein betrieblich genutzten Computers eine ordentliche oder auch fristlose Kündigung grundsätzlich rechtfertigen.

Zulässige Leseplätze und (un-)zumutbare Kontrollen?

Zum vorerst letzten Mal zur Zulässigkeit elektronischer Leseplätze

von Lennart Sydow

Seit seiner Einführung im Jahr 2008 hat der § 52b Urheberrechtsgesetz (UrhG) mehrfach die Gerichte beschäftigt und ging dabei durch alle Instanzen. Nachdem der Bundesgerichtshof (BGH) diesbezüglich schon 2012 den Europäischen Gerichtshof (EuGH) angerufen und dieser im letzten September über die Auslegung der zugrunde liegenden Richtlinie entschieden hatte, urteilte der BGH am 16. April 2015 nun abschließend über die Zulässigkeit elektronischer Leseplätze (Az.: I ZR 69/11).

I. § 52b UrhG

Die Vorschrift des § 52b UrhG wurde mit dem zweiten Korb der Urheberrechtsreform eingeführt und trat zum 1. Januar 2008 in Kraft. Sie setzt Vorgaben der Richtlinie 2001/29/EG (zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft) in nationales Recht um und erlaubt, unter gewissen Voraussetzungen, öffentlich zugänglichen Bibliotheken, Museen und Archiven, Werke aus ihrem Bestand innerhalb der Räume der jeweiligen Einrichtung an elektronischen Leseplätzen zur Verfügung zu stellen. Erforderlich ist dafür, dass die Einrichtung keine wirtschaftlichen Zwecke verfolgt, die Nutzung nur zur Forschung und für private Studien stattfindet und keine vertraglichen Regelungen mit den Rechteinhabern dem entgegenstehen. Der Gesetzgeber bezweckte damit, den genannten Einrichtungen die Erfüllung ihres Bildungsauftrages zu erleichtern und die Medienkompetenz der Bevölkerung zu fördern.

II. Weg durch die Instanzen und Vorlage an den EuGH

Um die Auslegung dieser Norm wird seit 2009 in einem Musterverfahren zwischen dem Ulmer Verlag und der Technischen Universität Darmstadt gestritten. Deren Zentralbibliothek betrieb öffentlich zugängliche elektronische Leseplätze, an denen die Nutzer ausgewählte Werke des Bibliotheksbestandes auch in digitaler Form abrufen konnten. Dazu hatte die TU Darmstadt zunächst die Inhalte, wie das im konkreten Fall betroffene Buch „Einführung in die neuere Geschichte“ des Ulmer Verlages, digitalisiert, um diese dann über die elektronischen Leseplätze verfügbar zu machen. Die Anzahl der gleichzeitig abrufbaren digitalen Dokumente war dabei auf die Anzahl der analog vorhandenen Exemplare der Bibliothek beschränkt. Ein Abruf per Netzzugriff, von außerhalb der Räumlichkeiten der Bibliothek, war nicht möglich. Die Nutzer hatten aber nicht nur die Möglichkeit die Inhalte einzusehen, sondern konnten diese auch ganz oder in Teilen ausdrucken oder auf mitgebrachten USB-Sticks abspeichern. Das Angebot des Verlages, die herausgegebenen Bücher als E-Books zu lizensieren, hatte die Universität nicht angenommen. Nach einer Abmahnung durch den Verlag reagierte die Bibliothek, indem sie für den Zugang die Vorlage eines Benutzungsausweises forderte und durch ein Hinweisschild darauf aufmerksam machte, dass nur die Verwendung zu wissenschaftlichen Zwecken oder privaten Studien erlaubt und die Weiterverbreitung und Vervielfältigung darüber hinaus untersagt sei.

Das Landgericht Frankfurt am Main hatte im Frühjahr 2011 (Urteil vom 16. März 2011 – 2/06 O 378/10) als erste Instanz zwar die Digitalisierung der Inhalte und das zur Verfügung Stellen an elektronischen Leseplätzen für zulässig erachtet, die darüber hinausgehende Möglichkeit, die Inhalte zu drucken

oder digital abzuspeichern, dagegen als rechtswidrige Urheberrechtsverletzung untersagt. Der als Revisionsgericht angerufene Bundesgerichtshof setzte das Verfahren dann im September 2012 aus, um mehrere Auslegungsfragen zu der dem § 52b UrhG zugrunde liegenden EU-Richtlinie dem EuGH vorzulegen (siehe dazu: Wörheide, „Digitale Leseplätze auf dem Weg nach Europa", DFN-Infobrief Recht 11/2012). Nachdem der EuGH dann im September 2014 über diese Auslegungsfragen entschied (Urteil vom 11. September 2014 – C-117/13; hierzu: Roos, „Weniger Papier ist mehr!", DFN-Infobrief Recht 11/2014 und auch „Bibliothek 2.0: Alles digital, oder was?" DFN-Infobrief Recht 08/2014), urteilte nun der Bundesgerichtshof, als im konkreten Fall höchste Instanz, über die streitigen Rechtsfragen.

III. Rechtliche Betrachtung

Von Anfang an unumstritten war die Tatsache, dass es sich bei dem fraglichen Buch um ein urheberrechtlich geschütztes Schriftwerk handelt und der Umstand, dass durch dessen Digitalisierung und Zurverfügungstellung in die Verwertungsrechte des Urhebers eingegriffen wurde. Der Streit der Parteien behandelte die Frage, ob dieser Eingriff der Bibliothek durch die Schrankenregelungen des Urheberrechtsgesetzes erlaubt war. Über die entscheidende Auslegung der § 52b UrhG zugrunde liegenden EU-Richtlinie hatte der EuGH Ende 2014 entschieden. Für den Bundesgerichtshof stand nach der Entscheidung des EuGHs zu den drei Vorlagefragen deren Umsetzung an. Thematisch ging es hier darum, ob das Angebot eines Lizenzvertrages eine „vertragliche Regelung" im Sinne des § 52b UrhG darstellt, ob die Erlaubnis des § 52b UrhG auch die vorherige Digitalisierung der Werke umfasst und ob die Möglichkeit, die Inhalte auszudrucken oder digital zu speichern, über den erlaubten Rahmen hinausgeht.

Laut § 52b S. 1 UrhG ist die Einrichtung elektronischer Leseplätze nur dann zulässig, wenn dem keine vertraglichen Regelungen mit den Rechteinhabern entgegenstehen. Der Entscheidung des EuGH folgend entschied der BGH, dass unter „vertragliche Regelungen" in diesem Sinne lediglich vereinbarte Regelungen in bestehenden Verträgen fallen. Ein bloßes Angebot zum Abschluss eines Nutzungsvertrages stehe dagegen der Erlaubnis des § 52b UrhG nicht entgegen. Der EuGH hatte dies unter anderem damit begründet, dass die praktische Wirksamkeit der Norm entfiele, wenn bereits das bloße Angebot eines Nutzungsvertrages die Erlaubnis des § 52b UrhG ausschließen würde. Der BGH führte aus, dass er aufgrund der Tatsache, dass die Norm in Umsetzung der EU-Richtlinie entstanden sei, dazu verpflichtet sei, diese richtlinienkonform auszulegen und sah sich daher an die Entscheidung des EuGH gebunden. Daher sei im Streitfall mangels Vertragsschlusses unerheblich, ob der Ulmer Verlag der Bibliothek ein angemessenes Angebot zum Erwerb des E-Books gemacht habe.

Bezüglich der Frage, ob die Digitalisierung der Inhalte zum Zwecke des Zugänglichmachens von der Erlaubnis des § 52b UrhG gedeckt ist, hatte der EuGH entschieden, dass die jeweiligen Mitgliedstaaten gesetzliche Regelungen vorsehen können, die es den oben genannten Einrichtungen erlauben, Inhalte zu digitalisieren, wenn dies für die Zugänglichmachung erforderlich ist. Der Bundesgerichtshof hat nun darauf aufbauend eine solche gesetzliche Erlaubnis angenommen. Diese ergebe sich zwar nicht ausdrücklich aus § 52b UrhG, nach Meinung des Gerichts aber aus einer entsprechenden Anwendung des § 52a Abs. 3 UrhG. § 52a UrhG erlaubt unter gewissen Umständen die öffentliche Zugänglichmachung von geschützten Werken für den Unterricht an Hochschulen und Schulen sowie für eigene wissenschaftliche Forschung. Der vom BGH angesprochene Abs. 3 gestattet auch die zur Erfüllung dieses Zweckes erforderlichen Vervielfältigungen. Dessen entsprechende Anwendung für die Einrichtung elektronischer Leseplätze wird ebenfalls damit begründet, dass ansonsten die praktische Wirksamkeit des § 52b UrhG verloren ginge. Zu dieser richterlichen Rechtsfortbildung sah sich der Senat durch das Gebot der europarechtskonformen Auslegung verpflichtet, welches nicht nur die klassische Auslegung bestehender Vorschriften erfordere, sondern auch darüber hinaus die Rechtsfortbildung im Sinne der zugrunde liegenden Richtlinie gebiete. Die dafür erforderliche planwidrige Regelungslücke ergebe sich daraus, dass aus der Gesetzesbegründung hervorgehe, dass die Regelung des § 52b UrhG es den Bibliotheken und sonstigen Einrichtungen ermöglichen sollte, Werke zu digitalisieren und dann den Nutzern zur Verfügung zu stellen. Soweit die Bücher aber lediglich in gedruckter Form vorliegen, sei die Digitalisierung für die Zugänglichmachung über den Terminal unbedingt erforderlich. Dass hierfür keine ausdrückliche Erlaubnis in § 52b UrhG enthalten ist, sei daher planwidrig und diese Regelungslücke aufgrund der vergleichbaren Interessenlage durch die entsprechende Anwendung des § 52a Abs. 3 UrhG zu schließen. Somit ist die Digitalisierung, bei der es sich um eine grundsätzlich dem Urheber vorbehaltene Vervielfältigung handelt, zulässig, soweit sie für die

Zugänglichmachung im Rahmen des § 52b UrhG erforderlich ist.

Auch beim letzten Streitpunkt – der Möglichkeit für die Nutzer, die Inhalte auszudrucken oder digital abzuspeichern – nutzt der Bundesgerichtshof den Spielraum, der sich aus den Vorgaben des EuGH ergibt. Der EuGH hatte auf die entsprechende Vorlagefrage geantwortet, dass Art. 5 Abs. 3 n) nur die Wiedergabe von Inhalten an elektronischen Leseplätzen erlaubt und daher das Ausdrucken und Speichern durch die Nutzer als Vervielfältigungshandlung nicht von dieser speziellen Erlaubnis erfasst sei. Diese Handlungen könnten aber durch nationale Umsetzungen des Art. 5 Abs. 2 a) oder b) der Richtlinie in den einzelnen Mitgliedstaaten gestattet werden, soweit die dort genannten Voraussetzungen (insbesondere ein gerechter Ausgleich für den Rechteinhaber) erfüllt sind. Der BGH entschied darauf aufbauend, dass die Einrichtung das Vervielfältigungsrecht des Urhebers auch dann nicht verletzt, wenn sie die Inhalte so zur Verfügung stellt, dass die Nutzer elektronischer Leseplätze diese ausdrucken oder auf einem USB-Stick speichern können. Eine Auslegung des § 52b UrhG dahingehend, dass die Inhalte nur in einer Weise zugänglich gemacht werden dürften, die ausschließlich das Lesen ohne die Möglichkeit, digitale oder analoge Kopien anzufertigen, erlaubt, lehnten die Richter mit Hinweis auf die zugrunde liegende Richtlinie ab. Diese enthalte nämlich in Art. 5 Abs. 3 n) weder eine Erlaubnis, noch ein Verbot der Vervielfältigungshandlungen durch Nutzer elektronischer Leseplätze. Deren Rechtmäßigkeit richte sich folglich alleine danach, ob die Vervielfältigungshandlung als solche durch eine andere Schranke erlaubt sei. Dies sei beispielsweise im Rahmen der Privatkopierfreiheit des § 53 UrhG denkbar. Danach können z. B. einzelne Vervielfältigungsstücke zum privaten oder wissenschaftlichen Gebrauch oder kleine Teile eines Werkes zur Veranschaulichung im Unterricht vervielfältigt werden. Dass die Nutzer möglicherweise diese Kopiermöglichkeit auch dazu nutzen, unrechtmäßige Kopien anzufertigen, führe nicht schon dazu, dass die Zugänglichmachung als solche unzulässig sei.

Auch wenn im vorliegenden Verfahren keine unrechtmäßigen Vervielfältigungen durch Nutzer festgestellt wurden, äußerte sich das Gericht dennoch zu einer möglichen Verantwortlichkeit der Einrichtung für solche Rechtsverletzungen. Es komme eine Haftung entweder als Teilnehmer oder Störer in Betracht. Da es sich beim Angebot elektronischer Leseplätze aber, wie gerade dargestellt, um ein grundsätzlich zulässiges Verhalten handelt, wäre dies nur der Fall, wenn eine Einrichtungen nicht die zumutbaren Vorkehrungen trifft, um solche Rechtsverletzungen zu verhindern. Um dies zu vermeiden, müssen zum einen die Nutzer darauf hingewiesen werden, dass eine Vervielfältigung nur im Rahmen der Voraussetzungen des § 53 UrhG zulässig ist, und zum anderen auch mögliche und zumutbare Maßnahmen zur Kontrolle und Überwachung dieser Voraussetzungen von der Einrichtung getroffen werden.

IV. Bewertung und Auswirkungen für Hochschulen und Forschungseinrichtungen

Dass ein bloßes Vertragsangebot keine vertragliche Regelung im Sinne des § 52b UrhG darstellt, war durch das Urteil des EuGH bereits vorgegeben. Auch dass den Mitgliedstaaten die gesetzliche Erlaubnis der Digitalisierung der Werke möglich sein muss, um die Wirksamkeit der Vorschrift nicht entfallen zu lassen, war durch das Urteil des EuGH festgestellt. Interessant war hierbei aber, dass der Bundesgerichtshof diese Lücke durch eine analoge Anwendung des § 52a Abs. 3 UrhG schloss, anstatt vom deutschen Gesetzgeber dafür eine ausdrückliche gesetzliche Erlaubnis zu fordern. Der Hinweis auf die Kontroll- und Überwachungspflichten der jeweiligen Einrichtung zur Abwendung einer Haftung als Teilnehmer oder Störer könnte aber die praktische Umsetzung der Angebote stark erschweren. Dabei ist jedenfalls problematisch, dass durch das unkonturierte Erfordernis erforderlicher und zumutbarer Maßnahmen zur Verhinderung von Rechtsverletzungen weitere Rechtsunsicherheit besteht. Während ein Hinweis auf die Voraussetzungen der Privatkopierfreiheit des § 53 UrhG ohne großen Aufwand umsetzbar ist, stellt sich die Frage, welcher Aufwand zur Verhinderung von Rechtsverletzungen betrieben werden muss.

Für Hochschulen und Forschungseinrichtungen bedeutet dieses Urteil deshalb nur zum Teil einen Erfolg. Die Bibliotheken müssen sich von nun an zwar sicher nicht mehr darauf verweisen lassen, dass ein Angebot besteht, Lizenzen für die digitale Nutzung der Werke vom Rechteinhaber zu erwerben. Sie können auch ohne Berücksichtigung eines solchen Angebots von ihren Rechten aus § 52b UrhG Gebrauch machen und elektronische Leseplätze einrichten. Auch die

dafür notwendige Digitalisierung der Inhalte ist zulässig, was die praktische Umsetzung vielfach überhaupt erst ermöglicht. Bezüglich der Art der Zugänglichmachung besteht darüber hinaus auch keine Verpflichtung, die Inhalte in einer Weise zugänglich zu machen, die das Ausdrucken und digitale Abspeichern durch die Nutzer verhindert. Die Bibliotheken müssen dabei keine Einschränkungen vornehmen. Dies befreit nicht nur von den technischen Maßnahmen, die erforderlich sind, um solche Vervielfältigungen zu verhindern, sondern es erhöht zudem die Attraktivität entsprechender Angebote erheblich und ist deshalb ebenfalls erfreulich. Genau solche technischen Maßnahmen erscheinen aber im Rahmen der erforderlichen und zumutbaren Verhinderung von Rechtsverletzungen durch Nutzer wieder denkbar. Zwar enthält das Urteil ausführliche Erläuterungen zu dieser Verpflichtung, dennoch geben diese keine eindeutigen Hinweise darauf, welcher Aufwand noch angemessen ist. So ist es derzeit leider auch nicht möglich, hierzu rechtssichere Empfehlungen auszusprechen.

Insgesamt ist das Urteil aus Hochschulsicht daher zwar einerseits zu begrüßen, weil es die Informationsfreiheit stärkt, indem es den Bibliotheken nach langer Unsicherheit endlich ermöglicht, elektronische Leseplätze in sinnvollem Umfang umzusetzen. Andererseits könnte aber die mangelnde Rechtssicherheit bezüglich der Maßnahmen zur Verhinderung von Rechtsverletzungen und die Bindung der zulässigerweise gleichzeitig verfügbaren elektronischen Dokumente an die Anzahl analog verfügbarer Werkstücke dazu führen, dass auch weiterhin erhebliche rechtliche Schwierigkeiten den Betrieb solcher Leseplätze erschweren.

Keine Lizenz zur Schätzung

Landgericht Berlin zur Höhe eines Schadensersatzanspruches im Falle der unbefugten Verwendung eines urheberrechtlich geschützten Fotos

von Clara Ochsenfeld

Für die Berechnung der Höhe eines Schadensersatzanspruchs nach den Grundsätzen der sogenannten Lizenzanalogie hat das Landgericht Berlin (LG Berlin) in seinem Urteil vom 30.07.2015 (Az.: 16 O 410/14) die Heranziehung der Vergütungstabelle der Mittelstandsvereinigung Fotomarketing (MFM-Tabelle) für das Foto eines professionellen Fotografen abgelehnt, da dieser seine Fotos in der Vergangenheit nicht tatsächlich am Markt angeboten hatte. Das Gericht hat damit den Rahmen für die Schätzung der Schadenshöhe erneut enger gesteckt und überhöhten fiktiven Lizenzgebühren eine Absage erteilt.

I. Schadensschätzung nach der Lizenzanalogie

Bei Urheberrechtsverletzungen jeglicher Art ist es in der Praxis häufig schwierig, die Schadenshöhe konkret zu beziffern. Für die Berechnung des dem Urheber aus der unberechtigten Bildverwendung entstandenen Schadens im Wege der Schadensschätzung, die das Gericht gem. § 287 Zivilprozessordnung (ZPO) vornimmt, stehen nach dem Urheberrechtsgesetz drei Methoden zur Verfügung, derer sich der Geschädigte zur Darlegung seines Schadens bedienen kann: Zum einen besteht die Möglichkeit, den konkret entstandenen Schaden (insbesondere den dem Geschädigten entgangenen Gewinn) zu ermitteln, darüber hinaus kann die Höhe auch anhand des Verletzergewinns bestimmt werden. Dies ist der Gewinn, den der Verletzer dadurch erlangt, dass er das geschützte Werk unerlaubt zum eigenen Vorteil nutzt. Als dritte Möglichkeit kommt die Bestimmung der Höhe über den Grundsatz der Lizenzanalogie in Betracht (§ 97 Abs. 2 Urheberrechtsgesetz (UrhG)). Danach kann der Anspruchsinhaber von dem Verletzer die Vergütung verlangen, die ihm bei ordnungsgemäßer Nutzungsrechtseinräumung gewährt worden wäre. Fingiert wird demnach der Abschluss eines Lizenzvertrages zu angemessenen Bedingungen. Letztere Methode ist zur Berechnung des Schadensersatzes im Urheberrecht am gebräuchlichsten. Ihr liegt die Überlegung zu Grunde, dass der Verletzer grundsätzlich nicht anders stehen soll als ein vertraglicher Lizenznehmer, der eine Lizenzgebühr entrichtet hätte.

Für diese Schadensschätzung nach der Methode der Lizenzanalogie hat die Rechtsprechung in der Vergangenheit oftmals die MFM-Tabelle als Referenzrahmen herangezogen, wenn es um die Arbeit eines professionellen Fotografen ging (z. B. OLG Brandenburg, Urt. v. 15.5.2009, Az.: 6 U 37/08O; LG Hamm, Urt. v. 13.2.2014, Az.: 22 U 98/13; AG München, Urt. v. 02.05.2014, Az.: 142 C 5827/14). Die bisher ergangenen Entscheidungen der Gerichte haben jedoch stets verdeutlicht, dass die Tabelle nicht pauschal und schematisch angewendet werden darf, sondern der Einzelfall Berücksichtigung finden muss. Die Heranziehung der MFM-Tabelle wurde demnach durch eine Vielzahl von Entscheidungen stark eingeschränkt.

Die MFM-Empfehlungen beruhen auf den Erfahrungswerten professioneller Marktteilnehmer wie z. B. Bildagenturen, Fotografen und Bildjournalisten (vgl. insoweit auch LG Düsseldorf, MMR 2013, S. 264). Aufgrund oftmals großer Qualitätsunterschiede zwischen professionellen Fotos eines Berufsfotografen und Bildern, die von Privatpersonen gemacht wurden, sowie der Tatsache, dass ein Berufsfotograf mit seinen erzielten Einnahmen auch seine Betriebsausgaben bestreiten muss, kann die Tabelle nach überwiegender Ansicht nur im Falle der Geltendmachung eines Schadensersatzes für professionelle Fotos herangezogen werden. Dies gilt jedoch nur insoweit, als auch der auf der anderen Seite stehende Erwerber gewerblich tätig ist und die Fotos nicht zu privaten Zwecken nutzt (z. B. OLG Braunschweig, Urt. v. 8.2.2012, Az.: 2 U 7/11).

Das Landgericht Berlin hat nun darüber hinaus die Schätzung unter Heranziehung der MFM-Tabelle auch für einen Fall abgelehnt, in dem die Voraussetzungen des gewerblichen Handelns auf beiden Seiten gegeben waren. Begründet wurde dies damit, dass der klagende Berufsfotograf nicht über eine entsprechende Lizenzpraxis verfügte. Das Gericht ging davon aus, dass die Honorarempfehlungen der Tabelle nicht die tatsächlichen Marktverhältnisse widerspiegelten. Die Schadenshöhe solle sich nur dann an die Empfehlungen der MFM-Tabelle anlehnen, wenn der den Anspruch geltend machende Fotograf diese Preise auch tatsächlich am Markt erzielt und dies entsprechend darlegt.

II. Argumentation des Landgerichts

Der Entscheidung des LG Berlin lag folgender Sachverhalt zugrunde. Die Beklagte verwendete für ihren Internetauftritt ein vom Kläger geschaffenes, von ihr anschließend leicht bearbeitetes Foto, ohne dass der Kläger ihr die entsprechenden Rechte hierfür eingeräumt hatte. Der Kläger, ein Berufsfotograf, der vornehmlich für eine GmbH arbeitet(e), deren Gesellschafter er auch ist, verklagte sie deshalb auf Unterlassung und Schadensersatz. Für die Höhe seiner Schadensersatzforderung stützte er sich auf die Berechnung nach der MFM-Tabelle, wonach sich eine fiktive Lizenzgebühr von 697,50 Euro ergab. Er war der Ansicht, dass die MFM-Tabelle auch dann gelten müsse, wenn er keine eigene Lizenzierungspraxis verfolge. Darüber hinaus sei der geforderte Betrag um 100% zu erhöhen, da die Beklagte ihn auf ihrer Internetseite nicht als Urheber der Fotografie genannt hatte.

Das Gericht gab der Klage im Hinblick auf die Schadensersatzforderung nur teilweise statt. Zwar sah es die Voraussetzungen für einen Schadensersatz nach § 97 Abs. 2 UrhG dem Grunde nach als gegeben an. Es war allerdings der Ansicht, dass die MFM-Empfehlungen aufgrund der fehlenden Lizenzierungspraxis des Klägers „schon im Ansatz nicht mehr zur Bestimmung der „angemessenen“ Lizenzgebühr zugrunde gelegt werden können“. Vielmehr schätzte das Gericht gem. § 287 ZPO wegen mangelnder anderweitiger Anhaltspunkte den Betrag auf einen (absoluten) Mindestschaden von lediglich 100 Euro, welcher wegen der fehlenden Urheberbenennung durch den Beklagten um 100% (demnach 100 Euro) zu erhöhen war. Das Gericht verdeutlichte in seiner Urteilsbegründung, dass der Schadensersatzanspruch des § 97 Abs. 2 UrhG den Verletzten grundsätzlich nicht besser stellen solle, als er ohne die Rechtsverletzung des Beklagten gestanden hätte. Die MFM-Empfehlungen bilden ihrem eigenen Anspruch nach eine marktgerechte – und nur insoweit „angemessene“ – Lizenzierungspraxis der tatsächlich am Markt tätigen Fotografen ab und sollen gerade nicht für den umgekehrten Fall gelten, in dem eine tatsächliche Praxis gar nicht besteht.

III. Empfehlung für die Hochschulen

Zunächst sollte jede Hochschule, die eine Webseite und/oder Social-Media Auftritte betreibt, sicherstellen, dass die Bilder, die sie öffentlich zugänglich macht, keine Urheberrechte Dritter verletzen. Auf „Nummer sicher“ geht man demnach nur, wenn man eigene Bilder verwendet oder sich die Bildrechte vertraglich zusichern lässt. Wichtig ist, dass sich insbesondere beim Ankauf von Bildlizenzen z. B. von Agenturen die Rechtekette zurückverfolgen lässt. Es ist demnach stets zu prüfen, ob der Vertragspartner auch tatsächlich Inhaber der Rechte ist. Die Rechtsprechung legt an diese Überprüfung strenge Maßstäbe an. Wer beispielsweise eine fremde Fotografie auf seiner Webseite veröffentlicht und sich lediglich die Rechteeinräumung von einer Agentur zusichern lässt, ohne etwaige Unterlagen zu überprüfen, kann sich dem Vorwurf der Fahrlässigkeit ausgesetzt sehen und macht sich unter Umständen schadensersatzpflichtig (vgl. zuletzt OLG München, Beschluss v. 15.1.2015, Az.: 29 W 2554/14). Darüber hinaus sollte darauf geachtet werden, dass im Zusammenhang mit der Veröffentlichung der Bilder stets auch der Name des Fotografen genannt wird. Hiervon kann nur abgewichen werden, wenn der Fotograf vertraglich explizit auf sein Namensnennungsrecht verzichtet hat.

Für den Fall, dass eine Hochschule das Urheberrecht oder Leistungsschutzrecht eines Dritten verletzt hat und der Dritte nun Schadensersatz- und Unterlassungsansprüche gegenüber der Hochschule geltend macht, ist stets eine genaue Prüfung der Ansprüche erforderlich. Insbesondere sollte vor einer etwaigen Anerkennung der Ansprüche, die Darlegung der Höhe des vom Verletzten geltend gemachten Schadensersatzes kontrolliert werden. Die Hochschulen sollten in diesen Fällen immer ihre Rechtsabteilung zu Rate ziehen, die die Ansprüche auf ihre Voraussetzungen hin überprüfen kann. Insbesondere sollte, sofern tatsächlich von einer Verletzung ausgegangen werden kann, die Höhe des geltend gemachten Schadensersatzanspruchs und dessen Darlegung einer genauen Kontrolle unterzogen werden. Oftmals legen Verletzte bereits bei der Geltendmachung ihrer Ansprüche im Falle einer vorgerichtlichen Abmahnung einen überhöhten Streitgegenstandswert

für die Berechnung der Abmahnkosten zugrunde, indem sie ihren Schadensersatzanspruch auf überhöhte Lizenzgebühren stützen, die einer tatsächlichen Grundlage entbehren. Bezieht sich die Höhe des Schadensersatzanspruchs auf eine Vergütung nach der MFM-Tabelle, sollte unbedingt für den konkreten Fall geprüft werden, ob es sich bei den streitgegenständlichen Bildern um professionelle Aufnahmen handelt, und ob der Anspruchssteller seine Bilder tatsächlich auch am freien Markt anbietet und hierfür Preise, die den Maßstäben der MFM-Tabelle entsprechen, erzielt.

Hinweis:

Zum Thema Verhalten bei Abmahnungen, siehe Handlungsempfehlungen: https://www.dfn.de/fileadmin/3Beratung/Recht/handlungsempfehlungen/Was_tun_bei_Abmahnungen.pdf

Das Schweigen der Forscher

OVG NRW verneint Pflicht einer Hochschule zur Offenlegung einer Forschungsvereinbarung mit einem Drittmittelgeber

von Florian Klein

Das Informationsfreiheitsrecht eröffnet Bürgern die Möglichkeit, von Behörden Auskünfte über amtliche Vorgänge zu erhalten. Dabei kommt es häufig vor, dass die zuständige Stelle die entsprechenden Informationen aus verschiedensten Gründen nicht herausgeben möchte. In diesen Fällen ist zu klären, ob einer der gesetzlichen Ausschlussgründe eingreift, der eine solche Verweigerung der Informationserteilung legitimiert. Im Hinblick auf eine Forschungsvereinbarung zwischen einer nordrhein-westfälischen Universität und einem großen Pharmaunternehmen hat das Oberverwaltungsgericht NRW nun mit Urteil vom 18.8.2015 (Az. 15 A 97/13) entschieden, dass diese in Gänze dem Bereich der Forschung zuzuordnen ist, für den das Informationsfreiheitsgesetz NRW aufgrund einer Bereichsausnahme gar nicht anwendbar ist.

I. Hintergrund und Rechtslage

In einem demokratischen Staat obliegt es der Verwaltung, gegenüber dem Souverän, dem Volk, Rechenschaft abzulegen. Eine größtmögliche Transparenz des staatlichen Handelns ermöglicht den Bürgern eine Kontrolle der Exekutive und macht ihre Entscheidungen für die Bürger nachvollziehbarer, was zugleich Akzeptanz schafft. Aus diesem Grund sind in den letzten Jahren auf Bundesebene und in einigen Bundesländern Informationsfreiheitsgesetze geschaffen worden, die allen Bürgern grundsätzlich freien Zugang zu den bei den öffentlichen Stellen vorhandenen Informationen gewährleisten und die die Voraussetzungen festlegen, unter denen derartige Informationen zugänglich gemacht werden sollen. Während das Informationsfreiheitsgesetz des Bundes die Informationszugangsansprüche gegenüber Bundesbehörden regelt, gelten die jeweiligen Landesgesetze für die öffentlichen Stellen der Länder, zu denen auch die Hochschulen gehören. Auf Landesebene gibt es Informationsfreiheitsgesetze bislang in elf der sechzehn Bundesländer. Die Länder ohne Informationsfreiheitsgesetz sind Bayern, Baden-Württemberg, Hessen, Niedersachsen und Sachsen. Insofern müssen bei der Gesetzesanwendung unbedingt die Besonderheiten der jeweiligen Landesgesetze berücksichtigt werden, auch wenn es zahlreiche gleichartige Regelungen gibt. Am Beispiel des Informationsfreiheitsgesetzes des Landes NRW (IFG NRW), welches dem oben angesprochenen Urteil zu Grunde liegt, werden die Grundzüge des Zugangsanspruches dargelegt und die sogenannte Bereichsausnahme für die Forschung erläutert.

Der Anspruch auf Zugang steht (nur) jeder natürlichen Person zu, sodass juristische Personen nicht anspruchsberechtigt sind, und kann sich nahezu gegen jede öffentliche Stelle des Landes NRW richten, die Verwaltungstätigkeiten ausübt. Natürliche oder juristische Personen des Privatrechts können nur ausnahmsweise Anspruchsgegner für Ansprüche nach dem Informationsfreiheitsrecht sein, wenn sie öffentlich-rechtliche Aufgaben wahrnehmen. Inhaltlich ist der Anspruch auf Zugang zu den bei diesen Stellen vorhandenen amtlichen Informationen gerichtet (§ 4 IFG NRW). Nach § 3 IFG NRW sind unter „Informationen“ in diesem Sinne alle Informationen zu verstehen, die in Schrift-, Bild-, Ton- oder Datenverarbeitungsform oder auf sonstigen Informationsträgern vorhanden sind, sofern sie im dienstlichen Zusammenhang erlangt wurden. Informationsträger sind dabei alle Medien, die Informationen in Schrift-, Bild-, Ton- oder Datenverarbeitungsform oder in sonstiger Form speichern können. Davon umfasst sind beispielsweise DVDs, Festplatten, Fotos oder herkömmliche Akten.

Da der Zugang aber nur zu solchen Informationen verschafft werden muss, die bei der jeweiligen Stelle bereits vorhanden

sind, trifft sie keine Verpflichtung, nicht vorhandene Informationen erst zu beschaffen oder solche, die schon vernichtet oder archiviert wurden, wiederherzustellen. Unerheblich ist dabei, ob die Behörde aufgrund der ihr zugewiesenen Zuständigkeiten eigentlich über die angefragten Informationen verfügen müsste, um ihre Aufgaben erledigen zu können.

Die Beschränkung auf amtliche Informationen bezweckt indes vorwiegend, gegebenenfalls vorhandene private Unterlagen von dem Anspruch auszuschließen. Im Übrigen ist noch zu beachten, dass besondere Rechtsvorschriften über den Zugang zu amtlichen Informationen, die Auskunftserteilung oder die Gewährung von Akteneinsicht den allgemeinen Vorschriften des IFG NRW gem. § 4 Abs. 2 S. 1 IFG NRW vorgehen. Darüber hinaus regelt § 5 IFG NRW detailliert das Verfahren, das bei der Geltendmachung des Anspruchs einzuhalten ist. Dazu gehört beispielsweise die Tatsache, dass Zugang nur auf Antrag gewährt wird und dass dies unverzüglich, aber spätestens innerhalb eines Monats nach Antragstellung erfolgen soll. Außerdem kann der Antrag abgelehnt werden, wenn die angefragte Information dem Antragsteller schon zur Verfügung gestellt wurde oder wenn sich der Antragsteller die Informationen in zumutbarer Weise aus allgemein zugänglichen Quellen beschaffen kann.

Schließlich finden sich in den §§ 6-9 IFG NRW näher bezeichnete Ablehnungsgründe, bei deren Vorliegen eine Informationserteilung nicht stattfinden darf. Dabei geht es vor allem um den Schutz öffentlicher Belange und der Rechtsdurchsetzung, den Schutz des behördlichen Entscheidungsprozesses, den Schutz von Betriebs- und Geschäftsgeheimnissen und den Schutz personenbezogener Daten.

Für staatliche Hochschulen als öffentliche Stellen des Landes (meist in der Rechtsform einer Körperschaft des öffentlichen Rechts) und sonstige staatliche Forschungseinrichtungen ist § 2 Abs. 3 IFG NRW von besonderer Bedeutung. Dieser enthält nämlich eine sogenannte Bereichsausnahme und legt fest, dass das IFG NRW für Forschungseinrichtungen, Hochschulen und Prüfungseinrichtungen nur gilt, soweit sie nicht im Bereich von Forschung, Lehre, Leistungsbeurteilungen und Prüfungen tätig werden. Soweit diese Tätigkeitsbereiche betroffen sind, ist das IFG NRW also von vornherein gar nicht anwendbar, sodass es keine Pflicht gibt, diesbezügliche Anträge positiv zu bescheiden.

II. Die Entscheidung des Gerichts

Wie weit diese Bereichsausnahme für die Forschung im Einzelfall reicht, hatte kürzlich das Oberverwaltungsgericht für das Land Nordrhein-Westfalen (OVG NRW) in einem Rechtsstreit zwischen einem Bürger und einer nordrhein-westfälischen Universität zu entscheiden.

1. Sachverhalt

Der Kläger, Geschäftsführer eines Vereins gegen chemische Gefahren, hatte von der beklagten Universität unter Berufung auf das IFG NRW verlangt, zum einen eine Rahmenvereinbarung offenzulegen, die ihre Universitätsklinik mit einem Pharmaunternehmen als Drittmittelgeber geschlossen hatte, und zum anderen bestimmte zusätzlich gestellte Fragen dazu zu beantworten. Gegenstand der Rahmenvereinbarung war ein Kooperationsvertrag, mit dem die Vertragspartner die Voraussetzungen für eine bevorzugte Partnerschaft im Bereich der Forschung und Entwicklung innovativer Therapien schaffen wollten, um entsprechende Forschungs- und Entwicklungsvorhaben auf bestimmten, im Vertrag benannten medizinischen Gebieten gemeinsam auszuwählen und durchzuführen. Die Universität hatte sich geweigert, diesen Kooperationsvertrag offenzulegen und sich dabei auf die Bereichsausnahme für Forschung berufen, sowie darlegt, dass zudem im Vertrag enthaltene Betriebs- und Geschäftsgeheimnisse einer Herausgabe entgegenstünden. Zu deren Schutz seien im Vertrag auch Verschwiegenheitsklauseln enthalten. Dennoch hatte die Universität aufgrund des öffentlichen Interesses und der vorangegangenen medialen Berichterstattung detailliert Auskunft über die Bestandteile und inhaltlichen Aspekte des Vertragswerks gegeben. Insofern gehörten zu dem Vertrag – wie für Drittmittelverträge üblich – Regelungen über sachliche und organisatorische Beiträge zur Findung und Durchführung von Einzelprojekten, Aufbau eines Graduiertenkollegs, finanzielle Kompensation einzelner Leistungen, Umgang mit Ergebnissen und Verteilung der Nutzungsrechte, Vertraulichkeit, Exklusivität der Kooperation in den Einzelprojekten, Verfahren bei der wissenschaftlichen Veröffentlichung aus Einzelprojekten, Haftung, Laufzeit und vertragstechnische Formalia.

Diese Auskünfte reichten dem Kläger jedoch nicht aus, der weiterhin die vollständige Offenlegung der Rahmenvereinbarung forderte, sodass das Verfahren nach Klageabweisung in der ersten Instanz das OVG NRW als Berufungsinstanz erreichte.

2. Urteil

Die Berufung des Klägers wurde vor dem OVG NRW indes als unbegründet zurückgewiesen. Der Kläger sei zwar grundsätzlich als natürliche Person anspruchsberechtigt, allerdings unterfalle die streitgegenständliche Rahmenvereinbarung der Bereichsausnahme für Forschung und Lehre. Darüber hinaus sei die Ablehnung des Auskunftsgesuchs auch deshalb zu Recht erfolgt, weil einzelne Regelungen der Vereinbarung Betriebs- und Geschäftsgeheimnisse des Pharmaunternehmens im Sinne von § 8 S. 1 IFG NRW enthielten.

Zu diesem Ergebnis kommt das Gericht nach intensiver Auseinandersetzung mit den Begriffen Forschung und Lehre im Sinne der Bereichsausnahme des Paragraphen § 2 Abs. 3 IFG NRW. Zugrunde zu legen sei das entsprechende verfassungsrechtliche Begriffsverständnis der Wissenschaftsfreiheit aus Art. 5 Abs. 3 Grundgesetz (GG), da der Zugang zu amtlichen Informationen nicht dazu führen solle, die Grundrechtspositionen von Wissenschaft und Forschung zu gefährden. Die Wissenschaftsfreiheit schütze als Abwehrrecht die freie wissenschaftliche Betätigung vor staatlichen Eingriffen und verpflichte den Staat zugleich zu ihrem Schutz und ihrer Förderung. Die Wissenschaft sei grundsätzlich ein von Fremdbestimmung freier Bereich, da sie dem Staat und der Gesellschaft nur dann bestmöglich dienen könne, wenn gesellschaftliche Nützlichkeits- und politische Zweckmäßigkeitsvorstellungen außen vor blieben.

Forschung sei dabei ein Unterfall der Wissenschaft und meine jede geistige Tätigkeit mit dem Ziel, in methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen. Dabei darf dieser Begriff nicht zu eng verstanden werden, so dass bei Einhaltung der Kriterien der Wissenschaftlichkeit und der Arbeit mit wissenschaftlichen Methoden auch die Zweck- oder Auftragsforschung zur geschützten Forschung gehöre, unabhängig davon, ob Private oder der Staat dahinter stehen und ob dies an Universitäten oder außerhalb davon geschieht.

Dem von der Forschungsfreiheit geschützten Bereich ordnet das Gericht sowohl die Fragestellung und die Grundsätze der Methodik als auch die Bewertung des Forschungsergebnisses und seine Verbreitung zu. Für den Kernbereich der wissenschaftlichen Betätigung müsse die freie Selbstbestimmung des einzelnen Grundrechtsträgers gewährleistet sein, was staatliche Eingriffe insoweit ausschließe. Ergänzend müsse der Staat organisatorische Maßnahmen zum Schutz der wissenschaftlichen Betätigung ergreifen. Deshalb sei die Gestaltungsfreiheit des Gesetzgebers im Bereich der Angelegenheiten, die Forschung und Lehre unmittelbar berühren, der sogenannten „wissenschaftsrelevanten“ Angelegenheiten, durch das Grundrecht der Wissenschaftsfreiheit begrenzt. Darin einbezogen sind alle Aktivitäten der Forschung mit allen vorbereitenden und unterstützenden Tätigkeiten. Nach diesen allgemeinen Ausführungen zum Begriffsverständnis von Wissenschaft und Forschung folgt eine umfangreiche Aufzählung solcher wissenschaftsrelevanter Tätigkeiten, bei welcher sich die Richter an einer Entscheidung des Bundesverfassungsgerichts aus dem Jahr 1973 orientiert haben und die hier zur Erleichterung der Bestimmung der Reichweite des Forschungsbegriffes im Wortlaut wiedergegeben werden soll:

„Dazu zählen insbesondere die Planung wissenschaftlicher Vorhaben, d. h. die Forschungsplanung, das Aufstellen von Lehrprogrammen und die Planung des Lehrangebotes, die Koordinierung der wissenschaftlichen Arbeit, also das Abstimmen der Forschungsvorhaben und der Lehrangebote aufeinander, die Harmonisierung der Lehraufgaben mit den Forschungsvorhaben, ferner die organisatorische Betreuung und Sicherung der Durchführung von Forschungsvorhaben und Lehrveranstaltungen, insbesondere ihre haushaltsmäßige Betreuung einschließlich der Mittelvergabe, die Errichtung und der Einsatz von wissenschaftlichen Einrichtungen und Arbeitsgruppen, die Festsetzung der Beteiligungsverhältnisse bei wissenschaftlichen Gemeinschaftsaufgaben, die Festlegung und Durchführung von Studien- und Prüfungsordnungen. Schließlich sind hierher auch die Personalentscheidungen in Angelegenheiten der Hochschullehrer und ihrer wissenschaftlichen Mitarbeiter zu rechnen.“ (OVG NRW, Urt. v. 18.8.2015 – 15 A 97/13, Rz. 53)

Unter Heranziehung dieses Begriffsverständnisses der Forschung ordnet das Gericht den streitgegenständlichen Rahmenvertrag mit den geschilderten Inhalten dem Bereich von Forschung und Lehre und damit der Bereichsausnahme des § 2 Abs. 3 IFG NRW zu, weil er unmittelbar wissenschaftsrelevante Angelegenheiten regle. Obwohl der Rahmenvertrag gerade nicht einzelne Forschungsprojekte auswählt, sondern dafür eine spätere Konkretisierung auf seiner Basis erforderlich ist, bleibt die Qualifizierung als unmittelbar wissenschaftsrelevant erhalten. Denn der Vertrag gebe schon verbindlich strukturell den Rahmen für das Ob und Wie der Durchführung und Auswertung von Forschungsprojekten vor und stelle damit eine unabdingbare organisatorische Grund-

entscheidung dar. Selbst die Nebenregelungen, zum Beispiel zu Laufzeit oder Kündigungsfrist, seien der Bereichsausnahme zuzuordnen, weil insoweit ein einheitliches Vertragswerk vorliege.

Auch dem Begehren, § 2 Abs. 3 IFG NRW einschränkend auszulegen und auf den absoluten Kernbereich der Forschung zu beschränken, erteilt das Gericht eine Absage. Schließlich stellt es noch fest, dass entgegen des klägerischen Vortrags keinerlei begründete Zweifel an der Verfassungsmäßigkeit von § 2 Abs. 3 IFG NRW bestünden. So ergebe sich aus der Informationsfreiheit nur ein Anspruch auf Zugang zu allgemein zugänglichen Informationsquellen, nicht aber auf Eröffnung einer solchen. Auch das Demokratieprinzip und der Gleichheitsgrundsatz seien nicht verletzt. Im Hinblick auf letzteren fehle es schon an einer Ungleichbehandlung vergleichbarer Personen und Sachverhalte, da § 2 Abs. 3 IFG NRW alle Normadressaten, die er betreffe, gleich behandle.

Obwohl damit feststand, dass der Anwendungsbereich des IFG NRW schon gar nicht eröffnet war, erörtert das Gericht noch zusätzlich, dass auf Basis von § 8 S. 1 IFG NRW eine Ablehnung des Anspruchs auch deshalb gerechtfertigt gewesen ist, weil die Rahmenvereinbarung Betriebs- und Geschäftsgeheimnisse des Pharmaunternehmens enthält. Diese Norm sieht nämlich vor, dass der Antrag auf Informationszugang abzulehnen ist, soweit durch die Übermittlung der Information ein Betriebs- oder Geschäftsgeheimnis offenbart wird und dadurch ein wirtschaftlicher Schaden entstehen würde.
Geschäftsgeheimnisse beträfen „den kaufmännischen Teil eines Gewerbebetriebes, der nur einem begrenzten Personenkreis bekannt ist und mit Blick auf die berechtigten wirtschaftlichen Interessen nach dem Willen des Unternehmers geheim gehalten werden soll. Hierzu zählen Preiskalkulationen, Bezugsquellen, Ertragslage, Kreditwürdigkeit, Geschäftsverbindungen, Marktstrategien sowie Kundenlisten“ (OVG NRW, Urt. v. 18.8.2015 – 15 A 97/13, Rz. 101). Ein wirtschaftlicher Schaden setzt voraus, dass die von der amtlichen Information betroffene Stelle konkret und substantiiert darlegt, dass die Offenbarung des Geheimnisses zu einer nachhaltigen Verschlechterung ihrer Wettbewerbssituation führen wird. Diese Voraussetzungen sah das Gericht als gegeben an, da aus der Rahmenvereinbarung Rückschlüsse auf die Marktstrategien sowie auf aktuelle und zukünftige Forschungsprojekte des Pharmaunternehmens gezogen werden könnten. Außerdem zeigten die Vertragskonditionen auf, unter welchen Bedingungen das Pharmaunternehmen zum Abschluss von Forschungskooperationen mit Universitäten bereit sei. Dadurch sei es Konkurrenten leicht möglich, die Marktstrategien zu durchkreuzen und bessere Vertragsbedingungen anzubieten, was zu einer Beeinträchtigung des Wettbewerbs um besonders qualifizierte Kooperationspartner führen würde. Daraus resultiere ein Schaden für die Forschungsarbeit, die Innovationsfähigkeit und die Marktbeständigkeit des Pharmaunternehmens, was im konkreten Fall weder durch Schwärzungen einzelner Zahlen abzuwenden noch durch ein überwiegendes Interesse der Allgemeinheit an dem Informationszugang (§ 8 Satz 3 IFG NRW) gerechtfertigt sei.

III. Fazit und Konsequenzen für die Hochschulpraxis

Das Urteil des OVG NRW zeigt deutlich, dass Hochschulen im Forschungsbereich weitgehend von Ansprüchen nach dem Informationsfreiheitsrecht befreit sind, solange das jeweilige Landesgesetz eine mit § 2 Abs. 3 IFG NRW vergleichbare Regelung enthält. Dies ist der Fall in Brandenburg (§ 2 Abs. 2 AIG), im Saarland (§ 1 Abs. 4 SIFG), in Sachsen-Anhalt (§ 3 Abs. 1 Nr. 9 IZG LSA) und in Thüringen (§ 2 Abs. 5 ThürlFG). In Hamburg besteht eine Ausnahme für Grundlagenforschung und anwendungsbezogene Forschung (§ 5 Nr. 7 HmbTG). In Bremen wird für die Veröffentlichung von Verträgen und Daten über Drittmittelforschung auf die Regelungen des Bremischen Hochschulgesetzes verwiesen.
Im Sinne des Grundrechts der Wissenschaftsfreiheit ist von einem weiten Begriffsverständnis von Wissenschaft und Forschung auszugehen, welches sich bei der Bestimmung wissenschaftsrelevanter Tätigkeiten niederschlägt. An dieser Stelle ist auf die oben zitierte Aufzählung des OVG NRW zu verweisen. Bezieht sich ein Informationszugangsgesuch auf solche Tätigkeiten, muss diesem nicht entsprochen werden. Für Hochschulen und Drittmittelgeber bringt dieses Urteil die Sicherheit mit sich, dass die Einzelheiten von Forschungskooperationen und entsprechende Vereinbarungen vor dem Einblick der Allgemeinheit geschützt sind. Dies gilt bei umfangreichen, einheitlichen Vertragswerken sogar für nicht unmittelbar wissenschaftsrelevante Nebenregelungen, auf die der Schutz gewissermaßen ausstrahlt. Auch die Bedeutung des Schutzes von Betriebs- und Geschäftsgeheimnissen wurde noch einmal hervorgehoben, der nur überwunden werden kann, wenn der durch die Offenle-

gung drohende wirtschaftliche Schaden ausnahmsweise nur geringfügig ist. Dies wiederum setzt voraus, dass der Informationszugang zum Schutz eindeutig höherrangiger Rechtsgüter der Allgemeinheit erforderlich ist. Die Ausführungen des Gerichts zu diesem Punkt sind insbesondere für Hochschulen in den Bundesländern von Interesse, in denen keine Bereichsausnahme für die Forschung besteht. Dies betrifft primär Berlin, Mecklenburg-Vorpommern, Rheinland-Pfalz und Schleswig-Holstein. Denn dort besteht nach dem jeweiligen Landesgesetz auch im Hinblick auf den Forschungsbereich grundsätzlich ein Informationszugangsanspruch, dessen Ablehnung dann auf andere Weise gerechtfertigt werden muss.

Ist den Hochschulen somit (in einigen Bundesländern) ein wirksames Instrument an die Hand gegeben, um ihre Forschungstätigkeiten auch bei Kooperationen mit Unternehmen der Privatwirtschaft unbehelligt von der Öffentlichkeit auszuüben, sollte dennoch erwogen werden, entsprechende Vereinbarungen zwecks Schaffung von Transparenz und Vertrauen auf freiwilliger Basis öffentlich zu machen, soweit Daten- und Geheimnisschutz oder andere Belange dem nicht entgegenstehen und ein öffentliches Interesse daran kundgetan wurde.

Unabhängig von Informationszugangsgesuchen von Bürgern ist zumindest in NRW aber unbedingt der relativ junge § 71a Hochschulgesetz NRW zu beachten, der dem Einzelnen zwar keine Ansprüche gewährt, aber eine objektive Informationspflicht der Hochschulen begründet. Demnach hat das Rektorat die Öffentlichkeit in geeigneter Weise über abgeschlossene, durch Drittmittel finanzierte Forschungsvorhaben zu informieren, wobei hinsichtlich personenbezogener Daten die Schutzvorschriften der §§ 9, 10 IFG NRW entsprechend anzuwenden sind. Im Übrigen muss eine solche Information der Öffentlichkeit unterbleiben, soweit durch die Übermittlung der Information ein Betriebs- oder Geschäftsgeheimnis offenbart wird und dadurch die Gefahr des Eintritts eines wirtschaftlichen Schadens entsteht. Dem Dritten ist dabei im Vorhinein Gelegenheit zur Stellungnahme zu geben. Schließlich gelten diese Grundsätze für Entwicklungsvorhaben und Vorhaben zur Förderung des Wissenstransfers entsprechend. Hieran zeigt sich, dass der nordrhein-westfälische Gesetzgeber die Bedeutung der Transparenz im Bereich der Drittmittelforschung nicht verkannt hat, auch wenn er nicht den Weg beschritten hat, die Transparenz durch eine Erweiterung des Informationsfreiheitsgesetzes zu stärken. Eine solche objektive Verpflichtung zur Information der Öffentlichkeit über Forschungstätigkeiten, insbesondere Drittmittelforschung, findet sich in unterschiedlichem Umfang auch in anderen Landeshochschulgesetzen. Insofern soll hier für die näheren Details für das jeweilige Bundesland auf die folgenden Regelungen verwiesen werden: in Bayern Art. 2 Abs. 6, 8 Abs. 2 BayHSchG; in Baden-Württemberg §§ 41, 41a LHG BW; in Berlin § 41 BerlHG; in Brandenburg §§ 3 Abs. 7, 36 Abs. 2 BbgHG; in Bremen § 75 BremHG; in Hamburg §§ 76-78 HmbHG; in Hessen §§ 12 Abs. 5, 29 Abs. 2 S. 2 HHG; in Mecklenburg-Vorpommern §§ 48, 49 LHG M-V; in Niedersachsen § 3 Abs. 1 S. 1 Nr. 10 NHG; in Rheinland-Pfalz §§ 2 Abs. 8, 14 Abs. 2 S. 2 HochSchG RPF; in Sachsen §§ 47, 48 SächsHSFG; in Sachsen-Anhalt §§ 24, 25 HSG LSA; im Saarland §§ 2 Abs. 10, 66 Abs. 2 UG SL; in Schleswig-Holstein §§ 3 Abs. 10, 37 Abs. 2 HSG SH; in Thüringen §§ 5 Abs. 9, 57 Abs. 3, 59 Abs. 2 ThürHG.

Weiterführende Hinweise:

- Zur Veröffentlichung von Mitarbeiterdaten im Internet nach den Informationsfreiheitsgesetzen der Länder siehe Overbeck, „Anderes Gesetz, neues Glück?“, in: DFN-Infobrief Recht 3/2014
- Allgemein zu Auskunftsansprüchen nach dem IFG: Handlungsempfehlung auf der Homepage des DFN-Vereins unter https://www.dfn.de/rechtimdfn/empfehlungen/handlungsempfehlungen/

Dein Name ist Programm

Warum Broadcast-Daten eine Gefahr für die Privatsphäre darstellen können und wie das Datenschutzrecht Anwendung auf den Umgang mit ihnen findet

von Hagen Sporleder

Broadcast-Daten, also Daten, die beispielsweise innerhalb eines lokalen Netzwerks von einem Nutzergerät automatisch und für alle anderen Nutzer sichtbar übermittelt werden, können unter Umständen eine Gefahr für die Privatsphäre des jeweiligen Nutzers darstellen, da sie mittelbar Aufschluss über seine Person und sein Verhalten geben können. Dies gilt insbesondere dann, wenn sie mit weiteren Daten kombiniert oder abgeglichen werden.
In rechtlicher Hinsicht stellen Broadcast-Daten unter bestimmten Voraussetzungen personenbezogene Daten im Sinne des Datenschutzrechts dar. Deshalb finden die Datenschutzgesetze der Länder oder das Bundesdatenschutzgesetz gegebenenfalls Anwendung auf ihre Erhebung und Speicherung. Aus diesem Grund ergeben sich einerseits ein gewisser Schutz für die Nutzer und andererseits rechtliche Pflichten für denjenigen, der mit Broadcast-Daten arbeitet.

I. Hintergrund

Broadcast-Daten zeichnen sich dadurch aus, dass sie bei ihrer Übertragung innerhalb eines Computernetzwerks nicht nur von einem bestimmten Nutzer, sondern von allen Nutzern innerhalb der Broadcast-Domain abgerufen und analysiert werden können. Im Hinblick darauf, dass der Broadcast häufig lediglich Informationen wie MAC- und IP-Adressen enthält, erscheint diese technisch bedingte Transparenz zunächst unbedenklich. Schließlich können Dritte mit diesen Informationen keine direkten Schlüsse zu natürlichen Personen ziehen.
Da die Broadcast-Übermittlung aktuell eine Renaissance feiert und in beliebten Programmen wie Dropbox, Spotify oder BitTorrent zur Anwendung kommt, ergibt sich neuerdings jedoch ein anderes Bild. Unter Umständen können die mit dem Broadcast übermittelten Daten nämlich sehr wohl Aufschluss über den hinter einem Gerät stehenden Nutzer geben. Das folgt unter anderem daraus, dass viele Nutzer dazu tendieren, ihr Gerät, mit dem sie zum Beispiel in einem WLAN angemeldet sind, nach sich selbst zu benennen. Dann taucht im Broadcast gegebenenfalls der Hostname „Macbook von Max Mustermann“ auf. Schon für sich genommen gibt dieses Datum einiges an Informationen über den Nutzer preis, nämlich seinen Namen, die Sprache, die er spricht und welches Gerät er nutzt. Zudem können die Einwahlzeitpunkte und -orte in Korrelation mit den Broadcast-Daten gebracht werden und so weitere Informationen über den Nutzer und sein Verhalten enthüllen.

II. Rechtliche Betrachtung

Die Anwendbarkeit der Datenschutzgesetze der Länder (LDSG) oder des Bundesdatenschutzgesetzes (BDSG) hängt zunächst davon ab, ob es sich bei den Broadcast-Daten um personenbezogene Daten handelt. Personenbezogene Daten sind Einzelangaben, die sich auf eine bestimmte natürliche Person beziehen oder die geeignet sind, einen Bezug zu ihr herzustellen. Hierzu gehören beispielsweise Name, Geburtsdatum, Adressen, Telefonnummern, Familienstände und auch den Inhaber benennende E-Mail-Adressen. Die Broadcast-Daten stellen demnach personenbezogene Daten dar, sofern mit ihnen ein Bezug zu bestimmten Personen hergestellt werden kann. Das ist wiederum der Fall, wenn Personen, ohne weitere Identifikationsmerkmale, klar zu erkennen sind. Zur Identifikation kann dabei bereits der Name ausreichen, wenn aufgrund des objektiven Zusammenhangs feststeht, dass die Daten nur

einen bestimmten Personenkreis betreffen. Genau dieser Fall liegt vor, wenn sich Hostnames, wie oben beschrieben, von den Namen natürlicher Personen ableiten. Da der Personenkreis in einem lokalen Netzwerk nämlich begrenzt ist, ergibt sich das Vorliegen personenbezogener Daten jedenfalls in Form der Gerätenamen. Abgesehen davon reicht es für die Bestimmbarkeit unter Umständen auch aus, dass bestimmte Personen mittelbar erkennbar sind. Das trifft zu, wenn etwa mittels bei der speichernden Stelle verfügbaren Zusatzwissens ein Rückschluss auf eine konkrete Person möglich ist und so eine Individualisierung vorgenommen werden kann. Insofern bestehen im Broadcast möglicherweise nicht nur in Form der abgeleiteten Gerätenamen personenbezogene Daten.

Für Universitäten und Forschungseinrichtungen ergeben sich aufgrund der rechtlichen Klassifizierung der Broadcast-Daten datenschutzrechtliche Probleme, wenn etwa der Broadcast in einem lokalen Netzwerk aufgezeichnet und analysiert werden soll. Da es sich bei Universitäten in aller Regel um öffentliche Einrichtungen handelt, gelten für sie die jeweiligen Landesdatenschutzgesetze. Sowohl diese als auch das BDSG erlauben die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur, sofern eine Einwilligung seitens des Betroffenen vorliegt oder eine Norm die Erhebung, Verarbeitung und Nutzung gestattet (vergleiche § 4 Abs. 1 BDSG und beispielsweise § 4 Abs. 1 LDSG NRW, § 6 Abs. 1 LDSG Berlin und Art. 15 Abs. 1 LDSG Bayern.)

Eine Rechtsnorm, die die Erhebung gestattet und die Einholung der Einwilligung entbehrlich macht, kann in Form von § 13 Abs. 1 BDSG oder im Fall von Universitäten beispielsweise in §§ 12 Abs. 1, 13 Abs. 1 LDSG NRW oder Art. 16 Abs. 1 BayDSG bestehen. Diese Normen erlauben die Erhebung bzw. Speicherung, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist. Sind einer Stelle Forschungsaufgaben übertragen worden, so wird sie grundsätzlich nämlich auch zu diesem Zweck Daten erheben und speichern dürfen. Dabei ist aber zu berücksichtigen, dass zwischen dem aus Art. 2 Abs. 1 iVm Art. 1 Abs. 1 Grundgesetz (GG) abgeleiteten Recht auf informationelle Selbstbestimmung, welches durch das Datenschutzrecht einfachgesetzlich abgesichert wird, und der ebenfalls grundgesetzlich geschützten Wissenschaftsfreiheit (Art. 5 Abs. 3 GG) ein Spannungsverhältnis besteht, das es aufzulösen gilt. Aus diesem Grund kann man nicht bei jedem beliebigen Forschungsvorhaben annehmen, dass es das Interesse des Betroffenen auf Geheimhaltung seiner Daten überwiegt. Daher wird gefordert, dass das Vorhaben einen engen Bezug zu einem bedeutenden Allgemeininteresse haben muss. (vgl. Oberlandesgericht Hamm NJW 1996 S. 940, 941). Wann ein solcher Bezug vorliegt, kann nur das Ergebnis einer Einzelfallentscheidung sein. Im Fall der Forschung mit Broadcast-Daten kann ein Allgemeininteresse jedenfalls dann bejaht werden, wenn das Vorhaben dem Zweck dient, auf die mögliche Sensibilität der Daten und die Gefahren für die Privatsphäre aufmerksam zu machen. Denn eine derart motivierte Forschung fördert letztendlich das Recht auf informationelle Selbstbestimmung.

Selbst wenn man ein überwiegendes Forschungsinteresse bejaht, ist der sogenannte Direkterhebungsgrundsatz zu berücksichtigen. Dieser fordert, dass grundsätzlich eine Mitwirkung des Betroffenen (gegebenenfalls passiv in Form einer Duldung) stattzufinden hat. Eine Erhebung darf demnach grundsätzlich nicht heimlich erfolgen, sondern muss mindestens mit einem Hinweis auf die Erhebung und ihren Zweck verbunden sein. Ausnahmen hiervon gibt es etwa in Bayern in Form von Art. 16 Abs. 2 S. 1 LDSG wonach Daten, die aus allgemein zugänglichen Quellen stammen, auch ohne Kenntnis erhoben werden dürfen. Da hiermit eine Quelle gemeint ist, die einerseits technisch geeignet, andererseits aber auch bestimmt sein muss, der Allgemeinheit Auskunft zu geben, fällt ein lokales Netzwerk trotz seiner freien Zugänglichkeit nicht unter diesen Begriff. Schließlich dient beispielsweise ein WLAN nicht dazu, Informationen über die anderen Nutzer in Form des Broadcasts bereitzustellen, sondern dazu, den Zugang zum Internet zu ermöglichen.

Weitere Ausnahmen vom Direkterhebungsgrundsatz finden sich in § 4 Abs. 2 S. 2 Nr. 1, 2 BDSG oder etwa in Art. 16 Abs. 2 S. 3 i.V.m. S. 2 Nr. 1 und 2 lit. a LDSG Bayern. Nach diesen Normen kann die Mitwirkung bzw. In-Kenntnis-Setzung entfallen, wenn eine Norm dies anordnet, es zur Erfüllung von Verwaltungsaufgaben erforderlich ist oder einen unverhältnismäßigen Aufwand bedeuten würde. Da im Fall der Erhebung von Broadcast-Daten zu Forschungszwecken aber weder eine die heimliche Erhebung gestattende Rechtsnorm besteht, noch eine Verwaltungsaufgabe vorliegt, kommt nur die Ausnahme wegen unverhältnismäßigen Aufwandes in Betracht. Diese ist wiederum zwar im BDSG angelegt, fehlt aber in den meisten Landesdatenschutzgesetzen, so dass die Ausnahme für die Universitäten häufig nicht gilt. Zudem ist der Zeit-, Arbeits-, und Kostenaufwand, den eine Hinweiserteilung auf die Broadcast-Datenerhebung zu Forschungszwecken bedeuten würde, als relativ gering einzuschätzen und wird sich bei Abwägung mit den schutzwürdigen Interessen der Nutzer an ihren Daten kaum als unverhältnismäßig darstellen. Im Ergebnis dürften

Universitäten und Forschungseinrichtungen deswegen jedenfalls nicht um eine Hinweiserteilung herum kommen.

III. Konsequenz und Fazit

Auch wenn der Broadcast technisch bedingt frei verfügbar ist, dürfen Universitäten und Forschungseinrichtungen ihn nicht ohne Weiteres speichern und auswerten. Grundsätzlich bedarf es einer Einwilligung eines jeden Nutzers, der sich im lokalen Netzwerk aufhält und damit bei Speicherung des Broadcasts im datenschutzrechtlichen Sinne betroffen werden kann.
Steht hinter der Speicherung und Analyse ein das Interesse des Betroffenen überwiegendes Forschungsinteresse, kann eine Einwilligung entbehrlich sein. Dieses muss als Ergebnis einer Abwägung im Einzelfall ermittelt werden. Auch wenn man im Ergebnis zu einem Überwiegen des Forschungsinteresses gelangt, müssen die Nutzer des lokalen Netzwerks in aller Regel über die Erhebung oder Speicherung in Kenntnis gesetzt werden. Dabei sind die Vorschriften der jeweiligen Landesdatenschutzgesetze zu beachten.
Weiterhin gelten bestimmte Anforderungen für die Behandlung der zu Forschungszwecken erhobenen Daten. Zum einen gilt eine Zweckbindung, wonach die zur Forschung erhobenen Daten nur für wissenschaftliche Zwecke verarbeitet oder genutzt werden dürfen (vergleiche § 40 Abs. 1 BDSG oder etwa § 33 Abs. 3 LDSG Hessen und Art. 23 Abs. 1 LDSG Bayern). Voraussetzung ist zum anderen, dass die personenbezogenen Daten anonymisiert werden, sobald dies nach dem Forschungszweck möglich ist (§ 40 Abs. 2 S. 1 BDSG oder zum Beispiel § 28 Abs. 1, 3 LDSG NRW, § 30 Abs. 2 LDSG Berlin und Art. 23 Abs. 3 LDSG Bayern). Solange noch keine Anonymisierung stattgefunden hat, sind einzelne Merkmale, die jeweils Aufschluss über eine bestimmte Person geben können, gesondert voneinander zu speichern. Sollten also mehrere Merkmale zu einer bestimmten Person im Broadcast erhoben werden, müssten diese getrennt voneinander gespeichert werden.

Kein sicherer Hafen für die Daten?

Urteil des EuGH zur Ungültigkeit des Safe-Harbor-Abkommens

von Lennart Sydow

Der Europäische Gerichtshof (EuGH) hat in seinem Urteil vom 6. Oktober 2015 in der Rechtssache C-362/14 die Ungültigkeit des Safe-Harbor-Abkommens festgestellt. Durch diese Entscheidung entfällt eine wichtige Möglichkeit der Legitimation der Datenübermittlung aus Mitgliedsstaaten der Europäischen Union in die USA, was gegebenenfalls Unternehmen sowie Hochschulen und Forschungseinrichtungen zur Anpassung ihrer Datenverarbeitungsprozesse zwingen kann.

I. Ausgangssituation

Die Übermittlung von Daten in die USA kann derzeit wohl als das meist diskutierte Problem im europäischen Datenschutzrecht bezeichnet werden. Die praktische Relevanz dieses Themas ergibt sich für öffentliche Stellen dabei weniger aus dem Erfordernis zur bewussten Weitergabe von personenbezogenen Daten an amerikanische Unternehmen, um diesen die weitere Verwendung der Daten zu ermöglichen, sondern immer öfter daraus, dass während der Verarbeitung personenbezogener Daten durch eine Stelle im Inland Infrastruktur und Dienste amerikanischer Unternehmen eingesetzt werden. Für Hochschulen und Forschungseinrichtungen der Länder sind dabei die jeweiligen Landesdatenschutzgesetze zu beachten. Diese enthalten bezüglich der Datenübermittlung in Drittstaaten inhaltsgleiche Vorschriften wie das hier beispielhaft angeführte Datenschutzgesetz Nordrhein Westfalen (DSG NRW).

Eine Übermittlung im Sinne des Datenschutzrechts liegt vor, wenn personenbezogene Daten einer externen Stelle bekanntgegeben werden, was durch eine Weitergabe der Daten oder ein Bereithalten zur Einsichtnahme auf Abruf erfolgen kann (vgl. § 3 Abs. 2 Nr. 4 DSG NRW). Für eine Übermittlung reicht daher schon aus, dass der Dritte faktisch die Möglichkeit hat, Kenntnis von den Inhalten der Daten zu nehmen (siehe insbesondere für den Fall der automatischen E-Mail-Weiterleitung dazu ausführlich: Klein, „Was lange währt… muss nicht immer gut sein – Teil 1. Rechtliche Probleme bei dem Angebot und der Nutzung einer automatischen E-Mail-Weiterleitung an Hochschulen“, in: DFN-Infobrief Recht 6/2015). Dies kann beispielsweise bei der Speicherung von Daten auf Cloud-Servern (wie z. B. Google Drive, Dropbox oder OneDrive) oder dem Einsatz von „Software as a Service“-Anwendungen der Fall sein. Eine faktische Zugriffsmöglichkeit des Anbieters ist sowohl bei Cloud-Speicherdiensten als auch bei der Verwendung von cloudbasierten Softwareanwendungen regelmäßig vorhanden.

Solch eine Übermittlung von Daten an eine andere private Stelle ist nur in den gesetzlich ausdrücklich erlaubten Fällen zulässig. Zwar wird in der juristischen Literatur in dem Verhältnis zwischen einer datenverarbeitenden Stelle und einem Cloud-Anbieter überwiegend eine vom Gesetz privilegierte Auftragsdatenverarbeitung gesehen, die zur Zulässigkeit der Datenweitergabe an den Cloud-Anbieter führen würde. Diese ist aber nach § 3 Abs. 4 Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) nur durch Stellen innerhalb der Europäischen Union möglich. Daher entfällt für die Nutzung US-amerikanischer Dienste die Möglichkeit einer Auftragsdatenverarbeitung und es ist von einer Übermittlung der betroffenen Daten im Sinne des Datenschutzrechts auszugehen.

Die Zulässigkeit einer solchen Übermittlung von personenbezogenen Daten an eine nichtöffentliche Stelle in einem Drittstaat (außerhalb der Europäischen Union) hängt von einer zweistufigen Prüfung ab. In einem ersten Schritt ist zu prüfen,

ob die Übermittlung an eine andere Stelle grundsätzlich – wenn diese nicht in einem Drittstaat liegen würde – zulässig wäre. Dazu muss einer der Erlaubnistatbestände des § 16 DSG NRW einschlägig sein. Das wäre unter anderem der Fall, wenn die Nutzung eines Dienstes für die rechtmäßige Erfüllung der Aufgaben der übermittelnden Stelle erforderlich wäre oder die Übermittlung im öffentlichen Interesse liegen würde. Selbst wenn diese hohen Anforderungen erreicht sind, ist aber darüber hinaus in einem zweiten Schritt zu prüfen, ob in der jeweiligen Situation auch die zusätzlichen Voraussetzungen für eine Übermittlung an eine Stelle außerhalb der Europäischen Union vorliegen. Soll eine Übermittlung in Drittstaaten ohne ein „angemessenes Datenschutzniveau" erfolgen, ist dies nur in den engen Grenzen des § 17 Abs. 2 DSG NRW möglich. Dies ist beispielsweise der Fall, wenn eine Einwilligung aller Betroffenen vorliegt, die von der EU-Kommission bereitgestellten Standardvertragsklauseln verwendet werden oder die Übermittlung zur Wahrung lebenswichtiger Interessen bzw. zur Geltendmachung oder Abwehr rechtlicher Ansprüche erforderlich ist. Eine Beschränkung auf diese wenigen Ausnahmen besteht nur dann nicht, wenn in dem Drittstaat, in welchem der Empfänger die Daten verarbeitet, ein angemessenes Datenschutzniveau herrscht, das mit dem Schutzniveau in der EU vergleichbar ist. Darüber, dass ein solches in den USA nicht vorliegt, besteht weitgehend Einigkeit.

Um dennoch einen umfangreichen Datenaustausch – vor allem europäischer Unternehmen – mit Stellen in den USA zu ermöglichen, sollte dieses Problem dadurch gelöst werden, dass die Europäische Kommission mit der zuständigen Stelle in den USA im Jahr 2000 das sogenannte Safe-Harbor-Abkommen schloss. Solange US-Unternehmen die darin festgeschriebenen Voraussetzungen erfüllten, sollte eine Übermittlung an sie grundsätzlich möglich sein, weil sie als empfangende Stellen ein angemessenes Datenschutzniveau garantierten. Diese Möglichkeit nutzten insgesamt über 3000 Unternehmen, darunter auch große Internetunternehmen, um die Übermittlung von Daten in die USA zu legitimieren. Der EuGH hat dieser Praxis jetzt in seiner jüngsten Entscheidung zu dieser Thematik einen Riegel vorgeschoben.

II. Verfahren vor dem EuGH

In dem Urteil vom 6. Oktober 2015 hatte der EuGH auf Vorlage des irischen High Courts darüber zu entscheiden, ob die Entscheidung der Kommission aus dem Jahr 2000, bei Firmen, die das Safe Harbor Abkommen unterschrieben haben, ein angemessenes Datenschutzniveau anzunehmen, nationale Datenschutzbehörden daran hindert, eigenständig zu prüfen, ob eine Übermittlung der Daten in einen Drittstaat rechtmäßig ist.

Das Verfahren kam zustande, nachdem der österreichische Jurist und Datenschutzaktivist Max Schrems bei der irischen Datenschutzbehörde Beschwerde gegen die Übermittlung von personenbezogenen Daten durch Facebook in die USA eingereicht hatte. Diese lehnte aber schon die Prüfung des Anliegens mit dem Hinweis auf die Safe-Harbor-Entscheidung der Kommission ab, die ihrer Ansicht nach das angemessene Schutzniveau festlege und folglich keine Prüfungskompetenz bei den nationalen Datenschutzbehörden ließe. Der daraufhin angerufene irische High Court legte den Fall dann, aufgrund des europarechtlichen Bezuges, dem EuGH vor.

Der EuGH erörterte in seinem Urteil zunächst, dass die Feststellung eines angemessenen Datenschutzniveaus durch die Kommission, entgegen der Ansicht der irischen Datenschutzbehörde, keinesfalls bindend für die nationalen Datenschutzbehörden sei. Diese sind daher, auch wenn eine solche Entscheidung vorliegt, dazu befugt und verpflichtet, die Rechtmäßigkeit einer Datenübermittlung in Drittstaaten zu überprüfen. Soweit dabei aber Zweifel an der Gültigkeit der Entscheidung der Kommission aufkommen, seien zunächst die nationalen Gerichte anzurufen, die diese dann dem EuGH vorlegen können. Nur der EuGH könne die Ungültigkeit einer solchen Kommissionsentscheidung feststellen. Diese Ungültigkeit nahm der EuGH sodann in einem zweiten Prüfungsschritt an, sodass die Einhaltung der Bestimmungen des Safe-Harbor-Abkommens von nun an nicht mehr zur Begründung eines angemessenen Datenschutzniveaus herangezogen werden können.

III. Rechtliche Betrachtung

Aus rechtlicher Sicht ist bemerkenswert, dass der EuGH nicht nur die konkrete Vorlagefrage nach der Kompetenz nationaler Datenschutzbehörden beantwortet, sondern darüber hinaus auch die Ungültigkeit der im konkreten Verfahren vom Kläger gerügten Safe-Harbor-Entscheidung der EU-Kommission herleitete. Dies begründet der EuGH in seinen Ausführungen damit, dass die Kommission in ihrer Entscheidung im Jahr 2000 ein angemessenes Datenschutzniveau nicht festgestellt habe.

Dagegen spreche schon, dass das Safe-Harbor-Abkommen zwar die betroffenen Unternehmen, nicht aber die Sicherheitsbehörden in den USA bindet. Aus dem Abkommen geht sogar ausdrücklich hervor, dass die darin enthaltenen Schutzbestimmungen hinter den gesetzlichen Eingriffsbefugnissen in den USA zurücktreten. Erfordernisse der nationalen Sicherheit, das öffentliche Interesse und die Durchführung von Gesetzen der Vereinigten Staaten haben danach uneingeschränkt Vorrang. Diese staatlichen Eingriffsbefugnisse sieht der EuGH als Eingriff in die Privatsphäre der Bürger, dessen Rechtfertigung in der Entscheidung der Kommission nicht nachgewiesen werde. Zum einen zeige diese weder Begrenzungen für staatliche Eingriffe, noch Rechtsschutzmöglichkeiten gegen diese. Zum anderen würden die vorliegenden Eingriffe in die Persönlichkeitsrechte der Betroffenen nicht auf das absolut Notwendige beschränkt, da generell die Speicherung aller personenbezogenen Daten, die in die USA übermittelt werden, vorgesehen sei, ohne jegliche Differenzierung, Einschränkung oder Ausnahmen mit Rücksicht auf das verfolgte Ziel. Da ein angemessenes Datenschutzniveau folglich schon durch die Entscheidung der Kommission gar nicht festgestellt worden sei, stehe ohne genaue inhaltliche Prüfung des Safe-Harbor-Abkommens fest, dass die Entscheidung ungültig ist.

Der EuGH brachte in seinen Ausführungen folglich zum Ausdruck, dass die Erwägungen der EU-Kommission, die diese in ihrer Entscheidung über die Anerkennung der Safe-Harbor-Regelungen im Jahr 2000 aufgeführt hatte, nicht die Anforderungen an eine strikte Kontrolle des Datenschutzniveaus erfüllen. Das erforderliche gleichwertige Datenschutzniveau ist daher auch durch die Einhaltung des Safe-Harbor-Abkommens nicht gewährleistet.

IV. Auswirkungen für Hochschulen und Forschungseinrichtungen

Der durch die Entscheidung ausgelöste Aufruhr ist erwartungsgemäß hoch. Die mehr als 3000 unter dem Abkommen zertifizierten Unternehmen nutzten dieses zumindest teilweise, um die Übermittlung von Daten in die USA zu legitimieren. Die zu erwartende Lücke ist groß und bis sie geschlossen wird, ist in vielen Situationen eine erhebliche Unsicherheit bezüglich der Rechtmäßigkeit der Übermittlung von Daten in die USA unvermeidbar. In Deutschland haben die nationalen Aufsichtsbehörden in einer gemeinsamen Stellungnahme angekündigt, während einer Übergangsfrist bis Ende Januar 2016 nicht gezielt gegen Verstöße, die auf der Ungültigkeit der Safe-Harbor-Regelungen beruhen, vorzugehen. Spätestens danach kann aber eine Übermittlung nicht mehr durch Berufung auf das Safe-Harbor-Abkommen gerechtfertigt werden. Dies gilt gleichermaßen auch für Hochschulen und Forschungseinrichtungen. Je nach Situation könnten die entstehenden Lücken gegebenenfalls durch den Einsatz von sog. Standardvertragsklauseln oder durch Einholung einer Einwilligung von allen Betroffenen geschlossen werden. Allerdings ist die Wirksamkeit der Standardvertragsklauseln nach dem Urteil des EuGH ebenfalls fraglich. Praktisch fällt es zudem oft schwer, mit Diensteanbietern in den USA den Einsatz der Standardvertragsklauseln zu vereinbaren. Eine Einwilligung sämtlicher Betroffener ist zum einen mit hohem praktischem Aufwand verbunden und muss zum anderen auch frei von (auch nur faktischem) Zwang erteilt werden. Dies ist insbesondere dann schwierig, wenn sich die von der Datenverarbeitung Betroffenen in einer gewissen Zwangssituation gegenüber der datenverarbeitenden Stelle befinden, wie z. B. Arbeitnehmer gegenüber ihrem Arbeitgeber oder Studenten gegenüber ihrer Hochschule. Soweit dies aber aus praktischer und technischer Sicht umsetzbar ist, stellt die direkte Einwilligung der Betroffenen die rechtssicherste Lösung dar.

Im Übrigen empfiehlt es sich, soweit möglich, auf Übermittlungen von Daten in die USA zu verzichten und Dienste einzusetzen, die eine Datenspeicherung innerhalb der EU garantieren und nicht dem Zugriff der US-Behörden unterliegen. Neben bestehenden Angeboten, wie den DFN-Cloud-Diensten, könnten zukünftig auch verstärkt große kommerzielle Anbieter Modelle entwickeln, die diese Kriterien erfüllen und somit die besonderen Anforderungen des europäischen Marktes berücksichtigen. In diese Richtung deutet jedenfalls der Vorstoß von Microsoft, die den Aufbau einer Cloud-Infrastruktur in Kooperation mit der Telekom-Tochter T-Systems planen. Dabei sollen die Daten ausschließlich auf Servern in Deutschland gespeichert und der Zugriff darauf lediglich von T-Systems als sog. Datentreuhänder ausgeübt werden, sodass US-Sicherheitsbehörden auch nicht über den Umweg über den Mutterkonzern Microsoft Zugriff auf die Daten erlangen können, wie dies etwa bei einer Speicherung durch ein Tochterunternehmen denkbar wäre.

Derzeit muss aber das Fazit gelten, dass eine Speicherung und Nutzung personenbezogener Daten immer dort, wo eine

Übermittlung der Daten in die USA im Raum steht, rechtlich problematisch und in jedem Fall mit gewissen Umständen und Einschränkungen verbunden ist, zumal eine solche Übermittlung, wie oben dargestellt, schnell auch unbewusst erfolgen kann.

Freie Gefahrenquelle

Landgericht Halle zur Reichweite der Wiederholungsgefahr bei der Verletzung der sogenannten General Public License (GPL)

von Clara Ochsenfeld

In einer im einstweiligen Rechtsschutz ergangenen Entscheidung vom 27. Juli 2015 hat sich das Landgericht Halle (Az.: 4 O 133/15) zu den Voraussetzungen eines Unterlassungsanspruchs bei Verletzung einer GPL geäußert. Das Gericht sah trotz der Beseitigung der streitgegenständlichen Urheberrechtsverletzung und einer in der mündlichen Verhandlung abgegebenen eidesstattlichen Versicherung der beklagten Hochschule die Wiederholungsgefahr einer erneuten Urheberrechtsverletzung als gegeben an und bejahte deshalb einen Unterlassungsanspruch des Softwareunternehmens gegenüber der Hochschule. Auch die durch den Lizenzgeber vertraglich eingeräumte „zweite Chance" der weiteren Lizenzierung stand nach Ansicht des Gerichts der durch die Rechtsverletzung indizierten Wiederholungsgefahr nicht entgegen.

I. Problemaufriss

Das Herunterladen von Free und Open Source Software ist aus dem Internet nicht mehr wegzudenken. Auch wenn die Bezeichnung zunächst anderes vermuten lässt, ist die Nutzung der Programme an die bestehenden urheberrechtlichen Anforderungen und somit an die lizenzvertraglichen Bedingungen gebunden. Die Bedingungen der Nutzung von Free und Open Source Software richten sich oftmals nach der GNU General Public License (kurz: GPL), eine von dem US-amerikanischen Programmierer Richard Stallmann entwickelte Lizenz, die ohne spezielle Anpassung bei einer Vielzahl von Projekten verwendet werden kann und die die vertraglichen Bedingungen der Nutzung und Weitergabe des Programms regelt. Die Idee besteht darin, dass der Nutzer unentgeltlich ein einfaches Nutzungsrecht erhält und sich im Gegenzug verpflichtet, seine Umgestaltungen wiederum zur allgemeinen Nutzung freizustellen, sodass letztlich alle Nutzer und die Gemeinschaft von diesem Modell profitieren können. Oftmals verkennen Lizenznehmer bei der Bereitstellung des Programms jedoch ihre Pflichten aus der GPL. Solche bestehen unter anderem darin, dem Dritten vor dem Herunterladen des Programmes den Lizenztext der GPL zur Kenntnis zu geben und den korrespondierenden Sourcecode des Programmes lizenzgebührenfrei bereitzustellen. Im Falle der Verletzung dieser vertraglichen Bestimmungen können die Nutzungsrechte unter Umständen erlöschen und der Verletzer vom Rechteinhaber wegen der Urheberrechtsverletzungen in Anspruch genommen werden. Die Rechteinhaber gehen inzwischen verstärkt gegen die Verletzungen durch Dritte vor, indem sie ihre Ansprüche u. a. durch vorgerichtliche Abmahnungen geltend machen und vom Verletzer die Abgabe strafbewehrter Unterlassungs- und Verpflichtungserklärungen verlangen.

II. Sachverhalt und Entscheidung des Gerichts

In dem der Entscheidung zugrundeliegenden Fall hatte eine Hochschule ihren Studenten und Mitarbeitern eine Software zum Download zur Verfügung gestellt, die den Lizenzbestimmungen der GPL unterlag. Die Hochschule versäumte es jedoch, gemäß den GPL-Lizenzbedingungen den entsprechenden Text der GPL vor dem Download zur Kenntnisnahme bereitzustellen (Ziff. 4 der dritten Version der GPL von 2007 (GPLv3)) und darüber hinaus, den vollständigen korrespondierenden Sourcecode der Software zugänglich zu machen (Ziff. 6 der GPLv3). Die Rechteinhaberin beanstandete die lizenzwidrige Verwendung und verlangte vorgerichtlich durch ihren Prozessbevollmächtigten von dem Rektor der Hochschule Auskunft über die

bisherige Nutzung der Software sowie die Abgabe einer strafbewehrten Unterlassungs- und Verpflichtungserklärung. Die Hochschule reagierte und nahm unmittelbar das Angebot des Softwaredownloads von ihrer Webseite, weigerte sich jedoch, die strafbewehrte Unterlassungs- und Verpflichtungserklärung abzugeben.

Die Rechteinhaberin machte daraufhin im einstweiligen Rechtsschutz ihre Ansprüche gegenüber der Hochschule geltend. In der mündlichen Verhandlung versicherten sowohl der Leiter des Rechenzentrums als auch der Kanzler der Hochschule an Eides statt, dass die Hochschule die Rechtsverletzung zukünftig unterlassen werde. Dennoch bejahte das Gericht zugunsten des Softwareunternehmens einen Unterlassungsanspruch nach § 97 Abs. 1 Urheberrechtsgesetz (UrhG) i.V.m. § 69c Nr. 4 UrhG. Durch die öffentliche Zugänglichmachung ohne Bereitstellung der GPL zur Kenntnisnahme durch den Nutzer und ohne die Offenlegung des Sourcecodes hat die beklagte Hochschule gegen die Bestimmungen der GPL verstoßen. Das Gericht sah zudem die für einen Unterlassungsanspruch erforderliche Wiederholungsgefahr trotz der sofortigen Entfernung der Software von der Webseite und der Abgabe der eidesstattlichen Versicherung durch den Leiter des Rechenzentrums und den Kanzler der Hochschule als gegeben an. Das Gericht begründete das Bestehen einer Wiederholungsgefahr damit, dass eine solche grundsätzlich durch die Begehung einer Rechtsverletzung in der Vergangenheit indiziert sei und ihr somit eine Vermutungswirkung zukomme. Nach ständiger Rechtsprechung kann diese indizierte Wiederholungsgefahr nicht dadurch ausgeräumt werden, dass der Verletzer eine rechtsverbindliche Erklärung, er werde die Zuwiderhandlung in Zukunft unterlassen, abgebe. Dies sei damit zu begründen, dass es bei der Erklärung an der nötigen rechtlichen Absicherung fehle. Eine solche kann nur durch die Abgabe einer ernsthaft, unbefristet und vorbehaltlos erklärten strafbewehrten Unterlassungserklärung herbeigeführt werden, d. h. sie muss das unbedingte Versprechen des Verletzers enthalten, im Fall der Zuwiderhandlung eine Vertragsstrafe zu entrichten. Da die beklagte Hochschule die Abgabe einer solchen Erklärung sowohl vorprozessual als auch innerhalb des Prozesses verweigerte, sah das Gericht die Wiederholungsgefahr als gegeben an und bejahte den Unterlassungsanspruch. Darüber hinaus erklärte das Gericht, dass entgegen der Ansicht der Hochschule auch die Klausel über die „zweite Chance“ einer Lizenzierung, die in Ziff. 8 der GPLv3 enthalten ist, der Wiederholungsgefahr nicht entgegenstehe. Diese Klausel beinhaltet eine Regelung, die dem Lizenznehmer gestattet, das Programm auch nach einer erstmalig begangenen Urheberrechtsverletzung weiterhin zu nutzen, wenn dieser die Urheberrechtsverletzung innerhalb von 30 Tagen, nachdem er auf die Verletzung aufmerksam gemacht wurde, beseitigt. Diese Klausel sei nach Ansicht des Gerichts nicht dahingehend auszulegen, dass der Rechteinhaber durch die Einräumung einer zweiten Chance zugleich auf die Geltendmachung seiner Ansprüche bzw. auf die gegnerische Abgabe einer strafbewehrten Unterlassungserklärung verzichte. Denn durch die freiwillige Einräumung der weiteren Nutzung der Software dürfe nicht das schützenswerte Interesse des Rechteinhabers unterlaufen werden, weiteren Rechtsverstößen nachhaltig vorbeugen zu wollen.

III. Hinweise für die Hochschulen

Für die Hochschulen stellt die Bereitstellung von Open Source Software eine willkommene Möglichkeit dar, ihren Mitarbeitern und Studenten kostenlos die benötigte Software zur Verfügung zu stellen, indem die Möglichkeit des Downloads unmittelbar auf der Webseite der Hochschule implementiert wird. Die Rechenzentren sollten bei diesem Vorgehen explizit auf den richtigen Umgang mit der entsprechenden Free und Open Source Software achten. Sie müssen stets sicherstellen, dass bei der öffentlichen Zugänglichmachung GPL-lizenzierter Software die Lizenzbedingungen der für die Software verwendeten GPL-Version eingehalten werden. Im Falle der Zurverfügungstellung sollten die entsprechenden Lizenzbedingungen demnach stets von der Rechtsabteilung der Hochschulen überprüft und entsprechende Maßnahmen getroffen werden.

Soweit ein möglicher Anspruchsinhaber an die Hochschule herantritt und eine Verletzung beanstandet, sollte zunächst unbedingt geprüft werden, ob der Anspruchsteller auch der tatsächliche Rechteinhaber ist. Außerdem sollten im Falle einer tatsächlich begangenen Verletzung zügig entsprechende Maßnahmen getroffen werden, um die Verletzung auszuräumen. Wie das Urteil des Landgerichts Halle zeigt, sollte die Hochschule nicht pauschal die Abgabe einer strafbewehrten Unterlassungserklärung verweigern. Unter Einbeziehung der Rechtsabteilung sollte vielmehr im Einzelfall geprüft werden, ob den Ansprüchen des Gegners weitere Argumente, die eine Wiederholungsgefahr verneinen, entgegengesetzt werden können. Aus der Entscheidung geht hervor, dass die Ausräumung der Verletzung in Verbindung mit der Abgabe

einer eidesstattlichen Erklärung durch die Hochschulleitung nicht ausreicht, um der Vermutungswirkung einer Wiederholungsgefahr entgegenzuwirken. Sollten darüber hinaus keine weiteren Umstände hinzutreten, die der durch die Rechtsverletzung grundsätzlich indizierten Wiederholungsgefahr entgegenzusetzen sind, kann die Abgabe einer strafbewehrten Unterlassungserklärung unter Umständen das günstigere Mittel sein, durch das oftmals einem teuren Rechtsstreit vorgebeugt werden kann.

Hinweis: Nähere Informationen zum Thema Abmahnungen erhalten Sie in der Handlungsempfehlung „Was tun bei Abmahnungen“
https://www.dfn.de/fileadmin/3Beratung/Recht/handlungsempfehlungen/Was_tun_bei_Abmahnungen.pdf

Mitgefangen, mitgehangen

Bundesgerichtshof zur Bewertung der Veranstaltereigenschaft nach § 13b Absatz 1 UrhWahrnG

von Jan Heuer

Gem. § 13b Absatz 1 Urheberrechtswahrnehmungsgesetz (UrhWahrnG) sind die Veranstalter von öffentlichen Wiedergaben urheberrechtlich geschützter Werke vor der Veranstaltung verpflichtet, die Einwilligung der Verwertungsgesellschaft einzuholen, welche die Nutzungsrechte an diesen Werken wahrnimmt. Der Bundesgerichtshof (BGH) bezieht mit seinem Urteil (12.02.2015 – AZ. I ZR 204/13) nun Stellung zu der Frage, wann die Eigenschaft als Veranstalter eines solchen Werkes zu bejahen ist, auch wenn der Betroffene nicht der ausübende Künstler ist.

I. Verwertungsgesellschaften im Urheberrecht

Jeden Tag werden vielfach urheberrechtlich geschützte Werke aufgeführt. Insbesondere Hochschulen, die im Bereich der „schönen Künste“ vertreten oder ausschließlich in diesem Bereich tätig sind, kommen mit diesem Phänomen unweigerlich in Berührung. Im Bereich von Musik und Theater sind die in Rede stehenden Aufführungen dabei grundsätzlich öffentlichkeitswirksam. Vielen wird insofern auch die Pflicht des Veranstalters, eine Veranstaltung bei der jeweiligen Verwertungsgesellschaft anzumelden, bekannt sein.

Verwertungsgesellschaften sind privatrechtliche Vereinigungen, die, gestützt auf § 1 UrhWahrnG, die Verwaltung von Vergütungsansprüchen, Nutzungs- und Einwilligungsrechten von Urhebern und den Inhabern von Schutzrechten wahrnehmen. Auf ihrem Gebiet kommt ihnen dabei eine Monopolstellung zu. Unter anderem hat die jeweilige Verwertungsgesellschaft Tarife in Bezug auf die Vergütung der von ihr wahrgenommenen Rechte aufzustellen (§ 13 UrhWahrnG). Dabei nimmt die Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte (GEMA) die Verwertungsrechte von Musikurhebern (Komponisten und Textdichtern) wahr. Für den Bereich der Aufführung solcher Werke ist damit vor einer Aufführung ihre Zustimmung einzuholen. Ist die Eigenschaft Veranstalter zu sein, im Rahmen von Festivitäten, bei denen keine ausübenden Künstler auftreten, relativ leicht zu klären, so werden gerade bei Veranstaltungen, denen mehrere Einzelleistungen (z. B. die Überlassung eines Theatersaals) zugrunde liegen, Schwierigkeiten deutlich.

II. Entscheidung des BGH

Die Beantwortung der Frage, wann bei mehreren Einzelleistungen die Eigenschaft Veranstalter im Sinne des UrhWahrnG gegeben ist, stand bei der Entscheidung des BGH im Mittelpunkt der Urteilsfindung.

Sachverhalt

Die Klägerin des zugrundeliegenden Verfahrens war die GEMA. Die Beklagte war Betreiberin eines Theaters, in dem am 27.11.2009 die Veranstaltung „Trassenfieber: Die Nordbahnrevue“ stattfand. Auf diese Veranstaltung wurde von der Beklagten in ihrem Veranstaltungskalender hingewiesen. Daneben wurde durch die Beklagte der Saal für die Veranstaltung bereitgehalten und die Bewirtung der Gäste sichergestellt. Die hieraus erzielten Einnahmen, den Erlös aus den Eintrittskarten der ausübende Künstler, behielt die Beklagte. Die Veranstaltung wurde nicht bei der Verwertungsgesellschaft angemeldet. Daraufhin nahm die GEMA die Beklagte als Mitveranstalterin wegen unerlaubter Wiedergabe von Musikwerken in Anspruch und forderte die Zahlung von Schadensersatz. Das erstinstanzlich zuständige Amtsgericht wies

die Klage der GEMA ab. Auch im Berufungsverfahren vor dem Landgericht Düsseldorf unterlag sie. Mit der vom Berufungsgericht zugelassenen Revision beim BGH hatte sie nun Erfolg.

Entscheidungsgründe

Grundlage des Zahlungsanspruchs der Klägerin war dabei § 97 Absatz 2 Satz 1 Urheberrechtsgesetz (UrhG). Nach dieser Regelung haftet derjenige, der ein fremdes Urheberrecht widerrechtlich und schuldhaft verletzt, auf Ersatz des daraus entstandenen Schadens. Da die Klägerin selbst nicht die Urheberin der verletzten Werke war, hatte sie ihre Berechtigung, den Anspruch geltend machen zu dürfen, nachzuweisen (sog. Aktivlegitimation). Diesbezüglich, so das Gericht, griff für die Verwertungsgesellschaft die sog. GEMA-Vermutung ein. Diese GEMA-Vermutung stützt sich auf das umfassende In- und Auslandsrepertoire der Verwertungsgesellschaft (GEMA) und führt nach der Rechtsprechung zu der tatsächlichen Vermutung der Wahrnehmungsbefugnis für die Aufführungsrechte an in- und ausländischer Tanz- und Unterhaltungsmusik. Die Vermutung wurde zur Erleichterung des Nachweises der Wahrnehmungsbefugnis geschaffen und kann durch die in Anspruch genommene Partei widerlegt werden. Im zugrundeliegenden Fall führte dies zu der Annahme, dass die Klägerin, zum einen zur Wahrnehmung der Aufführungsrechte des Urhebers (§§ 15 Absatz 2 und 19 Absatz 2 UrhG) befugt war, zum anderen dazu, dass die im Rahmen der Veranstaltung genutzten Musikwerke urheberrechtlich geschützt waren. Da keine Anmeldung der Aufführung erfolgte und eine Einwilligung der GEMA entsprechend nicht eingeholt worden war, lag eine Verletzung von Urheberrechten vor. Entscheidend für die Frage, ob der geltend gemachte Anspruch bestand, war, ob die Beklagte auch als Gegnerin des Anspruchs anzusehen war (sog. Passivlegitimation). Wurde diese Eigenschaft der Beklagten noch in den Vorinstanzen verneint, sah der BGH die Passivlegitimation als gegeben an.

Die Beklagte hatte zwar die in Rede stehenden Werke nicht selbst aufgeführt, dennoch konnte sie, so der BGH, für die unmittelbar durch die aufführenden Künstler begangenen Eingriffe in fremde Urheberechte verantwortlich gemacht werden. Ob jemand als Täter oder Teilnehmer an einer deliktischen Handlung eines Dritten beteiligt ist, beurteilt sich nach ständiger Rechtsprechung des BGH dabei nach den im Strafrecht entwickelten Grundsätzen. Insbesondere Mittäterschaft ist dann gegeben, wenn mehrere Personen bei der Herbeiführung eines Erfolges bewusst und gewollt zusammenwirken (vgl. § 830 Absatz 1 Satz 1 BGB). Eine Mittäterschaft wird dabei speziell im Urheberrecht für den Veranstalter gesehen, der neben den aufführenden Künstlern beteiligt ist.

Gem. § 13b Absatz 1 UrhWahrnG ist der Veranstalter verpflichtet, vor Beginn der Veranstaltung die Einwilligung der zuständigen Verwertungsgesellschaft einzuholen. Als Veranstalter ist dabei derjenige anzusehen, der die Aufführung angeordnet und sie durch seine Tätigkeit ins Werk gesetzt hat. Das ist insbesondere dann anzunehmen, wenn finanzielle und organisatorische Verantwortlichkeit gegeben sind. Kern der Streitigkeit war die Frage, ob die Beklagte damit als Veranstalterin anzusehen war. Bezugnehmend auf die bisherige Rechtsprechung des BGH war insbesondere auf das Kriterium hingewiesen worden, auf die Auswahl der aufzuführenden Stücke Einfluss nehmen zu können. Indes wurde im konkreten Fall hervorgehoben, dass auch ohne solche Einwirkungsmöglichkeiten organisatorische Beiträge zur Veranstaltung, die nach Art und Umfang oder Gewicht bedeutsam sind, es rechtfertigen können, dass Dritte als Veranstalter angesehen werden. In eine solche Gesamtbetrachtung der Beiträge können z. B. die Beauftragung der ausübenden Künstler, die Überlassung des Veranstaltungsraumes und der technischen Vorkehrungen, die Einlass- und Auslasskontrollen der Besucher, die Aufbewahrung der Garderobe, die Bewerbung der Veranstaltung, der Kartenverkauf sowie die Übernahme begleitender Dienstleistungen wie die Bewirtung der Veranstaltungsgäste einzubeziehen sein.

Besonders betont wurde, dass das bloße Treffen der äußerlichen Vorkehrungen (z. B. nur das mietweise Überlassen des Saales) nicht dazu führt, dass diese Person als Veranstalter anzusehen ist.

Für den vorliegenden Fall sah der BGH in seiner vorgenommenen Gesamtschau die Voraussetzungen für die Bejahung der Veranstaltereigenschaft der Beklagten als gegeben an.

Den Umständen, dass die Veranstaltung im Veranstaltungskalender der Beklagten beworben wurde, dass die Eintrittskarten über die Beklagte zu beziehen waren und dass die Bewirtung der Gäste von der Beklagten übernommen worden war, wurden im Zuge der Begründung der Entscheidung besonderes Gewicht beigemessen. Aufgrund der bestehenden Eigenschaft als Veranstalter hatte damit die Beklagte gemeinsam mit dem aufführenden Künstler die Aufführung ins Werk gesetzt.

Des Weiteren wurde auch ein schuldhaftes Handeln der Beklagten bejaht, denn es oblag ihr als Veranstalterin das Vorliegen einer Einwilligung der Verwertungsgesellschaft sicherzustellen. Im Ergebnis wurde damit das Vorliegen der Vorausset-

zungen nach § 97 Absatz 2 Satz 1 UrhG und dementsprechend der von der GEMA geltend gemachte Schadensersatzanspruch durch den BGH bejaht.

III. Fazit und Konsequenzen für die Hochschulen

Bei der Aufführung urheberrechtlich geschützter Werke ist Vorsicht geboten. Sollte die Hochschule den Rahmen für solche Aufführungen bieten, ist sicherzustellen, welche Beiträge genau erbracht werden und ob das Gewicht bzw. Art und Umfang dieser Beiträge dazu führen, dass die Hochschule als Veranstalterin im Sinne des § 13b Absatz 1 UrhWahrnG anzusehen ist. Ist dies der Fall, ist die Veranstaltung bei der zuständigen Verwertungsgesellschaft (für Musikwerke die GEMA) anzumelden, um die notwendige Einwilligung einzuholen. Andernfalls könnte sich eine Schadensersatzforderung der Verwertungsgesellschaft nach § 97 Absatz 2 Satz 1 UrhG auch gegen die Hochschule richten.