DFN

Infobrief Recht

11 / 2017

November 2017

Alles unter Kontrolle?

Die DSGVO und ihre Auswirkungen auf die Rolle des Datenschutzbeauftragten

Ist Internet nicht gleich Internet?

BGH legt dem EuGH eine Vorlagefrage zur urheberrechtlichen Beurteilung der Übernahme eines Bildes auf die eigene Homepage vor

Wer hat noch nicht, wer will noch mal?

Gesetzgeber schafft Störerhaftung für WLAN-Betreiber ab und führt Sperrverpflichtungen ein

Alles unter Kontrolle?

Die DSGVO und ihre Auswirkungen auf die Rolle des Datenschutzbeauftragten

von Charlotte Röttgen

Die Europäische Datenschutzgrundverordnung (DGSGVO), die am 25. Mai 2018 in allen Europäischen Mitgliedstaaten wirksam werden wird, bringt neben den Veränderungen in der datenschutzrechtlichen Regelungssystematik auch einige Neuerungen im Bereich der datenschutzrechtlichen Kontrollorgane mit sich. Insbesondere das Anforderungs- und Aufgabenprofil des Datenschutzbeauftragten erfährt Änderungen, die es bis zum Wirksamwerden der DSGVO in die internen Abläufe der Hochschulen und Forschungseinrichtungen zu integrieren gilt. Der folgende Beitrag zeigt einige wesentliche Unterschiede von bestehendem und künftigem Recht auf. Sofern der Gesetzgeber zwischen öffentlichen und nicht-öffentlichen Stellen unterscheidet, wird diesen Unterschieden im Folgenden Rechnung getragen; im Übrigen liegt ein regulatorischer Gleichklang vor.

I. Einleitung

Nach bisherigem Datenschutzrecht gibt es vor allem zwei entscheidende datenschutzrechtliche Institutionen, die Aufsichtsbehörde als obere datenschutzrechtliche Kontrollinstanz sowie den Datenschutzbeauftragten. Während die Aufgabe der Aufsichtsbehörde im Wesentlichen darin besteht, die Einhaltung datenschutzrechtlicher Vorschriften bei der Verarbeitung personenbezogener Daten durch datenverarbeitende Stellen zu überwachen und bei Verstößen einzuschreiten, war es bislang die Aufgabe des im Zentrum dieses Beitrags stehenden Datenschutzbeauftragten, auf die Einhaltung datenschutzrechtlicher Vorgaben bei der Verarbeitung personenbezogener Daten innerhalb der eigenen Behörde oder der nicht-öffentlichen Stelle hinzuwirken.

Mit Wirksamwerden der DSGVO innerhalb der Europäischen Mitgliedstaaten gehen hinsichtlich der Rolle des Datenschutzbeauftragten einige Neuerungen einher. Wird sich an Art und Anzahl der datenschutzrechtlichen Institutionen nichts ändern, gibt es aber bei der Bestellpflicht sowie beim Aufgaben- und Anforderungsprofil einige Punkte, die es nach der DSGVO zukünftig zu beachten gilt.

Die geänderten Vorschriften der DSGVO haben auch zur Folge, dass sich das Verhältnis von Personalrat bzw. Betriebsrat und Datenschutzbeauftragtem voraussichtlich verändern wird. Unterliegen Personal- und Betriebsrat in ihrer Tätigkeit – soweit sie die Verarbeitung personenbezogener Daten zum Gegenstand hat – bislang nicht der Kontrolle durch den Datenschutzbeauftragten, könnte sich dies ab Mai nächsten Jahres ändern.

II. Der Datenschutzbeauftragte im öffentlichen und nicht-öffentlichen Bereich

Der Datenschutzbeauftragte ist und bleibt auch nach der DSGVO das Kontrollorgan innerhalb einer öffentlichen oder nicht-öffentlichen Stelle. Er ist Ansprechpartner für die Behördenleitung, die Geschäftsführung und die Beschäftigten in allen, den Datenschutz betreffenden Angelegenheiten und ist in alle datenschutzrelevanten Abläufe der datenverarbeitenden Stelle einzubinden, um die Einhaltung der Datenschutzgesetze zu überprüfen. Die Aufgaben, die Anforderungen und das Verfahren der Bestellung des Datenschutzbeauftragten sind in der DSGVO abschließend in Art. 37-39 DSGVO geregelt.

1. Die Pflicht zur Bestellung eines Beauftragten für den Datenschutz

Nach bisherigem Recht auf Bundes- und Landesebene ist die Bestellung eines Datenschutzbeauftragten für öffentliche Stellen und Behörden bereits verpflichtend. Auf Bundesebene beispielsweise findet sich die Regelung zur Bestellpflicht des behördlichen Beauftragten für den Datenschutz im aktuell bestehenden Recht in § 4f Abs. 1 S. 1 BDSG, im nordrhein-westfälischen Datenschutzgesetz in § 32a Abs. 1 S. 1 DSG NRW und im Datenschutzgesetz von Berlin in § 19a Abs. 1 S. 1 Bln DSG. Teilweise hängt die Pflicht zur Bestellung des behördlichen Datenschutzbeauftragten davon ab, ob die Verarbeitung personenbezogener Daten automatisiert erfolgt.

Letzteres ist in der DSGVO nicht mehr der Fall; im Bereich der Bestellpflicht des Datenschutzbeauftragten wird eine Differenzierung zwischen automatisierter und nicht automatisierter Datenverarbeitung zukünftig nicht mehr vorgenommen. Mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln, sieht die DSGVO eine solche Bestellpflicht für öffentliche Stellen und Behörden, die personenbezogene Daten verarbeiten, nun verbindlich vor. Das heißt, beruhte die Einführung einer Bestellpflicht eines behördlichen Datenschutzbeauftragten bisher auf dem Willen des jeweiligen Bundes- oder Landesgesetzgebers, gibt es hier künftig keinen Abweichungsspielraum mehr und es besteht gem. Art. 37 Abs. 1 lit. a DSGVO in allen Ländern sowie im Bund die unmittelbare Pflicht durch einen behördlichen Datenschutzbeauftragten zu bestellen.
Für öffentliche Hochschulen und Forschungseinrichtungen wird sich also nur dann etwas ändern, wenn in dem jeweiligen Datenschutzrecht ihres Landes eine solche Bestellpflicht bislang nicht existierte.

Im nicht-öffentlichen Bereich stellt sich die Rechtslage folgendermaßen dar: Werden personenbezogene Daten automatisiert verarbeitet und sind mit dieser Datenverarbeitung mehr als neun Personen betraut, besteht nach derzeit geltendem Recht auch für nicht-öffentliche Stellen die Pflicht zur Bestellung eines Datenschutzbeauftragten (§ 4f Abs. 1 S. 3 BDSG). Im Falle der nicht-automatisierten Datenverarbeitung liegt die Schwelle der hiermit betrauten Personen bei 20 (§ 4f Abs. 1 S.2 BDSG). Wird die Mindestanzahl an Personen, die ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind, nicht überschritten, besteht nach noch geltendem Recht somit keine Pflicht zur Bestellung eines Datenschutzbeauftragten im nicht-öffentlichen Bereich. Ausnahmsweise besteht aber unabhängig von der Anzahl der Beschäftigten eine generelle Bestellpflicht für nicht-öffentliche Stellen, sofern sie „automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen, oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung automatisiert verarbeiten“ (§ 4f Abs. 1 S. 6 BDSG).

Ab dem 25. Mai 2018, wenn die DSGVO wirksam wird, ergibt sich die Pflicht zur Bestellung eines Datenschutzbeauftragten im nicht-öffentlichen Bereich aus Art. 37 Abs. 1 lit. b und c DSGVO. Hiernach wird es für die Frage nach einer Bestellpflicht wesentlich auf die Kerntätigkeit des Verantwortlichen ankommen. Besteht diese nämlich in der Durchführung von Verarbeitungsvorgängen, die “aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen“ (Art. 37 Abs. 1 lit. b DSGVO) oder besteht diese in der „umfangreichen Verarbeitung besonderer Kategorien von Daten“ (Art. 37 Abs. 1 lit. c DSGVO), trifft nicht-öffentliche Stellen die Pflicht zur Bestellung eines Datenschutzbeauftragten. Der Begriff Kerntätigkeit ist so zu verstehen, dass es sich um die Haupt- und nicht nur eine Nebentätigkeit handeln muss. Das bedeutet, dass die konkrete Datenverarbeitung für die Geschäftsabläufe erforderlich ist.

2. Interner, externer und gemeinsamer Datenschutzbeauftragter

Gem. Art. 37 Abs. 6 DSGVO besteht – wie auch schon nach altem Recht – die Möglichkeit, einen Datenschutzbeauftragten aus dem Kreis der Beschäftigten des Verantwortlichen zu wählen oder alternativ einen externen Beauftragten für den Datenschutz auf Grundlage eines Dienstleistungsvertrags zu verpflichten.

Außerdem können nach bisher geltendem Recht auf Bundes- und Landesebene die Behörden und öffentlichen Stellen für mehrere Einrichtungen einen gemeinsamen Datenschutzbeauftragten bestellen (vgl. § 5 Abs. 3 S. 2 HDSG; § 32a Abs. 1 S. 3 DSG NRW). Das aktuelle Bundesdatenschutzgesetz sieht hier eine Einschränkung insoweit vor, als dass der Datenschutzbe-

auftragte nur dann für mehrere Stellen gleichzeitig ernannt werden darf, wenn dies aufgrund der Struktur der Stellen bzw. Behörden erforderlich ist (§ 4f Abs. 1 S. 5 BDSG).
Auch zukünftig werden mehrere öffentliche Stellen oder mehrere Behörden gem. Art. 37 Abs. 3 DSGVO einen gemeinsamen Datenschutzbeauftragten bestellen können. Hierbei haben sie künftig allerdings ihrer jeweiligen Organisationsstruktur und Größe Rechnung zu tragen. Die Anzahl der öffentlichen Stellen und Behörden, für die ein Datenschutzbeauftragter bestellt werden kann, darf nicht so groß sein, dass er nicht mehr in der Lage ist, seine ihm obliegenden Aufgaben angemessen in dem gebotenen Rahmen wahrzunehmen.

Hinsichtlich der nicht-öffentlichen Stellen ist im aktuellen BDSG keine ausdrückliche Regelung dazu enthalten, unter welchen Voraussetzungen und Rahmenbedingungen ein gemeinsamer Datenschutzbeauftragter für eine Unternehmensgruppe bestellt werden kann. Die DSGVO schafft diesbezüglich in Art. 37 Abs. 2 DSGVO Klarheit. Nach künftigem Recht wird die Bestellung eines gemeinsamen Datenschutzbeauftragten einer Unternehmensgruppe dann zulässig sein, wenn dieser von jeder Niederlassung aus leicht erreicht werden kann. Ob es sich bei der geforderten Erreichbarkeit um eine solche via Kommunikationsmittel oder eine örtliche Erreichbarkeit handelt, geht aus der Norm nicht hervor. Da eine Erreichbarkeit über Kommunikationsmittel de facto keine Einschränkung in einer Unternehmensstruktur darstellen würde, ist es wahrscheinlicher, dass der Gesetzgeber hier auf die örtliche Erreichbarkeit abstellen wollte.

3. Anforderungsprofil

Eine Neuerung stellen die erhöhten Anforderungen an die fachliche Qualifikation des Datenschutzbeauftragten nach der DSGVO dar. Wird bisher die „erforderliche Fachkunde und Zuverlässigkeit“ verlangt (bspw. § 4f Abs. 2 S. 1 BDSG; § 32a Abs. 1 S. 2 DSG NRW; § 19a Abs. 2 S. 1 Bln DSG), enthält Art. 37 Abs. 5 DSGVO zu dem Anforderungsprofil des Datenschutzbeauftragten nun ausdrückliche Vorgaben. Zukünftig wird der Datenschutzbeauftragte sowohl im öffentlichen, als auch im nicht-öffentlichen Bereich „auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt […].“ Mit der ausdrücklichen Betonung von Fachwissen im Bereich des Datenschutzrechts und der Datenschutzpraxis macht der Unionsgesetzgeber deutlich, dass sowohl eine rechtliche als auch eine spezielle technische Vorbildung bei der Person vorhanden sein sollten, die in das Amt des Datenschutzbeauftragten berufen wird. Inwieweit sich dies in der Praxis umsetzen lassen wird, ist fraglich, da längst nicht jede Behörde oder nicht-öffentliche Stelle über Personal verfügt, das die verlangten Kenntnisse vorweisen kann.

Von der DSGVO abweichende Auswahlkriterien, wie sie in der Vergangenheit in Behörden und Unternehmen entwickelt worden sind, um die erforderliche Fachkunde des Datenschutzbeauftragten feststellen zu können, werden mit Wirksamwerden der DSGVO nicht mehr anwendbar sein, da die Regelungen diesbezüglich abschließend sind und so die bisherige nationale Rechtspraxis verdrängen. Darüber hinaus verlangt Art. 37 Abs. 5 DSGVO, dass der Datenschutzbeauftragte die erforderlichen Fähigkeiten besitzt, um die in Art. 39 genannten Aufgaben erfüllen zu können. Neben der Aufgabe die Einhaltung der datenschutzrechtlichen Vorschriften zu überwachen, muss er etwa auch die fachliche Qualifikation zur Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten besitzen (Art. 39 Abs. 1 lit. a DSGVO) und den Verantwortlichen im Zusammenhang mit der Datenschutz-Folgenabschätzung beraten können (Abs. 1 lit. c).

4. Das Aufgabenprofil des Datenschutzbeauftragten

Dass der Datenschutzbeauftragte vertiefte fachliche Kenntnisse besitzen sollte, kommt nicht von ungefähr. Abhängig davon, in welchem Umfang die jeweilige Einrichtung Daten verarbeitet, kann sich der Tätigkeitsaufwand des Datenschutzbeauftragten durch die DSGVO deutlich erweitern. Der in Art. 39 Abs. 1 DSGVO enthaltene Aufgabenkatalog des Datenschutzbeauftragten reicht von der Unterrichtung und Beratung der verantwortlichen datenverarbeitenden Stelle sowie der Beschäftigten (lit. a), über die Überwachung der Einhaltung datenschutzrechtlicher Vorschriften (lit. b) bis hin zu der Beratung des Verantwortlichen im Zusammenhang mit der Datenschutz-Folgenabschätzung (lit. c). Die Überwachung der Einhaltung datenschutzrechtlicher Vorschriften dürfte verglichen mit der alten Rechtslage voraussichtlich die größte Änderung im Aufgabenprofil des Datenschutzbeauftragten darstellen.

a) Überwachungsaufgabe

Infolge der sprachlichen Neuformulierung der Aufsichtsfunktion wird sich voraussichtlich eine wesentliche Änderung in der Tätigkeit des Datenschutzbeauftragten ergeben. Gem. Art. 39 Abs. 1 lit. b DSGVO „überwacht" der Datenschutzbeauftragte die Einhaltung der DSGVO und anderer Datenschutzvorschriften. Vergleicht man diese Formulierung mit denen der alten Datenschutzgesetze, offenbart sich eine deutliche Verschärfung der Verantwortlichkeit. Nach dem alten Recht „unterstützt" der Datenschutzbeauftragte bislang die verantwortliche Stelle bei der Sicherstellung des Datenschutzes (§ 32a Abs. 1 S. 5 DSG NRW) oder „wirkt" auf die Einhaltung datenschutzrechtlicher Vorschriften „hin" (§ 4g Abs. 1 S. 1 BDSG). Sowohl das „Unterstützen" bei der Einhaltung von Datenschutzgesetzen als auch das „Hinwirken" darauf implizieren eine helfende aber zugleich untergeordnete Rolle. Mit Wirksamwerden der DSGVO wird der Datenschutzbeauftragte nunmehr für die „Überwachung der Einhaltung" verantwortlich. Indem er zukünftig die Einhaltung der Datenschutzgesetze zu überprüfen hat, wird er voraussichtlich in die Rolle eines Letztverantwortlichen kommen; seine Verantwortung im Bereich der Datenschutz-Compliance wird dadurch deutlich erhöht werden.

b) Unterrichtungs- und Beratungstätigkeit

Die Unterrichtungs- und Beratungsfunktion kann etwa die Durchführung regelmäßiger Schulungen der Verantwortlichen sowie der Beschäftigten durch den Datenschutzbeauftragten erfordern, in denen der Datenschutzbeauftragte hinreichende Kenntnisse im Bereich des Datenschutzrechts und insbesondere für die konkret durchzuführenden Datenverarbeitungen vermitteln soll. In Wahrnehmung dieser Aufgaben dient der Datenschutzbeauftragte hierbei als Ansprechpartner sowohl der verantwortlichen Stelle, als auch den Beschäftigten gegenüber. Dieses Aufgabenfeld gehört auch nach bisherigem Recht zu einer der Haupttätigkeiten eines Datenschutzbeauftragten. Durch die DSGVO wird es hier zu keinen gravierenden Änderungen kommen.

c) Datenschutz-Folgenabschätzung

Ist es bislang noch die Aufgabe des Datenschutzbeauftragten, eine Vorabkontrolle in etwaig risikobehafteten Verarbeitungsverfahren durchzuführen (bspw. § 4d Abs. 5, 6 BDSG; § 32a Abs. 1 DSG NRW), bringt die DSGVO in diesem Bereich eine Änderung mit sich. Zukünftig wird es keine Vorabkontrolle mehr geben, sondern eine Datenschutz-Folgenabschätzung (Art. 35 DSGVO), die inhaltlich aber im Wesentlichen der Vorabkontrolle entspricht. Die Datenschutz-Folgenabschätzung ist eine Risikobewertung, die vorzunehmen ist, wenn bei der Verarbeitung personenbezogener Daten voraussichtlich ein erhöhtes Risiko für Rechte und Freiheiten natürlicher Personen bestehen könnte. Ein solches Risiko gilt es im Rahmen der Folgenabschätzung zu erkennen und zu bewerten. Gehörte die Durchführung der Vorabkontrolle bislang gänzlich in den Aufgabenbereich des Datenschutzbeauftragten, wird die Datenschutz-Folgenabschätzung nach der DSGVO von dem für die Datenverarbeitung Verantwortlichen selbst durchzuführen sein. Der Datenschutzbeauftragte soll den Verantwortlichen bei der Datenschutz-Folgenabschätzung nur noch beraten.

III. Die Aufsichtsfunktion des Datenschutzbeauftragten im Verhältnis zu Personal- und Betriebsrat

Im datenschutzrelevanten Tätigkeitsbereich des Personal- und des Betriebsrats wird es ab dem 25. Mai 2018 eine wesentliche Änderung geben. Zukünftig dürften nämlich beide der Kontrolle durch den Datenschutzbeauftragten unterliegen. Das würde bedeuten, soweit ihre Tätigkeit den Umgang mit und die Verarbeitung von personenbezogenen Daten zum Gegenstand hat, dürfte der Datenschutzbeauftragte diese Arbeitsabläufe im Hinblick auf ihre Konformität mit den Vorgaben des Datenschutzrechts überprüfen. Dies ergibt sich aus Art. 38 Abs. 2 DSGVO, der vorschreibt, dass dem Datenschutzbeauftragten in Wahrnehmung seiner Aufgaben ausnahmslos Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen zu gewähren ist. Eine Einschränkung im Hinblick auf den Personal- und/oder den Betriebsrat ist in der Norm nicht enthalten.
Nach der bisherigen Rechtsprechung der deutschen Gerichte stellt sich die Rechtslage – sowohl auf Bundes-, als auch auf Landesebene – derzeit noch so dar, dass Personalrat und Betriebsrat keiner Kontrolle durch den Datenschutzbeauftragten unterliegt. Diese Rechtspraxis wird mit großer Wahr-

scheinlichkeit zukünftig, unter Geltung der DSGVO, nicht aufrechterhalten bleiben können. Grund hierfür ist, dass diese richterrechtliche Regelung nicht mit den Vorgaben der DSGVO im Einklang steht.

IV. Zusammenfassung und Ausblick

Die Europäische Datenschutzreform, die ab dem 25. Mai 2018 ihre Wirksamkeit entfalten wird, hat auch Auswirkungen auf die Rolle des Datenschutzbeauftragten. Während es hinsichtlich der Pflicht zur Bestellung eines Beauftragten für den Datenschutz im öffentlichen Bereich nur marginale Änderungen geben wird, werden vor allem nicht-öffentliche Einrichtungen durch den Wegfall des Schwellenwerts von der Gesetzesänderung betroffen sein. Bei dem Anforderungs- und Aufgabenprofil des Datenschutzbeauftragten kommt es schließlich zu mehreren wesentlichen Neuerungen. Insbesondere weist Art. 39 DSGVO dem Datenschutzbeauftragten einen erweiterten und stärker ausdifferenzierten Aufgabenbereich zu, der mit gesteigerten Qualifikationsanforderungen an seine Person im Zeitpunkt der Bestellung korrespondiert. Die Aufgabe der Überwachung der Einhaltung datenschutzrechtlicher Vorschriften dürfte hierbei die wichtigste Neuerung und diejenige mit dem größten Verantwortungszuwachs darstellen.

Es ist den Datenschutzbeauftragen von Hochschulen und Forschungseinrichtungen daher angeraten, sich bis zum Wirksamwerden der DSGVO auf die inhaltlichen Neuerungen ihrer Tätigkeit vorzubereiten. Insbesondere die zukünftige Überwachungsaufgabe verlangt eingehende Kenntnisse der Vorgaben der DSGVO und der datenschutzrechtlichen Spezialvorschriften. Da die Aufsichtsbehörde im Falle von Verstößen des Datenschutzbeauftragten gegen Art. 37-39 DSGVO die Hochschulen und Forschungseinrichtungen mit Sanktionen belegen kann, ist es auch im Interesse der Verantwortlichen, eine zeitnahe Weiterbildung ihrer Datenschutzbeauftragten zu fördern. Ob und wie sich das Verhältnis von Datenschutzbeauftragtem und Personalrat bzw. Betriebsrat aufgrund des neuen Hierarchieverhältnisses zwischen den beiden Akteuren in der Praxis ändern wird, bleibt abzuwarten.

Ist Internet nicht gleich Internet?

BGH legt dem EuGH eine Vorlagefrage zur urheberrechtlichen Beurteilung der Übernahme eines Bildes auf die eigene Homepage vor

von Armin Strobel

Mit seinen Entscheidungen zur urheberrechtlichen Beurteilung von sogenannten Hyperlinks und Framelinks auf geschützte Werke, die mit Erlaubnis des Rechteinhabers veröffentlicht wurden, hat der Europäische Gerichtshof (EuGH) wesentliche Grundsätze aufgestellt, die es bei urheberrechtlichen Fragestellungen im digitalen Raum zu beachten gilt. Mit der Frage inwiefern diese Grundsätze auch auf andere Sachverhaltskonstellationen übertragbar sind, musste sich nun der Bundesgerichtshof (BGH) auseinandersetzen. Mit seinen Vorlagefragen an den EuGH vom 23.02.2017 (Az. I ZR 267/15) bittet er den EuGH die Frage abschließend zu beantworten, ob die aufgestellten Grundsätze auf diejenigen Situationen übertragbar sind, in denen ein frei zugängliches Bild, das mit Erlaubnis des Rechtinhabers auf einer Internetseite veröffentlicht wurde, kopiert und auf einer anderen Internetseite veröffentlicht wird. Der BGH deutet an, dass er eine Übertragbarkeit in diesem Zusammenhang ablehne.

I. Hintergrund

Mit der voranschreitenden Digitalisierung werden das Urheberrecht und die Betroffenen vor immer neue Fragen gestellt. Die Vielfalt und die damit verbundenen Möglichkeiten des Internets führen regelmäßig zu neuen Fallkonstellationen, die es mit Hilfe des Urheberrechts interessengerecht zu lösen gilt. Im Fokus steht dabei immer wieder die Nutzung eines im Internet frei zugänglichen Werks für eigene Zwecke. Die freie Zugänglichkeit der Werke führt jedoch nicht automatisch dazu, dass die Werke auch ohne Weiteres genutzt werden dürfen. Sowohl nationale als auch europäische Urheberrechtsbestimmungen gilt es zu beachten, um eine Haftung für eigene Handlungen zu verhindern.

In der Vergangenheit hat sich der EuGH bereits mit Fragen der Haftung für sogenannte Hyperlinks beschäftigt. Die dort aufgestellten Grundsätze haben bei der rechtlichen Beurteilung von urheberrechtlichen Fallgestaltungen im digitalen Raum wesentliche Bedeutung gewonnen. Es stellt sich nun die Frage, ob diese Grundsätze auch auf andere, vergleichbare Sachverhaltskonstellationen übertragen werden können.

Im Zentrum dieser Fragestellungen steht dabei das Recht der öffentlichen Zugänglichmachung nach § 19a Urheberrechtsgesetz (UrhG). Es handelt sich hierbei um eine besondere Form der öffentlichen Wiedergabe im Sinne des § 15 Abs. 2 und 3 UrhG, nach welchem es dem Rechteinhaber vorbehalten ist, ein urheberrechtlich geschütztes Werk drahtgebunden oder drahtlos der Öffentlichkeit in einer Weise zugänglich zu machen, dass es Mitgliedern der Öffentlichkeit von Orten und zu Zeiten ihrer Wahl zugänglich ist. Da die Vorschrift auf einer europäischen Richtlinie beruht, ist bei der Anwendung der Vorschriften auf eine richtlinienkonforme Auslegung zu achten. Die abschließende Auslegungskompetenz des europäischen Rechts obliegt dabei dem EuGH. Aus diesem Grund besteht für Gerichte die Möglichkeit ein Gerichtsverfahren auszusetzen und Fragen dem EuGH vorzulegen, wenn es die Auslegung von europarechtlichen Vorschriften für den konkreten Fall als erforderlich ansieht und die Fragen nicht unter Berücksichtigung vorheriger Rechtsprechung des EuGH beantwortet werden können (vgl. Art. 267 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV)).

II. Sachverhalt

Von dieser Möglichkeit hat im vorliegenden Fall auch der BGH Gebrauch gemacht. In dem zugrundeliegenden Rechtsstreit macht ein Fotograf (Kläger) sein Recht der öffentlichen Zugänglichmachung geltend, das er durch ein online veröffentlichtes Referat auf einer Schulhomepage als verletzt ansieht.

Als Rechteinhaber einer Fotografie der Stadt Cordoba hat der Kläger einzig einem Online-Reisemagazin ein einfaches Nutzungsrecht für die Veröffentlichung im Internet eingeräumt. Eine Schülerin hat dieses Bild kopiert und in ein Referat eingefügt. Das Schülerreferat wurde anschließend auf dem Server der Schule gespeichert und zusätzlich auf der Schulhomepage veröffentlicht. Durch die Einstellung des Referats mit der Fotografie sieht der Kläger sein Recht der öffentlichen Zugänglichmachung verletzt und verlangt die Entfernung des Referats von der Homepage sowie Schadensersatz. Hiergegen wehrt sich die Beklagte (Bundesland, das die Schulaufsicht ausübt). Sie ist der Ansicht, dass keine Urheberrechtsverletzung vorliege, da die Fotografie durch die Veröffentlichung in dem Online-Reisemagazin bereits für jedermann frei zugänglich war und somit keine Verletzung des Rechts der öffentlichen Zugänglichmachung anzunehmen sei.

III. Vorlagefrage des BGH

Nachdem die vorinstanzlichen Gerichte eine Urheberrechtsverletzung durch das Einstellen des Referats mit der Fotografie bejahten, muss sich nun auch der BGH mit dieser Frage auseinandersetzen. Wie bereits angedeutet, geht es auch hier um die Frage, ob durch die Veröffentlichung des Referats das Recht der öffentlichen Zugänglichmachung des Klägers bezüglich der Fotografie von Cordoba verletzt wird. Von zentraler Bedeutung ist dabei, ob die vom EuGH aufgestellten Grundsätze zur Linkhaftung auf die hier vorliegende Situation übertragen werden können.

Eine öffentliche Zugänglichmachung ist anzunehmen, wenn die beiden Tatbestandsvoraussetzungen – Handlung der Wiedergabe und Öffentlichkeit dieser Wiedergabe – erfüllt sind.

Die Handlung der Wiedergabe ist nach dem BGH weit zu verstehen, um ein hohes Schutzniveau des Urheberrechts zu gewährleisten. Entscheidend ist, dass einem Dritten absichtlich und gezielt der Zugang zu einem urheberrechtlich geschützten Werk verschafft wird, den dieser ohne diese Handlung nicht hätte. Das eingesetzte technische Mittel oder Verfahren ist nicht erheblich. Im vorliegenden Fall bejaht das Gericht diese Voraussetzung. Durch das Einstellen des Referats auf der Schul-Homepage werde die Fotografie von Cordoba den Besuchern der Schulhomepage zugänglich gemacht. Es schade insofern nicht, dass die Besucher der Schulhomepage das Bild auch über die Internetseite des Online-Reisemagazins hätten abrufen können, weil ihnen durch die Veröffentlichung auf der Schulhomepage zumindest ein weiterer Zugang ermöglicht wurde, der ohne die Einstellung nicht bestanden hätte.

Der BGH stellt außerdem fest, dass sich die Veröffentlichung des Referats auf der Internetseite der Schule grundsätzlich an die Öffentlichkeit richtet, da das Referat für jeden Internetnutzer zugänglich ist und sich damit an eine unbestimmte Zahl potentieller Adressaten richtet. Um eine öffentliche Zugänglichmachung im Sinne des Urheberrechts annehmen zu können, ist darüber hinaus jedoch erforderlich, dass die Veröffentlichung unter Verwendung eines anderen technischen Verfahrens als bei der Erstveröffentlichung erfolgt oder zumindest für ein neues Publikum wiedergegeben wird.

Ein anderes technisches Verfahren der Veröffentlichung verneint der BGH in diesem Fall mit dem Hinweis, dass sowohl bei der Erstveröffentlichung in dem Online-Reisemagazin als auch bei der Veröffentlichung auf der Schulhomepage eine Wiedergabe im Internet erfolgte und sich damit die Verfahren der Veröffentlichung nicht unterscheiden.

Zweifel äußert der BGH aber hinsichtlich der Wiedergabe gegenüber einem neuen Publikum. Ein solches kann grundsätzlich angenommen werden, wenn durch die zweite Veröffentlichung ein Publikum angesprochen wird, an das der Rechteinhaber bei der ersten Veröffentlichung nicht dachte.
Die Zweifel sind darin begründet, dass die Beklagte geltend macht, dass die Grundsätze des EuGH zur Linkhaftung auf die vorliegende Fallkonstellation übertragen werden könnten. Der EuGH verneint eine Wiedergabe gegenüber einem neuen Publikum, wenn ein Link zu einem urheberrechtlich geschützten Werk führt, dass auf der anderen Internetseite mit Erlaubnis des Rechteinhabers veröffentlicht wurde und ohne Zugangsbeschränkungen für jedermann zugänglich ist. Nach Auffassung des EuGH richtet sich sowohl die erste Veröffentlichung als auch der Link an jeden potentiellen Internetnutzer,

sodass in beiden Fällen jedermann als Adressat der jeweiligen Handlung angesehen werden kann. Da sich die Adressatenkreise somit überschneiden und die Erstveröffentlichung auch bewusst an jeden Internetnutzer adressiert war, kann für diesen Fall kein neues Publikum angenommen werden.
Diese Grundsätze möchte die Beklagte auf die hier zugrundeliegende Sachverhaltskonstellation übertragen wissen. Auch hier sei es so, dass die Fotografie in dem Online-Reisemagazin ohne jegliche Zugangsbeschränkung veröffentlicht wurde. Dadurch richte sich diese Veröffentlichung an alle potentiellen Internetnutzer. Eine erneute Veröffentlichung auf der Schulhomepage könne sich dann nicht an ein neues Publikum richten. Die Situation sei mit der bei der Linksetzung vergleichbar, sodass auch die Grundsätze übertragbar seien.

Der BGH teilt die Argumentation und Ansicht der Beklagten hingegen nicht. Die Entscheidung des EuGH bei der Linksetzung basiere auf der Abwägung zwischen den Interessen des Urhebers und denen der Nutzer von urheberrechtlich geschützten Werken. Für das Funktionieren des Internets seien dabei elektronische Verweise in Form der Hyperlinks von besonderer Bedeutung, um sich in dem Medium zurechtzufinden und zu bewegen. Das Interesse auf einen funktionierenden Meinungs- und Informationsaustauschs übersteige daher das Interesse des Rechteinhabers, das Werk nach seinem Ermessen zu nutzen. Eine vergleichbare Sachlage sei hier jedoch nicht zu erkennen. Für das Funktionieren des Internets und einen regen Meinungs- und Informationsaustausch sei das Kopieren eines Werks auf den eigenen Server und das Einstellen auf eine andere Internetseite nicht erforderlich. Die Interessenabwägung ginge vielmehr zu Gunsten des Urhebers aus, der sein Werk verwerten wolle und von einem hohen Urheberrechtsschutz profitieren möchte.
Außerdem stellt der BGH die zentrale Rolle des Nutzers eines urheberrechtlich geschützten Werks heraus. Bei der Linksetzung habe der Linksetzende keine abschließende Kontrolle über das verlinkte Werk. Allein der Betreiber der ersten Internetseite – der mit Erlaubnis des Rechteinhabers agiere – könne darüber entscheiden, ob das Werk im Internet abrufbar sei oder nicht. Werde das Werk von der ersten Internetseite gelöscht, gehe der Link ins Leere und der Linksetzende könne das Werk keinem mehr zugänglich machen. Im hier zu entscheidenden Fall nehme die Beklagte hingegen eine zentrale Rolle bei der öffentlichen Zugänglichmachung ein. Durch das Kopieren der Fotografie auf den Server und das Einstellen auf der Schulhomepage könne sie alleine darüber entscheiden, ob die Fotografie Dritten zugänglich gemacht werde. Auch bei einer Löschung des Bildes von der Internetseite des Online-Reisemagazins wäre es weiterhin auf der Schulhomepage abrufbar. Der Rechteinhaber könne somit nicht mehr alleine entscheiden, ob das Bild abrufbar ist. Das Gericht sieht in der Handlung der Beklagten daher vielmehr eine eigenständige Verwertungshandlung, die der Erlaubnis des Rechteinhabers bedürfe.

Aus diesen Gründen lehnt der BGH eine Übertragung der Grundsätze zur Linkhaftung des EuGH auf diese Fallkonstellation ab. Zugleich stellt der BGH jedoch fest, dass die Frage auch unter Berücksichtigung der bisherigen Rechtsprechung des EuGH nicht zweifelsfrei abschließend beantwortet werden könne. Da die Regelung zum Recht der öffentlichen Zugänglichmachung auf einer europäischen Richtlinie beruht, obliege es daher dem EuGH die Frage abschließend zu beantworten. Deshalb legt das Gericht die Frage der Übertragbarkeit der Grundsätze dem EuGH vor und unterlässt eine abschließende Endscheidung zu diesem Zeitpunkt.

IV. Fazit und Konsequenzen für die Hochschulen

Die Vorlage des BGH an den EuGH ist die Fortsetzung einer Reihe höchstrichterlicher Entscheidungen auf nationaler und europäischer Ebene zum Urheberrecht im digitalen Umfeld. Die Entscheidung des BGH zur Vorlage ist dabei im Ergebnis zu begrüßen. Eine endgültige Entscheidung hat – unabhängig in welche Richtung sie geht – weitreichende Auswirkungen, die es nicht zu unterschätzen gilt.

Auch wenn das Interesse der Beklagten auf Übertragung der Grundsätze auf die vorliegende Konstellation nachvollziehbar ist, erscheinen die vom BGH angeführten Argumente gegen eine solche Übertragbarkeit überzeugend. Die Kopie eines Bildes auf den eigenen Server mit der anschließenden Veröffentlichung auf der eigenen Homepage ist nicht vergleichbar mit einem Link zu einem urheberrechtlich geschützten Werk. Vor allem der Kontrollverlust des Rechteinhabers über sein Werk führt zu einer Situation, die eine andere rechtliche Beurteilung erfordert. Eine Übertragung der genannten Grundsätze würde die Position des Rechteinhabers erheblich schwächen und zu einem Absenken des Schutzniveaus des Urheberrechts führen. Gerade bei der stetig wachsenden und schon jetzt erheblichen

Bedeutung des Internets würde das quasi zu einem Schutzverlust des Urhebers führen, sobald das urheberrechtlich geschützte Werk einmal mit Erlaubnis veröffentlicht wurde. Ein gerechter Interessenausgleich würde durch eine so weitreichende Konsequenz gefährdet.

Für die Hochschulpraxis haben die Vorlagefragen des BGH zunächst einmal keine direkten Auswirkungen. An der Rechtslage ändert sich durch sie erst einmal nichts. Es gilt der Grundsatz der Vorsicht bei der Verwendung von Werken, die aus dem Internet beschafft werden. Ohne eine explizite Erlaubnis des Rechteinhabers sollten Bilder oder andere Werke nicht vorschnell kopiert und für eigene Zwecke auf Internetseiten veröffentlicht werden. Zumindest eine sorgfältige Klärung der Rechtslage an dem Werk sollte in jedem Fall erfolgen. Dennoch sollten die Hochschulen die Entwicklung in dieser Rechtssache verfolgen. Es geht hierbei um eine Fragestellung, die sich der ein oder andere Mitarbeiter schon einmal gestellt haben dürfte und die auch nicht gänzlich von der Hand zu weisen ist. Eine Entscheidung durch den EuGH führt daher zu Rechtssicherheit in einer Frage, die aufgrund der Vielfältigkeit des Internets und den daraus resultierenden Möglichkeiten nicht unerheblich ist. Der BGH hat mit seinen Ausführungen zwar angedeutet, welche Rechtsauffassung er vertritt, die abschließende Klärung erfolgt jedoch erst durch den EuGH und darf mit Spannung erwartet werden.

Weiterführende Hinweise

Bei der Frage, ob die vom EuGH aufgestellten Grundsätze auf die vorliegende Fallkonstellation übertragen werden könne, beziehen sich sowohl die Beklagte im Rahmen ihrer Argumentation als auch der BGH in seiner Begründung auf die Entscheidungen des EuGH zu Hyperlinks und zum sogenannten Framing. Zu Zwecken der einfacheren Lesbarkeit wird in diesem Infobrief aber nur auf die Entscheidung zu den Hyperlinks ausdrücklich Bezug genommen.

Zur Rechtsprechung des EuGH zur Haftung für Hyperlinks siehe Strobel, „Links, Links, Links und immer noch nicht der rechte Weg?“, in: DFN-Infobrief Recht 11/2016.

Zur Rechtsprechung des EuGH zur Haftung für Framelinks siehe Hinrichsen, „Alles bleibt im Rahmen!“, in: DFN-Infobrief Recht 12/2014.

Wer hat noch nicht, wer will noch mal?

Gesetzgeber schafft Störerhaftung für WLAN-Betreiber ab und führt Sperrverpflichtungen ein

von Florian Klein

Der Umfang der Haftung von WLAN-Betreibern für Rechtsverletzungen ihrer Nutzer ist seit einigen Jahren ein stark umstrittenes Thema unter Juristen. Die daraus resultierende Rechtsunsicherheit hat dafür gesorgt, dass offene WLAN-Netze in Deutschland noch immer ein seltenes Angebot sind. Um die Hemmschwelle für potenzielle WLAN-Betreiber im Hinblick auf das Angebot eines WLAN zu senken, hat der Gesetzgeber nun endlich ausdrücklich die sogenannte Störerhaftung von Access-Providern abgeschafft. Doch dieser erfreuliche Schritt hat einen hohen Preis: zeitgleich mit der Haftungsbefreiung wird gesetzlich verankert, dass WLAN-Betreiber unter bestimmten Voraussetzungen zur Sperrung der Nutzung von Informationen verpflichtet sein können.

I. Ausgangslage und Gesetzgebungsverfahren

Gelegentlich kommt es vor, dass Nutzer eines fremden WLAN dieses missbrauchen, um im Internet Rechtsverletzungen zu begehen. Hierbei sind vielfältige Arten von Verletzungen denkbar. Praktisch geht es zuvorderst um Verletzungen von Rechten des geistigen Eigentums (insbesondere Urheberrechte), aber auch Verletzungen des Persönlichkeitsrechts beispielsweise durch Beleidigungen oder Diffamierungen sind an der Tagesordnung. Bei offenen WLANs ist es für den Rechteinhaber oder Betroffene in der Regel nicht möglich zu ermitteln, wer die Verletzung begangen hat, soweit keine Nutzerregistrierung und entsprechende Datenspeicherung im WLAN erfolgt. Deshalb war es für die Rechteinhaber fraglich, ob sie stattdessen gegen den Betreiber des WLAN, dessen IP-Adresse ermittelbar ist, vorgehen können und ob dieser für die Rechtsverletzungen seiner Nutzer haftet. Dabei ging es nicht nur um die Frage, ob der WLAN-Betreiber eine Pflicht hatte, etwaige Abmahnkosten zu erstatten, sondern auch ob der Rechteinhaber vom WLAN-Betreiber verlangen kann, bestimmte Webseiten oder Inhalte mithilfe von Netzsperren zu sperren oder andere Sicherheitsvorkehrungen zu treffen. Als solche wurden insbesondere eine Verschlüsselung des WLAN, eine Registrierung der Nutzer oder die Einrichtung einer Vorschaltseite mit einer Verpflichtungserklärung des Nutzers über die Einhaltung des geltenden Rechts diskutiert. Rechtsgrundlage für einen entsprechenden Anspruch der Rechteinhaber sollte die von der Rechtsprechung entwickelte Störerhaftung sein, wonach als Störer jeder haftet, der ohne Täter oder Teilnehmer zu sein in irgendeiner Weise willentlich und adäquat kausal zur Verletzung des geschützten Rechtsguts beiträgt. Ein Störer kann dann vom Rechteinhaber auf Unterlassung und Beseitigung der Rechtsverletzung in Anspruch genommen werden, sofern er zumutbare Prüfpflichten verletzt hat. Wie weit diese Störerhaftung jedoch im Einzelfall reichte, welche konkreten (Unterlassungs-)Pflichten sich aus ihr ergeben konnten und was noch als zumutbar angesehen werden konnte, war in hohem Maße unklar. Daher bestand eine erhebliche Rechtsunsicherheit für WLAN-Betreiber, die als Störer angesehen wurden, weil die konkrete Rechtsverletzung überhaupt erst durch die Bereitstellung des WLAN ermöglicht wurde.

Diese unklare Rechtslage war bisher der primäre Grund dafür, dass sich Deutschland zu einer „Wüste“ für offene WLANs entwickelt hat, da nur wenige bereit waren, die kaum kalkulierbaren Haftungsrisiken zu tragen. Nicht zuletzt deshalb wurde die Störerhaftung immer wieder kritisiert und der Ruf nach dem Gesetzgeber wurde laut. Dieser wollte sich der Problematik auch vermeintlich annehmen und schuf das „Zweite Gesetz zur Änderung des Telemediengesetzes“, welches im Juli 2016 in Kraft trat. Dabei handelte es sich jedoch bestenfalls um einen halbherzigen Kompromiss der Großen Koalition, die das Ziel der Abschaffung der Störerhaftung nicht ausdrücklich ins

Gesetz schrieb, sondern nur in die Gesetzesbegründung und damit wohl ihr Ziel verfehlte. Kurz danach überraschte nämlich der Europäische Gerichtshof im September 2016 mit seiner Entscheidung im Fall „McFadden", in welcher er ausdrücklich klarstellte, dass das EU-Recht Unterlassungsansprüche gegen WLAN-Anbieter zulässt, die insbesondere durch eine Sicherung des Netzes und eine Identifizierung der Nutzer erfüllt werden könnten (s. hierzu Klein, „Oft büßt das Gute ein, wer Besseres sucht", in: DFN-Infobrief Recht 10/2016). Damit hatte das deutsche Instrument der Störerhaftung mittelbar einen starken Unterstützer gefunden, sodass wieder einmal unklar war, ob sich die nur in der Gesetzesbegründung eindeutig manifestierte Absicht der Abschaffung der Störerhaftung vor Gerichten würde durchsetzen können. Aus diesem Grund hat die Bundesregierung im April 2017 und damit kurz vor Ablauf der Legislaturperiode mit dem Entwurf eines Dritten Gesetzes zur Änderung des Telemediengesetzes einen erneuten Anlauf gestartet, um die entstandene Rechtsunsicherheit endgültig zu beseitigen und damit in Deutschland den Weg für eine flächendeckende Versorgung mit offenen WLANs frei zu machen. Nach einigen kleinen Änderungen erfolgte die Verabschiedung des Gesetzes im Bundestag am 30.06.2017 und damit an dessen letztem Sitzungstag vor der Bundestagswahl. Nachdem das Gesetz auch im Bundesrat in dessen Sitzung am 22.09.2017 nicht beanstandet und der Vermittlungsausschuss nicht angerufen wurde, konnte es am 12.10.2017 im Bundesgesetzblatt verkündet werden und am 13.10.2017 schließlich in Kraft treten.

II. Inhalt der Gesetzesänderung

Neben der ausdrücklichen Abschaffung der Störerhaftung führt die Gesetzesänderung eine Rechtsgrundlage ein, aufgrund derer eine Verpflichtung von WLAN-Betreibern zur Einrichtung von Sperren entstehen kann. Außerdem regelt sie die Kostenverteilung.

Abschaffung der Störerhaftung und Einschränkung behördlicher Anordnungen

§ 8 Abs. 1 S. 2 Telemediengesetz (TMG) bestimmt nun ausdrücklich, dass Zugangsdiensteanbieter wegen rechtswidriger Handlungen ihrer Nutzer nicht auf Schadensersatz, Beseitigung oder Unterlassung in Anspruch genommen werden können, sodass sich diese Regelung wie ein Schild zwischen Rechteinhaber und WLAN-Betreiber schiebt. Für eine Störerhaftung, die auf Unterlassung und Beseitigung gerichtet war, bleibt somit kein Raum mehr, sodass diese im Hinblick auf Access-Provider als abgeschafft betrachtet werden kann. Dieser vollständige Haftungsausschluss gilt jedoch nur in Fällen, in denen der Diensteanbieter nicht verantwortlich ist, womit auf die Regelung in § 8 Abs. 1 S. 1 TMG Bezug genommen wird: Voraussetzung ist somit zusätzlich, dass der Diensteanbieter bloß fremde Informationen in einem Kommunikationsnetz übermittelt oder den Zugang zur Nutzung vermittelt und dabei weder die Übermittlung veranlasst noch den Adressaten der Übermittlung auswählt oder die übermittelten Informationen auswählt oder verändert. Er darf somit keinen Einfluss auf die übermittelten Inhalte nehmen, sondern muss sich auf die bloß technische, automatische und passive Tätigkeit der Diensterbringung beschränken, weil es nur dann berechtigt ist, ihn haftungsrechtlich zu privilegieren.

Gültig ist der Haftungsausschluss zudem nicht nur für WLAN-Betreiber, sondern für alle Diensteanbieter im Sinne des § 8 TMG, also für alle Betreiber von Kommunikationsnetzen und Anbieter von Zugängen zu Kommunikationsnetzen wie dem Internet. In diesen Fällen einer rein technischen Zugangsvermittlung ist weder eine Haftung auf Schadensersatz noch auf Unterlassung möglich. Zu beachten ist jedoch, dass der Haftungsausschluss dadurch relativiert wird, dass gleichzeitig in bestimmten Grenzen Netzsperren ermöglicht werden. Schließlich gilt der Haftungsausschluss des § 8 Abs. 1 S. 2 TMG gemäß § 8 Abs. 1 S. 3 TMG nicht bei einem kollusiven Zusammenwirken, das heißt, wenn Diensteanbieter und Nutzer absichtlich zusammenarbeiten, um rechtswidrige Handlungen zu begehen. Dabei handelt es sich jedoch um eine übliche Ausnahme, die nur dazu dient, einen Missbrauch der privilegierenden Regelungen auszuschließen.

Neu eingefügt wird außerdem die Regelung des § 8 Abs. 4 TMG, der vom Wortlaut her zunächst einmal regelt, was Behörden gegenüber WLAN-Betreibern – nicht aber generell gegenüber Access-Providern – nicht anordnen dürfen. So dürfen Behörden einen WLAN-Betreiber nicht dazu verpflichten, vor Gewährung des Zugangs die persönlichen Daten von Nutzern zu erheben und zu speichern (Nutzerregistrierung) oder die Eingabe eines Passworts zu verlangen. Die vom EuGH im Fall McFadden als EU-rechtlich zulässig eingestuften Maßnahmen werden somit ausgeschlossen, um die Existenz offener WLANs zu sichern.

Eine unmittelbare Beanstandung des neuen Gesetzes durch den EuGH ist allein deswegen jedoch nicht zu erwarten, da er nur die europarechtliche Zulässigkeit dieser Maßnahmen festgestellt hat, ohne deren Einsatz zwingend anzuordnen. Insofern ist auch zu bedenken, dass der Prüfungsumfang des EuGH aufgrund prozessualer Vorgaben in dieser Entscheidung auf drei konkrete Maßnahmen beschränkt war und er nicht generell alle denkbaren Möglichkeiten prüfen konnte. Außerdem dürfen Behörden gemäß § 8 Abs. 4 Nr. 2 TMG nicht die dauerhafte Einstellung des Dienstes verlangen. Zu Recht wird insoweit kritisiert, dass dies offensichtlich Anordnungen zur vorübergehenden Sperrung nicht ausschließt. Solche könnten dann insbesondere auf ordnungs- und polizeirechtlicher Grundlage zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung erfolgen, bedürften aber stets einer hinreichend konkreten landesrechtlichen Ermächtigungsgrundlage. Unabhängig von dieser Einschränkung der behördlichen Befugnisse bleiben solche Maßnahmen auf freiwilliger Basis aber möglich, sodass niemand gezwungen ist, beispielsweise ein WLAN ohne Passwortsicherung anzubieten. Auch die vorübergehende oder dauerhafte Einstellung des Dienstes steht natürlich weiterhin im Ermessen des Anbieters.

Aus der Gesetzesbegründung ergibt sich zudem ausdrücklich, dass die Beschränkung dieses Verbots zur Anordnung solcher Maßnahmen auf Behörden bewusst erfolgt ist. Hätte der Gesetzgeber allgemein festgeschrieben, dass die Anordnung solcher Maßnahmen unzulässig ist, wäre niemand dazu befugt gewesen, was zwischenzeitlich auch vom Bundesrat gefordert wurde. So sollen aber nun zumindest Gerichte in der Lage sein, entsprechende Maßnahmen anzuordnen, wobei jedoch fraglich ist, auf welcher Rechtsgrundlage das erfolgen sollte, da die Störerhaftung ja gerade ausgeschlossen ist und auch Gerichte stets eine gesetzliche Grundlage für Anordnungen benötigen. Die Bundesregierung scheint hier die noch zu erörternde Norm des § 7 Abs. 4 TMG als Rechtsgrundlage sehen zu wollen, in welcher es um die Sperrverpflichtung der WLAN-Betreiber geht. Allerdings räumt diese allenfalls einen Anspruch auf Sperrung der Nutzung von Informationen ein. Inwiefern dies beispielsweise durch eine Nutzerregistrierung verwirklicht werden soll, erschließt sich nicht. Hier ist also die Entwicklung in der Rechtsprechung abzuwarten. Unabhängig davon werden wohl auch Gerichte in aller Regel keine dauerhafte Einstellung des WLAN-Betriebs anordnen können, da dies der Rechtsprechung des EuGH zuwiderlaufen würde, der eine solche Maßnahme als unverhältnismäßig angesehen hat.

Einführung von Netzsperren

Ein Novum in der Geschichte des TMG ist neben dem ausdrücklichen Ausschluss der Störerhaftung, dass in § 7 Abs. 4 TMG explizit eine Gesetzesgrundlage für die Verpflichtung von WLAN-Betreibern zur Einrichtung von Sperren geschaffen wird. Dabei handelt es sich um eine Art Kompromiss, mit dem ein Ausgleich der betroffenen Interessen hergestellt werden soll, weil auch die Rechteinhaber nicht vollkommen schutzlos gestellt werden dürfen. Mangels Registrierung der Nutzer und einer Haftung des WLAN-Betreibers wäre es für die Rechteinhaber in vielen Fällen unmöglich, Rechtsverletzungen zu verfolgen. Ihr Recht am geistigen Eigentum ist jedoch sowohl verfassungsrechtlich als auch auf Ebene der EU-Grundrechte besonders geschützt und gebietet es deshalb zwingend, dass man ihnen gewisse Schutzinstrumente an die Hand gibt. Der nun gefundene Kompromiss besteht also darin, dass zwar eine Haftung des WLAN-Betreibers ausgeschlossen wird, dieser aber im Gegenzug unter bestimmten Voraussetzungen zu Sperrmaßnahmen verpflichtet wird, um Nutzern Rechtsverletzungen zu erschweren.

§ 7 Abs. 4 TMG besagt, dass der Rechteinhaber vom WLAN-Betreiber, dessen WLAN von einem Nutzer für eine Verletzung von dessen geistigen Eigentumsrechten verwendet wurde, die Sperrung der Nutzung von Informationen verlangen kann. Anspruchsgegner und damit potenziell zur Einrichtung von Sperrmaßnahmen Verpflichtete sind nicht alle Access-Provider, sondern ausschließlich WLAN-Betreiber, sodass gerade die Betreiber der Kommunikationsnetze und Anschlussanbieter aufgrund des für sie geltenden vollumfänglichen Haftungsausschlusses nicht mehr zur Einrichtung von Netzsperren verpflichtet werden können. Der Anspruch kann erst entstehen, wenn ein Nutzer über das WLAN ein Recht am geistigen Eigentum verletzt hat, wozu insbesondere Urheberrechte gehören, nicht aber Persönlichkeitsrechte. Außerdem darf der Rechteinhaber keine andere Möglichkeit haben, der Verletzung des Rechts abzuhelfen. Daraus ergibt sich, dass – soweit möglich – vorrangig tatnähere Akteure (z. B. der Nutzer, sein Host-Provider o. ä.) in Anspruch genommen werden müssen, was zumutbare Anstrengungen des Rechteinhabers zu deren Ermittlung erfordert, wie z. B. die Einschaltung von Privatdetektiven oder auch der Strafverfolgungsbehörden. Erst wenn deren Inanspruchnahme scheitert oder ihr jede Erfolgsaussicht fehlt, sodass andernfalls eine Rechtsschutzlücke entstünde, ist ein Vorgehen gegen den WLAN-Betreiber zulässig. Die erforderliche Wiederholungsgefahr dürfte in der Regel

durch die erstmalige Rechtsverletzung indiziert sein. Schließlich muss die Sperrung noch zumutbar, verhältnismäßig und natürlich technisch möglich sein. Dabei sind dann insbesondere Aufwand, Kosten und Größe des WLAN-Betreibers zu berücksichtigen, was gerade an Hochschulen in besonderem Maße die Einbeziehung der Wissenschaftsfreiheit und der speziellen Anforderungen von Forschung und Lehre erfordert. Im Rahmen der notwendigen Einzelfallabwägung muss außerdem das Fernmeldegeheimnis und die Gefahr eines Overblocking berücksichtigt werden, weil die Maßnahmen nicht über ihr Ziel hinausschießen dürfen. Liegen diese Voraussetzungen vor, kann der Rechteinhaber die Sperrung der Nutzung von Informationen verlangen.

Als Maßnahme zur Umsetzung dieses Anspruchs stellt sich der Gesetzgeber beispielsweise die Sperrung bestimmter Ports am Router vor, um den Zugang zu Peer-to-Peer-Netzwerken zu verhindern und damit eine Tauschbörsennutzung zu blockieren. Problematisch ist daran jedoch, dass Portsperren fast immer zu einem Overblocking, also einer unberechtigten Mitsperrung rechtmäßiger Inhalte, führen, da gerade über die von Tauschbörsen genutzten Ports auch zahlreiche rechtmäßige Inhalte verteilt werden. Eine solche Portsperre dürfte deshalb nur selten ein zumutbares Mittel der Sperrung sein. Eine andere Variante soll das Sperren des Zugriffs auf eine bestimmte Webseite am Router sein. Hier könnten möglicherweise Dateien herausgegeben werden, die auf den Router aufgespielt werden können, so wie die Bundesprüfstelle für jugendgefährdende Schriften dies im Hinblick auf Belange des Jugendschutzes tut. Die vorgeschlagenen Maßnahmen sind für technische Laien jedoch häufig relativ kompliziert und aufwändig, zumal Portsperren gerade durch Tauschbörsenanbieter umgangen werden können. Darüber hinaus erscheint es bedenklich, wenn WLAN-Betreiber mit dem Aufwand belastet werden, die Routersoftware zur Blockade von Webseiten kontinuierlich anzupassen. Als dritte Variante wurden schließlich noch schlichte Datenmengenbegrenzungen vorgeschlagen. Dem ist zuzugeben, dass für viele typische Urheberrechtsverletzungen im Bereich der Musik und des Films größere Datenmengen benötigt werden. Doch gibt es ebenfalls zahlreiche rechtmäßige Anwendungen, bei denen große Datenmengen anfallen, sodass eine solche Maßnahme den Nutzen flächendeckender freier WLANs wiederum erheblich einschränken würde. Gerade im Wissenschaftsbereich, in welchem häufig große Datenmengen beim Austausch von Forschungsergebnissen übermittelt werden, erscheint eine solche Maßnahme als ungeeignet. Da somit alle drei beispielhaft genannten Maßnahmen Bedenken unterliegen, bleibt fraglich, in welcher Form die Sperrung der Nutzung von Informationen erfolgen kann. Der Rechtsanwender kann hier nur auf eine (unbefriedigende) Einzelfallprüfung verwiesen werden. In dieser müssen einerseits die Intensität der Rechtsverletzung und andererseits der Aufwand und die technischen, finanziellen und organisatorischen Möglichkeiten des WLAN-Betreibers gegenübergestellt und zu einem Ausgleich gebracht werden. Denn die Sperrverpflichtung steht unter dem Vorbehalt der Zumutbarkeit und Verhältnismäßigkeit, welcher sich in besonderem Maße auf den Umfang der Verpflichtung auswirkt.

Die Gesetzesmaterialien vermitteln an einigen Stellen den Eindruck und die Absicht, dass die Verpflichtung zur Einrichtung von Sperren erst mit gerichtlicher Anordnung entstehen soll, damit im Einzelfall die komplexe Interessenabwägung durch staatliche Stellen erfolgt. Eine solche Beschränkung findet sich im Gesetzeswortlaut aber nicht eindeutig. Deshalb ist davon auszugehen, dass die Verpflichtung des WLAN-Betreibers schon allein aufgrund des Gesetzes besteht und nicht erst einer Konkretisierung durch ein Gericht bedarf, sobald die materiellen Anspruchsvoraussetzungen erfüllt sind. Hier hat es der Gesetzgeber leider versäumt, die nötige Rechtssicherheit für WLAN-Betreiber dadurch zu schaffen, dass die Verpflichtung tatsächlich erst mit Erlass einer gerichtlichen Anordnung nach einer Einzelfallprüfung entsteht. Dem WLAN-Betreiber wird somit in gewisser Weise die Richterrolle aufgedrängt, wenn er mit einem Sperrverlangen eines Rechteinhabers konfrontiert wird.

Kostenverteilung

Das neue Gesetz äußert sich deutlich zur Frage, welche Kostenlasten den WLAN-Betreiber noch treffen können. Korrespondierend mit der vollständigen Abschaffung der Störerhaftung können von Access-Providern gemäß § 8 Abs. 1 S. 2 TMG keinerlei Kosten, also weder vorgerichtliche, außergerichtliche noch gerichtliche, für die Geltendmachung von Schadensersatz-, Unterlassungs- oder Beseitigungsansprüchen gefordert werden. Dies ist allerdings ohnehin selbstverständlich, da schon nach allgemeinen Grundsätzen keine Kostenerstattung für die Geltendmachung unbegründeter oder nicht existenter Ansprüche vorgesehen ist. Insofern sind nun jedoch ganz klar auch Abmahnkosten ausgeschlossen.

Darüber hinaus regelt das Gesetz in § 7 Abs. 4 S. 3 TMG, dass bezüglich des Anspruchs auf Einrichtung von Sperren – außer im Fall der Kollusion – keine vor- und außergerichtlichen Kosten vom Diensteanbieter gefordert werden können, sodass WLAN-Betreiber auch hier vor der Forderung von Abmahnkosten geschützt sind. Bei genauer Betrachtung der Norm fällt jedoch auf, dass die Tragung gerichtlicher Kosten nicht ausgeschlossen ist. Weigert ein WLAN-Betreiber sich also, auf Verlangen der Rechteinhaber Sperren einzurichten, und wird daraufhin vom Rechteinhaber verklagt, muss der WLAN-Betreiber nach den allgemeinen Regelungen des Zivilprozessrechts die Gerichtskosten tragen, wenn er den Prozess verliert und gerichtlich zur Sperrung verpflichtet wird. Nicht von der Pflicht zur Tragung der Gerichtskosten erfasst sind jedoch die Rechtsanwaltskosten der Rechteinhaber im Prozess, da diese unter die ausgeschlossenen Rechtsverfolgungskosten fallen. Dennoch könnten WLAN-Betreiber zukünftig angesichts des (Gerichts-)Kostenrisikos und des mit einem Prozess verbundenen Aufwandes geneigt sein, etwaigen Sperrverlangen lieber vorschnell Folge zu leisten, als sich auf einen Prozess einzulassen, was zu einem Overblocking und damit zu Einschränkungen der Informationsfreiheit führen könnte. Unklar ist zudem, wie hoch in einem solchen Fall der Streitwert läge, von dem die konkrete Höhe der Gerichtskosten abhängt. Insgesamt lässt sich festhalten, dass durch die neuen Kostenregelungen eine erhebliche Beschränkung des Kostenrisikos für WLAN-Betreiber eintritt, was die Hemmschwelle für die Bereitstellung eines WLAN für die Öffentlichkeit erheblich senken sollte. Einzig zu befürchten ist die Auferlegung von Gerichtskosten nach einer Niederlage vor Gericht. Allerdings ist zweifelhaft, ob in der Praxis noch häufig mit einer gerichtlichen Durchsetzung von Sperransprüchen gegen einzelne WLAN-Betreiber zu rechnen ist. Da Rechteinhaber fortan keinerlei Erstattung von Abmahn- und eigenen Rechtsanwaltskosten mehr vom WLAN-Betreiber verlangen können, haben sie selbst bei einem Obsiegen vor Gericht einen erheblichen Kostenanteil zu tragen. Aus diesem Grund wird ein solches Vorgehen selten wirtschaftlich sein, zumal der Nutzerkreis eines WLAN-Betreibers in der Regel deutlich kleiner ist als der großer Internetzugangsanbieter. Somit ist die Reichweite der Wirkung von Sperrmaßnahmen in einem einzelnen WLAN eher gering, während die Rechtsdurchsetzung nicht unerhebliche Kosten verursachen wird. Dazu kommt, dass auch Rechteinhaber durchaus ein Prozessrisiko tragen, da nur selten wirklich klar sein wird, ob und welche Sperren tatsächlich zumutbar und verhältnismäßig sind, was im Falle einer Fehleinschätzung dazu führen kann, dass sie zusätzlich auch noch die Gerichtskosten oder zumindest Teile davon zahlen müssen.

III. Fazit und Konsequenzen für die Hochschulpraxis

Aus Sicht der Diensteanbieter und potentieller WLAN-Nutzer, die Profiteure einer Angebotsausweitung sind, ist es zunächst erfreulich, dass der Gesetzgeber es endlich geschafft hat, eindeutig und unmissverständlich Unterlassungs- und Beseitigungsansprüche gegen sämtliche Access-Provider auszuschließen und damit der Störerhaftung einen Riegel vorzuschieben. Im Sinne der Rechtssicherheit ist dies ein sehr zu begrüßender Schritt. Letztlich wird die Problematik aber durch die Einführung des neuen Anspruchs auf Einrichtung von Sperren nur von einer Rechtsgrundlage zur anderen verlagert. Statt zu prüfen, ob Sperrmaßnahmen Ausfluss einer zumutbaren Prüfpflicht sein könnten (wie bei der Störerhaftung erforderlich), ergeben sich die vergleichbaren Kriterien der Zumutbarkeit und Verhältnismäßigkeit nun ausdrücklich aus § 7 Abs. 4 S. 2 TMG. Ein Zugewinn verbleibt aber dadurch, dass sonstige Zugangsvermittler, die keine WLANs betreiben, vollständig von der Haftung befreit sind und keine Netzsperren einrichten müssen, auch wenn dies vor dem Hintergrund der Vorgaben des europäischen Rechts zumindest bedenklich erscheint. Außerdem ist klargestellt, dass der Anspruch allenfalls auf die Sperrung der Nutzung von Informationen gerichtet sein kann, während sonstige Maßnahmen wie eine zwingende Passwortsicherung oder Nutzerregistrierung außen vor bleiben.

Der kritischste Punkt ist jedoch sicherlich, dass die Sperrverpflichtung gerade nicht von einer gerichtlichen Anordnung abhängig ist, sodass keine unabhängige Stelle die Umstände des Einzelfalls prüft, bevor Sperren eingerichtet werden müssen. Insofern ist es aufgrund der weiterhin bestehenden Unsicherheiten im Einzelfall für den Rechtsanwender bedauerlich, dass der Gesetzgeber nicht auf das Modell des urheberrechtlichen Auskunftsanspruchs gemäß § 101 Abs. 9 Urheberrechtsgesetz zurückgegriffen hat. Bei diesem darf der in Anspruch genommene Diensteanbieter unter bestimmten Voraussetzungen erst aufgrund einer richterlichen Anordnung Auskunft über Nutzerdaten erteilen und die Kosten für die Anordnung trägt der Rechteinhaber. Insofern bestünde für den WLAN-Betreiber als Diensteanbieter keinerlei Kosten-

risiko und zusätzlich wäre die Entscheidungs-/Prüfungslast auf das Gericht übertragen. Dieses Modell wurde erst kürzlich im Rahmen der Schaffung des sogenannten Netzwerkdurchsetzungsgesetzes noch auf den Anspruch auf Auskunft über Bestandsdaten gegen Diensteanbieter (insbesondere Betreiber sozialer Netzwerke) im neu geschaffenen § 14 Abs. 4 TMG übertragen. Dies spricht ebenfalls dafür, dass es sich um eine bewusste Entscheidung des Gesetzgebers handelt, dass er eine entsprechende Regelung bei WLAN-Anbietern nicht vorgesehen hat. Die Belastung des WLAN-Betreibers mit dem Gerichtskosten- und vor allem dem Entscheidungsrisiko sieht der Gesetzgeber also als angemessen an. Aus Sicht der WLAN-Betreiber ist schließlich die klare Einschränkung der Kostenrisiken ein großer Gewinn, zumal damit die Anreize für die Geltendmachung von Sperransprüchen aufgrund der beschriebenen schlechten Kosten-Nutzen-Bilanz für die Rechteinhaber deutlich gesenkt wurden.

Die aufgezeigten Änderungen gelten für Hochschulen als WLAN-Betreiber in gleichem Maße. Auch für sie steht nun also fest, dass sie für Rechtsverletzungen, die Studenten oder Mitarbeiter über das Hochschul-WLAN begehen, nicht mehr als Störer haften können und Schadensersatz- und Unterlassungsansprüche gegen sie ausgeschlossen sind. Zwar sind sie potenzieller Adressat der neuen Rechtsgrundlage für Sperrverpflichtungen, allerdings haben sie die verfassungsrechtlich stark geschützte Wissenschaftsfreiheit auf ihrer Seite, die voraussichtlich in vielen Fällen entscheidenden Einfluss auf die nötige Interessenabwägung haben und zu einer Unzumutbarkeit oder Unverhältnismäßigkeit von Sperrmaßnahmen führen wird. Somit sollten Sperrforderungen von Rechteinhabern aufgrund von Rechtsverletzungen über das WLAN gerade an Hochschulen sehr sorgfältig und kritisch geprüft und die Auswirkungen etwaiger Sperrmaßnahmen auf den Forschungs- und Wissenschaftsbetrieb untersucht werden, bevor sie vorschnell erfüllt werden und damit ein Overblocking riskiert wird. Im Zweifel kann es ratsam sein, bei entsprechender Beurteilung der Rechtslage durch das Justiziariat eher das Gerichtskostenrisiko in Kauf zu nehmen, als sich dem Vorwurf einer Beschränkung der Informationsfreiheit auszusetzen. Dabei ist auch zu berücksichtigen, dass es im Einzelfall nicht ohne Weiteres ausgeschlossen ist, dass die Nutzer, deren rechtmäßige Inhalte wegen einer voreiligen Sperrung zu Unrecht gesperrt wurden, Schadensersatz- oder zumindest Unterlassungsansprüche gegen die sperrende Institution geltend machen. Rein faktisch dürften Hochschulen jedoch davon profitieren, dass eine Rechtsdurchsetzung für Rechteinhaber gegen WLAN-Anbieter durch das neue Gesetz deutlich unattraktiver geworden ist, sodass das Gesetz für die Hochschulen tendenziell zu einer Erleichterung führt. Insbesondere die klaren Regelungen zum Haftungsausschluss und zur Kostenverteilung tragen so zu einer verstärkten Rechtssicherheit bei. Zu beachten ist schließlich, dass eine Passwortsicherung des WLAN auf freiwilliger Basis weiterhin zulässig ist, sodass daran an Hochschulen aus diversen Gründen, die außerhalb des unmittelbaren Haftungsrechts liegen, festgehalten werden sollte.

Weiterführende Hinweise, insbesondere zur Entwicklung der Störerhaftung von WLAN-Betreibern in Rechtsprechung und Gesetzgebung:

Klein, „Oft büßt das Gute ein, wer Besseres sucht – Europäischer Gerichtshof konkretisiert Haftungsprivilegierung für WLAN-Betreiber“, DFN-Infobrief Recht 10/2016

Sydow, „Privilegierte Störer?“, in: DFN-Infobrief Recht 6/2016

Klein: „Den Letzen beißen die Hunde – Bundesgerichtshof öffnet die Tür für obligatorische Netzsperren durch Access-Provider“, DFN-Infobrief Recht 4/2016

Klein, „Macht die Schotten dicht – oder doch nicht? – Oberlandesgericht Köln hält Verpflichtung zur Einrichtung von Netzsperren durch Internetzugangsanbieter für unzumutbar“, DFN-Infobrief Recht 11/2014

Klein, „Löst dem Internet die Fesseln! – OLG Hamburg verneint Pflicht eines Access-Providers zur Einrichtung von IP-, URL- und DNS-Sperren“, DFN-Infobrief Recht 3/2014

Impressum

Der DFN-Infobrief Recht informiert über aktuelle Entwicklungen in Gesetzgebung und Rechtsprechung und daraus resultierende mögliche Auswirkungen auf die Betriebspraxis im Deutschen Forschungsnetz.

Herausgeber

Verein zur Förderung eines Deutschen Forschungsnetzes e. V.
DFN-Verein
Alexanderplatz 1, D-10178 Berlin
E-Mail: DFN-Verein@dfn.de

Redaktion

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
E-Mail: recht@dfn.de