DFN infobrief recht

1/2020
Januar 2020

Der Feind in meinem Netz – Teil 1

Die Melde- und Benachrichtigungspflichten aus Artikel 33, 34 DSGVO im Zusammenhang mit Emotet-Angriffen

First Rule: You Do Not Talk About Uploadfilter!

Die ungefilterte Wahrheit über Artikel 17 DSM-RL

Vergriffen heißt nicht vergessen

Neuregelung der vergriffenen Werke nach der EU-Urheberrechtsrichtlinie

Der Feind in meinem Netz – Teil 1

Die Melde- und Benachrichtigungspflichten aus Artikel 33, 34 DSGVO im Zusammenhang mit Emotet-Angriffen

von Steffen Uphues

Eine kleine Quizfrage zu Beginn: Was haben die Stadtverwaltung Frankfurt am Main, das Kammergericht (KG) Berlin, die Humboldt-Universität (HU) Berlin und die Heise-Gruppe gemeinsam? Korrekt: Sie alle waren zuletzt – den bisherigen Erkenntnissen bzw. Vermutungen zufolge – Betroffene eines Emotet-Angriffs. In diesem Beitrag und in dem im Februar folgenden zweiten Teil soll dargestellt werden, wie sich ein Emotet-Angriff vollzieht, unter welchen Voraussetzungen der datenschutzrechtlich Verantwortliche einer Meldepflicht nach Art. 33 DSGVO unterliegt (hierzu Teil 1), wie der Meldepflicht nachzukommen ist, wann die betroffene Person gemäß Art. 34 DSGVO zu benachrichtigen ist und welche Konsequenzen die Emotet-Angriffe für die Praxis wissenschaftlicher Einrichtungen beinhalten (hierzu Teil 2).

I. Wie funktioniert Emotet?

Bei Emotet handelt es sich um ein PC-Virenprogramm, das ursprünglich für den Einsatz im Bereich des Online-Bankings konzipiert wurde. Nach dem Durchlaufen mehrerer Evolutionsstufen ist das Programm mittlerweile in der Lage, authentisch erscheinende Mails zu versenden und sich hierdurch Zugang zu Netzen zu verschaffen. Diese verbesserte Vorgehensweise ermöglicht es, Informationen über das potentielle Opfer zu sammeln und dann eine personalisierte und authentisch wirkende Mail zu verschicken. Diese kann dann etwa mit einer Frage zu einem im Anhang befindlichen Dokument versehen sein. Im Fall der Heise-Gruppe war es beispielsweise so, dass ein Mitarbeiter eine Mail erhielt, die dem Anschein nach von einer Kollegin kam und mit der Bitte versehen war, eine angehängte DOC-Datei noch einmal zu überprüfen. Als er die Datei öffnen wollte, erschien die Meldung, dass die aktuelle Word-Version hierzu nicht in der Lage sei und er doch bitte auf „Bearbeiten erlauben“ klicken solle. Dem kam der Mitarbeiter nach, wodurch der PC mit Emotet infiziert wurde. Sobald sich der Angreifer Zutritt zum Netzwerk verschafft hat, besteht die Gefahr, dass er Zugangsdaten abgreift oder an Kontakte des Betroffenen authentisch wirkende Mails verschickt, um weitere Konten zu befallen.

Sobald Emotet in ein Netz eingedrungen ist, werden in der Folge zumeist weitere Schadprogramme auf den PC nachgeladen. Bei dieser Schadsoftware handelt es sich unter anderem um „Trick-Bots“. Mit Hilfe dieser kann sich ein Eindringling Zugangsdaten beschaffen. Interessant wird dies für Eindringlinge im Zusammenhang mit Hochschulen und Forschungseinrichtungen vor allem dann, wenn die interne IT-Abteilung eine Verdachtsmeldung eines Nutzers erhält und sich im Rahmen der Untersuchung selbst an einem befallenen PC anmeldet. Hierdurch kann der Eindringling Zugang zu den Daten der IT-Abteilung erhalten und in der Folge auch deren Befugnisse nutzen, um etwa Daten zu löschen oder zu verändern. Daneben breitet sich der Virus – sobald ein Netzwerk einmal befallen ist – vor allem über internen Mail-Verkehr schnell aus. Als weitere Schadsoftware kann beispielsweise noch ein Verschlüsselungs-Trojaner (z. B. Ryuk) installiert werden, um den Betroffenen zu einer Zahlung von Lösegeld zu bewegen. So hat die Stadtverwaltung Alsfeld zu Beginn dieses Jahres nach einem Angriff ein Erpresserschreiben erhalten. Gegen einen Lösegeldbetrag, der in Bitcoin zu zahlen sei, würden verschlüsselte Daten wieder freigegeben werden. Vereinfacht ausgedrückt könnte man demnach sagen, dass Emotet gewissermaßen als „Türöffner“ fungiert, der den Einsatz weiterer Schadprogramme ermöglicht.

II. Aktuelle Emotet-Angriffe

In letzter Zeit werden immer wieder Emotet-Angriffe öffentlich gemacht. Dabei sind die unterschiedlichsten Institutionen betroffen. Die Folgen der oben angesprochenen Angriffe hatten unterschiedliche Intensitäten; teilweise brachten sie für die Beteiligten verheerende Folgen mit sich. Bei der Stadtverwaltung Frankfurt am Main wurden zunächst die Amtsstuben geschlossen, da aus Sicherheitsgründen alle PCs heruntergefahren worden waren. Die Webseite der Stadt war jedoch relativ zügig wieder erreichbar und auch der Bürobetrieb konnte zeitnah wiederaufgenommen werden. Das KG Berlin wurde im letzten September zum Opfer einer Emotet-Attacke. Noch heute ist die Einrichtung lediglich telefonisch, mittels Fax oder über den Postweg zu erreichen – Mail-Kontakt mit dem Gericht ist nicht möglich.
Die HU Berlin war im letzten November Adressat eines Angriffs mittels Emotet. Der ganz große Kelch scheint jedoch an der Universität vorbeigegangen zu sein. Der Virus hatte wohl nur einen Bruchteil der Accounts befallen und die Handlungsfähigkeit der Einrichtung war nicht erheblich beeinträchtigt.
Schon zuvor – nämlich im letzten Sommer – war die Heise-Gruppe betroffen. Bemerkenswert ist, wie transparent das Unternehmen mit dem Angriff umgeht. Auf der eigenen Webseite findet sich hierzu ein langer Artikel sowie ein ausführliches Video-Interview zu dem Thema. Daneben bietet das Unternehmen auch Webinare an, um anderen Einrichtungen beim Umgang mit Angriffen zu helfen und diesen vorzubeugen. Betroffene Einrichtungen konnten dadurch erste Erkenntnisse über den Umgang mit Emotet gewinnen.

III. Sinn und Zweck der Meldepflicht aus Art. 33 DSGVO

An verschiedenen Stellen legt die DSGVO dem Verantwortlichen Pflichten auf. Art. 32 DSGVO verpflichtet den Verantwortlichen etwa dazu, bei einer Datenverarbeitung ein dem Risiko angemessenes Schutzniveau zu gewährleisten; die Norm dient somit bezüglich des Schutzes personenbezogener Daten zur Prävention. Hieran knüpft Art. 33 DSGVO an und befasst sich mit der Frage, wie zu verfahren ist, sofern es zu einer Verletzung des Schutzes von personenbezogenen Daten gekommen ist. In Art. 33 Abs. 1 DSGVO ist für diesen Fall eine Meldepflicht des Verantwortlichen an die zuständige Aufsichtsbehörde festgelegt, deren Vorliegen sich vor allem danach bestimmt, ob es voraussichtlich zu einem Risiko für die betroffene Person kommt.

Um den Sinn und Zweck der Meldepflicht aus Art. 33 DSGVO herauszustellen, bedarf es eines Blickes auf das Zusammenspiel mit weiteren DSGVO-Normen: Die Einhaltung der durch die DSGVO getroffenen Regelungen zu überwachen und durchzusetzen, ist nach Art. 51 Abs. 1 DSGVO primäre Aufgabe der datenschutzrechtlichen Aufsichtsbehörden. Zur Erfüllung dieser Aufgabe darf sie sich der mannigfaltigen Befugnisse aus Art. 58 DSGVO bedienen. Diese Norm unterstützt die Arbeit der Aufsichtsbehörden, indem diesen zur Ermittlung von DSGVO-Verstößen verschiedene Maßnahmen gestattet werden. Insbesondere die Untersuchungsbefugnisse aus Art. 58 Abs. 1 DSGVO beabsichtigen, einer Informationsasymmetrie zwischen den Verantwortlichen und den Aufsichtsbehörden entgegenzuwirken. Dieselbe Zielrichtung verfolgt auch die Pflicht aus Art. 33 DSGVO. Das Wissen von einem möglichen Verstoß gegen Sicherheitsbestimmungen der DSGVO ist eine Grundvoraussetzung für die Aufsichtsbehörden, um gegen diese vorzugehen.

Die Meldepflicht soll jedoch nicht nur eine Sanktionierung des Verantwortlichen ermöglichen. Sie soll vielmehr auch präventive Wirkung entfalten. Nachdem eine Verletzung gemeldet wurde, können Gegenmaßnahmen getroffen werden, um zu verhindern, dass sich das Risiko für die Rechte und Freiheiten natürlicher Personen tatsächlich realisiert.

IV. Voraussetzungen der Meldepflicht

1. Verletzung des Schutzes personenbezogener Daten

Notwendige Voraussetzung für eine Meldepflicht des Verantwortlichen ist zunächst eine Verletzung des Schutzes personenbezogener Daten. Eine solche wird in Art. 4 Nr. 12 DSGVO definiert als eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden (Schutzverletzung).

Eine solche Schutzverletzung ist auf Verletzungen der Sicherheit beschränkt. Es geht somit um das Überwinden oder Missachten technischer Sicherheitsvorkehrungen. Eine rechtswidrige Datenverarbeitung stellt dagegen keine Verletzung im Sinne des Art. 4 Nr. 12 DSGVO dar – es handelt sich in einem solchen Fall also zwar um einen Verstoß gegen DSGVO-Regelungen zur Datenverarbeitung, die Meldepflicht aus Art. 33 DSGVO wird hier jedoch nicht ausgelöst.

Bei den personenbezogenen Daten kann es sich – anders als noch in § 42a BDSG-alt – um jegliche Datenkategorie handeln. Somit kann auch in Bezug auf nicht-risikobehaftete Daten eine Verletzung im Sinne des Art. 4 Nr. 12 DSGVO erfolgen.

2. Kenntnisnahme von der Verletzung

Die Meldepflicht wird ausgelöst, sobald der Verantwortliche von der Schutzverletzung Kenntnis nimmt. Liegen dem Verantwortlichen Tatsachen vor, die eine sinnvolle Meldung an die Aufsichtsbehörde ermöglichen, ist von einer solchen Kenntnisnahme auszugehen. Die Schutzverletzung wird objektiv bestimmt, sodass es nicht von Bedeutung ist, ob der Verantwortliche die ihm zur Verfügung stehenden Informationen rechtlich korrekt einordnet. Zwar führt alleine der Verdacht bezüglich einer möglicherweise bestehenden Schutzverletzung gerade noch nicht zu einer Meldepflicht des Verantwortlichen. Man wird jedoch in der Folge Maßnahmen zur Aufklärung dieses Verdachts ergreifen müssen. Im Übrigen dürfte der Verantwortliche juristisch so behandelt werden, als läge eine Kenntnisnahme vor, wenn er sich bewusst solchen Aufklärungsmaßnahmen verweigert.

An dieser Stelle ist noch darauf hinzuweisen, dass bei der Kenntnisnahme auf den Verantwortlichen abzustellen ist. Ein Auftragsverarbeiter ist nicht zu einer Meldung an die Aufsichtsbehörden verpflichtet. Im Bereich der Auftragsverarbeitung führt der Auftragsverarbeiter allerdings die technischen Maßnahmen eigenständig aus und ist somit näher an den technischen Risikoquellen für Verletzungen im Sinne des Art. 4 Nr. 12 DSGVO als der Verantwortliche. Dementsprechend ist es interessengerecht, dass der Auftragsverarbeiter nach Art. 33 Abs. 2 DSGVO den Verantwortlichen über eine Schutzverletzung informieren muss.

3. Risiko für die Rechte und Freiheiten natürlicher Personen

Die grundsätzlich durch eine Schutzverletzung ausgelöste Meldepflicht entfällt nach Art. 33 Abs. 1 S. 1 DSGVO für den Fall, dass von der Verletzung voraussichtlich kein Risiko für die Rechte und Freiheiten natürlicher Personen ausgeht. Der hinter der Ausnahme aus Art. 33 Abs. 1 S. 1 DSGVO stehende Grundgedanke basiert auf dem risikobasierten Ansatz der DSGVO. In der Entstehungsgeschichte der DSGVO zeigten einige Beteiligte durchaus Sensibilität bezüglich der hohen Anforderungen, die in administrativer und bürokratischer Hinsicht an den Verantwortlichen gestellt werden. Der hierdurch entstehende Aufwand solle nur für den Fall gerechtfertigt sein, dass die Pflichten des Verantwortlichen an potentielle Risiken einer Datenverarbeitung geknüpft sind. Eine solche Einschränkung war in den Regelungen der vor Geltungsbeginn der DSGVO maßgeblichen Datenschutz-Richtlinie (DS-RL) nicht vorgesehen. Gewissermaßen geht mit Art. 33 DSGVO eine Korrektur der zuvor sehr weit gefassten Meldepflichten einher.

Es bleibt die Frage, welcher Risikobegriff zugrunde zu legen ist. Dabei sollte der möglicherweise drohende Schaden berücksichtigt werden. Je stärker die Schutzverletzung die Rechte und Freiheiten natürlicher Personen betreffen kann, desto geringere Anforderungen sind an die Eintrittswahrscheinlichkeit zu stellen. Eine meldepflichtige Schutzverletzung liegt daher bei sensiblen Daten im Sinne von Art. 9 DSGVO regelmäßig vor. Bei Datenverarbeitungsvorgängen in Krankenhäusern ist somit aufgrund der Sensibilität der Gesundheitsdaten bei den meisten Schutzverletzungen von einem möglichen Risiko auszugehen. Ähnliches dürfte für Online-Dating-Plattformen gelten. Im Bereich der Forschung ist je nach Datenkategorie ebenfalls eine erhöhte Aufmerksamkeit erforderlich und eine Meldung bei Schutzverletzungen zu empfehlen – so etwa bei Projekten zum politischen Meinungsbild oder bei Langzeitstudien in der Medizin.

Ebenfalls in die Beurteilung miteinzubeziehen ist die Verletzungshandlung. Bei einem vorsätzlichen Eindringen in ein IT-System liegt ein zielgerichteter Angriff vor, bei dem der Angreifer im Regelfall mit Schädigungsabsicht auftritt. Das gesteigerte Risiko für die Betroffenen besteht darin, dass der Angreifer es gerade auf die Realisierung dieses Risikos oder zumindest eine hierauf gerichtete Androhung (Lösegelderpressung) abgesehen hat. In solchen Fällen verfügen die

Angreifer oftmals auch über die technischen Fähigkeiten und Möglichkeiten, eine Vielzahl an Daten zu erlangen und treten nicht selten mit dem Ziel an, den Personen ganz bewusst durch eine Veröffentlichung der Daten oder eine Erpressung gegen Lösegeldforderungen zu schaden.

V. Zwischenfazit

Angriffe mittels Emotet stellen eine neue Herausforderung für die IT-Sicherheit dar und können schwerwiegende Folgen für die Betroffenen haben. Aufgrund der gezielten Angriffe und des mitunter perfiden Vorgehens der Angreifer ist davon auszugehen, dass die Schutzverletzungen in Bezug auf betroffene personenbezogene Daten im Regelfall ein relevantes Risiko darstellen und eine Meldung nach Art. 33 Abs. 1 DSGVO erforderlich machen. Dies gilt insbesondere, sofern sensible Daten im Sinne von Art. 9 Abs. 1 DSGVO betroffen sind.

Hinweis: Dieser Beitrag wird im DFN Infobrief Recht 02/2020 fortgesetzt.

First Rule: You Do Not Talk About Uploadfilter!

Die ungefilterte Wahrheit über Artikel 17 DSM-RL

von Nico Gielen

Dieser Infobrief ist erneut der EU-Urheberrechtsrichtlinie (DSM-RL) gewidmet. Nachdem in der letzten Ausgabe das Text- und Data-Mining (Art. 3 DSM-RL) beleuchtet wurde[1], wird nun das Augenmerk auf Art. 17 DSM-RL gelegt. Diese Vorschrift ist als ehemaliger Art. 13 in den Fokus der Öffentlichkeit gelangt und bildet den umstrittensten Teil der Richtlinie; die Diskussion rund um den Uploadfilter hat zu gar abstrusen Wortgefechten geführt. Der Entwurf der Richtlinie wurde bereits in einem Infobrief dargestellt[2]; nun kann über die endgültige Fassung der Vorschrift berichtet werden. Da eine Richtlinie – anders als eine Verordnung – nicht unmittelbar gilt, muss sie innerhalb der nächsten zwei Jahre von den Mitgliedstaaten umgesetzt werden. Diese haben dabei einen gewissen Spielraum, der hier aufgezeigt werden soll.

I. Hintergrund

Die großen Plattformen des Internets – allen voran YouTube – sind alle erst nach der Jahrtausendwende entstanden. Dennoch galten für solche Plattformen lange keine speziellen Regeln. Blickt man auf den Themenbereich der Haftung, ist dort insbesondere die E-Commerce-RL (EC-RL) hervorzuheben, die die Verantwortlichkeit seither stark für Host-Provider einschränkt. Dies sind Diensteanbieter, die lediglich Speicherplatz bereitstellen, aber keinen Einfluss auf die hochgeladenen Inhalte nehmen. Nach der EC-RL können solche Plattformen demnach für die Inhalte ihrer Nutzer erst selbst verantwortlich werden, wenn sie Kenntnis von deren Rechtswidrigkeit erlangen und die Inhalte nicht unverzüglich entfernen oder den Zugang zu ihnen sperren. Dieses Verfahren – auch als notice and take down bezeichnet – wurde aber ebenfalls auf Online-Plattformen wie YouTube angewendet, die nicht mehr nur rein passive Vermittler waren. Statt nur Speicherplatz zur Verfügung zu stellen, bereiten viele Plattformen die Nutzerinhalte zusätzlich auch auf.

Die nunmehr aus der Zeit geratene Haftungsprivilegierung soll zu einem Missverhältnis zwischen den Einnahmen kommerzieller Plattformen wie YouTube und der Rechteinhaber geführt haben. Insbesondere die Musikindustrie befürwortete, dass diese sog. Wertschöpfungslücke («value gap») durch eine Abmilderung der Haftungsprivilegierung wieder geschlossen werden müsse. Andererseits zweifelten Kritiker bereits das Vorliegen einer Wertschöpfungslücke stark an, weil es an belastbaren Belegen mangelt. In der Rechtsprechung waren gleichwohl Entwicklungen erkennbar, wonach der pauschalen Haftungsprivilegierung teilweise ein Riegel vorgeschoben wurde. Der BGH urteilte, dass sich eine Plattform Inhalte der Nutzer auch zu Eigen machen könne, indem nach außen sichtbar die inhaltliche Verantwortung für die Inhalte übernommen wird. In solchen Fällen sei eine Plattform nicht mehr bloß passiver Vermittler fremder Inhalte, sondern biete selbst Inhalte an und stehe dafür voll in der Haftung (Urteil v. 12.11.2009, Az. I ZR 166/07). Auch der EuGH hielt die Privilegierung nicht für alle Plattformen anwendbar. Sobald eine Plattform hinsichtlich der Inhalte eine „aktive Rolle“ einnehmen würde, die ihr eine Kenntnis oder eine Kontrolle über die Inhalte verschaffe, sollte auch hier die Haftungsprivilegierung entfallen (Urteil v. 12.7.2011, Az. 324/09).

1 Gielen, Die neue urheberrechtliche Schranke zum Text- und Data-Mining, DFN-Infobrief Recht 12/2019.

2 Tiessen, Anfang vom Ende?, DFN-Infobrief Recht 01/2019.

Diese Bemühungen der Rechtsprechung kam der Unionsgesetzgeber entgegen, indem für bestimmte Online-Plattformen (II) die alte Haftungsprivilegierung abgeschafft (III) und eine neue Haftungsprivilegierung entwickelt wurde (IV). Dabei ist insbesondere der Schutz von Jungunternehmen unzureichend ausgefallen (V).

II. Erfasste Online-Plattformen

Art. 17 DSM-RL findet nur Anwendung auf „Diensteanbieter für das Teilen von Online-Inhalten". Dies sind Online-Plattformen, auf die Nutzer große Mengen geschützter Inhalte hochladen, wobei die Plattformen diese Inhalte organisieren und zum Zwecke der Gewinnerzielung bewerben müssen. Bei der Auslegung der „großen Menge" soll unter anderem die Anzahl der hochgeladenen Dateien und die Zielgruppe der Online-Plattform Berücksichtigung finden (ErwGr. 63). Weiterhin sollen nur solche Dienste erfasst werden, die auf dem Markt für Online-Inhalte eine „wichtige Rolle" spielen, indem sie mit anderen Online-Inhaltediensten, wie Audio- und Video-Streamingdiensten, um dieselben Zielgruppen konkurrieren (ErwGr. 62). Erkennbar hatte der Gesetzgeber Dienste wie Spotify und Netflix vor Augen, die das Angebot von YouTube teilweise ersetzen.

Es werden keine Dienste erfasst, deren Hauptzweck ein anderer als der beschriebene ist. Beispielhaft werden aufgezählt: Online-Enzyklopädien, bildungsbezogene und wissenschaftliche Repositorien, Entwicklungs- und Weitergabeplattformen für quelloffene Software, Online-Marktplätze, elektronische Kommunikationsdienste und Cloud-Dienste. Werden Cloud-Dienste allerdings als Piraterie-Plattformen missbraucht, greift Art. 17 DSM-RL gleichwohl (ErwGr. 62).

III. Abschaffung der alten Haftungsprivilegierung

Die Haftungsprivilegierung nach der EC-RL setzt voraus, dass allein der hochladende Nutzer eine urheberrechtliche Nutzungshandlung vornimmt – allein er ist Täter der Urheberrechtsverletzung. Die Plattform, auf die die Inhalte geladen werden, ist demnach kein Täter und kann daher allenfalls auf Unterlassung, nicht aber auf Schadensersatz haften. Der verletzte Rechteinhaber wird also auf die aussichtslose Suche nach dem hochladenden Nutzer verwiesen.

Art. 17 Abs. 1 DSM-RL stellt nun aber für die erfassten Plattformen unzweifelhaft fest: Wer Zugang zu hochgeladenen Inhalten verschafft, nimmt zukünftig selbst eine urheberrechtliche Nutzungshandlung vor. Daher muss diese auch eine Erlaubnis vom Rechteinhaber einholen. Ist dies nicht geschehen, liegt folglich ein Rechtsverstoß des Plattformbetreibers selbst vor – er ist nun Täter. Somit können Rechteinhaber von Plattformbetreibern künftig auch Schadensersatz verlangen. Die Haftungsprivilegierung aus der EC-RL gilt für diese Plattformen nicht mehr.

IV. Die neue Haftungsprivilegierung

Auch das neue Haftungssystem sieht jedoch keine ausnahmslose Haftung der Plattformen vor, sondern enthält einen eigenen Privilegierungstatbestand. In Abs. 4 werden drei Voraussetzungen genannt, die eine Plattform erfüllen muss, um der Haftung zu entgehen:

1. Erlaubnis der Rechteinhaber

Erstens muss die Plattform nachweisen, alle Anstrengungen unternommen zu haben, um die Erlaubnis vom Rechteinhaber einzuholen. Hier stellt sich zunächst die Frage, wann „alle Anstrengungen" unternommen worden sind. Der Begriff ist unbestimmt und wird durch die DSM-RL auch nicht weiter definiert. Der nationale Gesetzgeber kann ihn bei der Umsetzung der DSM-RL dazu nutzen, Einzelfallgerechtigkeit herzustellen. In Übereinstimmung mit dem Grundsatz der Verhältnismäßigkeit könnte beispielsweise zwischen einzelnen Formen von Plattformen differenziert werden. Eine solche Differenzierung könnte an Art. 17 Abs. 5 DSM-RL anknüpfen und die dort genannten Faktoren berücksichtigen: Art, Publikum und Umfang des Dienstes, Art der hochgeladenen Inhalte, Verfügbarkeit geeigneter und wirksamer Mittel und deren Kosten.

Bezogen auf die erste Voraussetzung der Haftungsprivilegierung wäre eine Pflicht, von jedem Rechteinhaber eine Erlaubnis einzuholen, allerdings schlicht unverhältnismäßig. Dies würde zum einen die urheberrechtliche Überprüfung aller hochgeladenen Inhalte und zum anderen die Kontaktierung aller betroffenen Rechteinhaber erfordern. Denkbar sind daher allenfalls Verträge mit Verwertungsgesellschaften, in denen sich Rechteinhaber vereinigt haben. Dann können die

Plattformbetreiber mit den Verwertungsgesellschaften Verträge über die Nutzungsrechte gebündelt schließen. Allerdings sind auch nicht alle Rechteinhaber in Verwertungsgesellschaften vereinigt. Um dieses Problem zu lösen, wird die kollektive Lizenzvergabe mit erweiterter Wirkung nach Art. 12 Abs. 1 DSM-RL diskutiert. Dadurch soll Verwertungsgesellschaften ermöglicht werden, Lizenzvereinbarungen auch für solche Rechteinhaber abschließen zu können, die diesen kein Mandat erteilt haben. Allerdings wird dieser Lösungsansatz bezweifelt, weil die kollektive Lizenzvergabe mit erweiterter Wirkung primär im Zusammenhang mit vergriffenen Werken diskutiert worden ist.[3]

2. Gewährleistung der Nichtverfügbarkeit (Uploadfilter)

Zweitens muss die Plattform alle Anstrengungen unternommen haben, um zu gewährleisten, dass die geschützten Inhalte, für die keine Erlaubnis eingeholt werden konnte, nicht verfügbar sind. Dies hat insbesondere eine Frage provoziert: Verpflichtet die DSM-RL zur Implementierung von Uploadfiltern? Dieser Begriff beschreibt ein technisches System, mithilfe dessen hochgeladene Inhalte auf Urheberrechtsverstöße untersucht und gegebenenfalls gesperrt werden. Zwar schreibt die DSM-RL solche Maßnahmen nicht ausdrücklich vor und darauf haben sich auch die Verfechter der Reform stets berufen. Vor dem Hintergrund der Menge hochgeladener Inhalten, ist lediglich eine technische Überprüfung denkbar.

Geht man also davon aus, dass kein Weg an Uploadfiltern vorbeiführt, entstehen Folgeprobleme. Eins davon ist Art. 17 Abs. 8 UAbs. 1 DSM-RL. Diese Vorschrift verbietet allgemeine Überwachungsmaßnahmen durch Online-Plattformen. Es drängt sich die Schlussfolgerung auf, dies stehe gerade der Einführung eines technischen Systems entgegen, mit dem eine Überwachung der gesamten auf die Plattform hochgeladenen Inhalte einherginge. Ob die Vorschriften der DSM-RL vor diesem Hintergrund in Einklang zu bringen sind, wird durch den nationalen Gesetzgeber oder letztlich die Rechtsprechung zu entscheiden sein.
Ein weiteres Problem ist, dass Uploadfilter ein weniger geeignetes Mittel sind, die Rechtslage zu prüfen. Zwar hat YouTube bereits ein Filtersystem entwickelt, das akkurat arbeiten soll («Content ID»). Art. 17 DSM-RL ist aber nicht nur auf den Musik- und Videobereich, sondern auf alle Werkarten anwendbar. Für andere Werkarten gibt es aber bislang keine zuverlässigen Filtersysteme. Wenn aber eine Pflicht zur Einführung von Uploadfiltern nicht umsetzbar ist, kann sie auch keine rechtliche Wirkung entfalten.

Ein drittes Problem von Uploadfiltern wird oftmals mit Overblocking überschrieben. Dies beschreibt den Effekt, das Online-Plattformen rechtmäßig hochgeladene Inhalte aus Furcht vor der Haftung dennoch sperren. Dies betrifft insbesondere Inhalte, die sich im rechtlichen Graubereich bewegen. Es wurden zwar einige Gegenmaßnahmen eingebaut, um den Effekt des Overblocking vorzubeugen. Unter anderem sollen Schranken des Urheberrechts für Zitat, Kritik, Karikatur und Parodie vorgesehen werden. Weiterhin sollen im Falle von unrechtmäßigen Blockierungen, Beschwerden von Nutzern unverzüglich von einem Menschen bearbeitet werden. Aber auch wenn diese Gegenmaßnahmen Wirkungen zeigen sollten – was bereits sehr fraglich ist – bleibt dennoch eine Erkenntnis: Kommunikation auf Online-Plattformen besteht künftig unter Vorbehalt. Nach bisheriger Rechtslage durften Nutzer zunächst Inhalte hochladen, bevor die Online-Plattform eventuell zum Mittel der Sperrung greifen musste. Fortan muss die Plattform prüfen, bevor die Inhalte auf der Plattform überhaupt erst verfügbar sind. Online-Plattformen müssen in Zukunft also nicht mehr repressiv, sondern präventiv handeln. Dies kann, insbesondere aus Sicht der Rechteinhaber, begrüßt werden. Es kann aber auch als Gefahr gesehen werden. Der Wert und Nutzen vieler Inhalte sind gerade bei der schnelllebigen digitalen Kommunikation von ihrer Aktualität abhängig. Durch den Einsatz von Uploadfiltern könnte der Zugang zu Informationen in Zukunft hingegen erschwert werden. Im Übrigen hängt es wesentlich von der Effektivität des Beschwerdeverfahrens ab, ob dem Overblocking getrotzt werden kann. Kann eine Beschwerde online mit wenigen Klicks eingereicht werden, mag dies noch tolerabel sein. Ist der Nutzer aber vom Beschwerdeverfahren überfordert, entsteht die Gefahr, dass seine Passivität dazu führt, dass der Inhalt überhaupt nicht mehr hochgeladen wird.

3 Ein Themenbereich der DSM-RL, der ebenfalls in diesem Infobrief besprochen wird.

3. Notice and stay down

Die letzte Voraussetzung wiederholt einerseits das gängige Verfahren des notice and take down. Andererseits wird weitergehend gefordert, dass auch das künftige Hochladen einmal gesperrter Inhalte verhindert werden muss (notice and stay down).

V. Schutz von Jungunternehmen

Die drei Voraussetzungen der neuen Haftungsprivilegierung gelten nicht für alle Online-Plattformen gleichermaßen. Vielmehr differenziert Art. 17 DSM-RL zwischen drei Gruppen von Plattformen.

In der ersten Gruppe befinden sich die Online-Plattformen, die alle drei Voraussetzungen erfüllen müssen. In der zweiten Gruppe finden sich Plattformen, die weniger als drei Jahre in der Union verfügbar sind und einen Jahresumsatz von weniger als zehn Millionen Euro aufweisen. Solche Plattformen sind von der Pflicht befreit, Uploadfilter einzuführen und unterliegen damit lediglich dem bekannten Verfahren des notice and take down. Die Plattformen der dritten Gruppe sind ebenfalls jünger als drei Jahre und setzen weniger als zehn Millionen Euro im Jahr um, weisen aber eine monatliche Besucherzahl von über fünf Millionen Euro auf. Sie sind nur augenscheinlich von der Pflicht zur Einführung von Uploadfiltern (Art. 17 Abs. 4 lit. b DSM-RL) befreit. Allerdings müssen sie neben dem notice and take down auch ein notice and stay down gewährleisten. Eine Plattform kann aber ohne einen Uploadfilter nicht gewährleisten, dass einmal gesperrte Inhalte nicht nochmal hochgeladen werden.

Letzteres ist durchaus kritisch zu sehen. Denn solche Plattformen sind aufgrund ihrer (noch) geringen Umsatzzahl aber ihrer hohen Besucherzahl besonders erfolgsversprechend. Die Verpflichtung zu einem Uploadfilter wirkt daher innovationsschädlich. Weil kleinere Plattformen mangels Ressourcen keine eigenen Uploadfilter entwickeln können, müsste sie auf die von großen Plattformen zurückgreifen. Dass diese damit noch mächtiger werden, läuft der Zielsetzung der DSM-RL allerdings entgegen. Wie bereits oben vorgeschlagen, sollte der nationale Gesetzgeber daher über die Definition der erfassten Online-Plattformen genauer differenzieren und insbesondere junge Online-Plattformen schützen.

VI. Bedeutung für Hochschulen und Forschungseinrichtungen

Wie jeder Internetnutzer sind Hochschulen und Forschungseinrichtungen von Art. 17 DSM-RL nur mittelbar betroffen. Durch die die Ausnahmebestimmungen in Art. 2 DSM-RL sind Online-Plattformen, die durch Hochschulen und Forschungseinrichtungen betrieben werden, von dem Haftungssystem nicht betroffen. Dies gilt jedenfalls für Plattformen, die nicht zur Gewinnerzielung betrieben werden. Gleichwohl hat Art. 17 DSM-RL das Potenzial, das Kommunikationsverhalten im Internet grundlegend zu verändern – dessen sollte sich jeder bewusst sein. Nun sind die Mitgliedstaaten gefragt, die Richtlinie in nationales Recht zu gießen. Dafür haben sie nicht nur zwei Jahre Zeit, sondern auch die Möglichkeit, den bestehenden Umsetzungsspielraum bestmöglich zu nutzen.

Vergriffen heißt nicht vergessen

Neuregelung der vergriffenen Werke nach der EU-Urheberrechtsrichtlinie

von Marten Tiessen

Die Richtlinie (EU) 2019/790 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt (DSM-RL) enthält eine wichtige Neuregulierung zu vergriffenen Werken. Sie beseitigt die bestehende Rechtsunsicherheit nach der jüngsten EuGH-Rechtsprechung und ebnet den Weg für europäische Digitalisierungsprojekte. Letztere werden gerade auch von den Hochschulbibiliotheken vorangetrieben. Damit kommt ihnen eine herausragende Rolle bei der Bewahrung kultureller Schätze zu. Auch auf die Umsetzung der Richtlinie können die Hochschulen Einfluss nehmen.

I. Vergriffene Werke

Nach dem Urheberrechtsgesetz stehen allein dem Schöpfer eines Werkes die Verwertungsrechte an seinem Werk zu. Dazu gehören das Recht, das Werk zu vervielfältigen, zu verbreiten und öffentlich wiederzugeben. Als Urheber steht es ihm frei, anderen Nutzungsrechte an seinem Werk einzuräumen. Er kann dabei auch bestimmen, in welchem Umfang er diese übertragen möchte. Häufig wird er einen Teil dieser Rechte einem Verwerter einräumen, der daraufhin das Werk auf den Markt bringt. Im Fall eines Buches würde also beispielsweise der Autor dem Verlag das Recht einräumen, das Buch in einer bestimmten Stückzahl zu drucken und zu vertreiben. Für die Übertragung dieser Rechte beteiligt der Verlag den Autor an den Erlösen. Der Verlag setzt darauf, dass sich seine Investitionen in den Vertrieb des Werkes durch den Verkauf amortisieren. Stellt er fest, dass die Kosten nicht mehr im angemessenen Verhältnis zu den Einnahmen stehen, stellt er in der Regel den Druck des Buches ein. Wenn das Buch dann nach einer gewissen Zeit nicht mehr auf dem normalen Vertriebsweg erhältlich ist, spricht man von einem vergriffenen Werk.

Ist ein Werk erstmal vergriffen, führt das zu zwei faktischen und einem rechtlichen Problem: Das erste faktische Problem sind die beschränkten Zugangsmöglichkeiten der Allgemeinheit zum Werk. Nur weil es nicht mehr im Handel erhältlich ist, bedeutet dies im Umkehrschluss nicht, dass die Allgemeinheit kein Interesse mehr an dem Werk hat. Es kann zum Beispiel sein, dass das Werk von vornherein nur unter Druckkostenbeteiligung des Urhebers in einer begrenzten Auflage gedruckt wurde. Das wird vor allem bei vielen wissenschaftlichen Werken der Fall sein. Sie werden nicht zwangsläufig mit der Absicht veröffentlicht, kommerziell rentabel zu sein, da sie sich sowieso ausschließlich an ein stark begrenztes Fachpublikum richten. Ist ein solches Werk erstmal vergriffen, kann ein Zugangsinteressierter nur noch versuchen, das Werk antiquarisch zu erwerben oder er muss hoffen, dass das Werk in einer Bibliothek ausleihbar ist.

Das zweite und gravierendere faktische Problem ist, dass die Werke in Vergessenheit zu geraten drohen. Denn ein Zugangsinteresse kann nur bestehen, wenn die Existenz des Werkes überhaupt bekannt ist. Es liegt in der Natur der Sache, dass vergriffene Werke kaum noch in den Umlauf geraten und auch nicht in digitalen Suchdatenbanken erscheinen. Dadurch bleibt das in ihnen erhaltene Wissen ungenutzt.

Diese zwei faktischen Probleme ließen sich eigentlich beheben. Bibliotheken und Archive, in denen sich vergriffene Werke befinden, könnten diese durch ihre Digitalisierung und Online-Veröffentlichung wieder einem breiteren Publikum zugänglich machen. Dabei könnten sie mit anderen Einrichtungen in Digitalisierungsprojekten zusammenarbeiten und die gesammelten Daten auf einer gemeinsamen Plattform verfügbar machen. Durch Suchmasken würde der Interessierte dann bei Eingabe der entsprechenden Schlagwörter auf das Werk

stoßen. Will er das Werk in Gänze rezipieren, könnte er dies entweder auf der Website der Einrichtung tun oder indem er sich eine analoge Kopie ausleiht. Solche Digitalisierungsbestrebungen gibt es bisher auch schon für gemeinfreie Werke, die zurzeit beispielsweise länderübergreifend durch das Digitalisierungsprojekt Europeana bereitgestellt werden. Das Projekt wurde von der Europäischen Union mit dem Ziel ins Leben gerufen, das wissenschaftliche und kulturelle Erbe Europas digital zugänglich zu machen. Die Plattform dient dabei als Aggregator für Inhalte, die von teilnehmenden Institutionen beigesteuert werden. In der Datenbank von Europeana werden nur Metadaten und Thumbnails der Werke und nicht die Digitalisate selbst gesammelt. Diese verbleiben auf der Seite der teilnehmenden Einrichtung und werden nur auf Europeana verlinkt. Zu den teilnehmenden Institutionen gehören unter anderem auch zahlreiche Forschungs- und Universitätsbibliotheken.

Die rechtliche Situation verhinderte bisher, dass solche Digitalisierungsprojekte auch vergriffene Werke miteinbeziehen. Das liegt daran, dass für Vervielfältigungshandlungen und für die öffentliche Wiedergabe des Werkes die Erlaubnis des Rechteinhabers nötig ist. Die Werke werden zwar kommerziell nicht mehr genutzt und weisen bereits ein beträchtliches Alter auf, sind aber auch noch nicht gemeinfrei. Gemeinfrei sind Werke, an denen das Urheberrecht inzwischen erloschen ist, weil die urheberrechtliche Schutzfrist abgelaufen ist. Diese beträgt 70 Jahre ab dem Tod des Urhebers. Bei vergriffenen Werken stehen dem Urheber oder einem Rechtsnachfolger die Verwertungsrechte an dem Werk hingegen weiterhin zu. Will eine Bibliothek also ein vergriffenes Werk vervielfältigen und öffentlich zugänglich machen, müsste sie versuchen, vorher die Erlaubnis des Rechteinhabers einzuholen. Die Rechteeinholung für vergriffene Werke kann aber einen enormen Aufwand beinhalten. Das allein schon deshalb, weil häufig nicht eindeutig zu bestimmen ist, wer überhaupt Rechteinhaber ist. Die Recherche nach dem Rechteinhaber und die Aushandlung eines individuellen Lizenzvertrages kosten Zeit und Geld. Sollen gleich ganze Bestände an vergriffenen Werken digitalisiert werden, multipliziert sich der Aufwand um ein Vielfaches. Durch diese unverhältnismäßigen Anstrengungen sind Digitalisierungsprojekte auf diese Weise schlicht nicht realisierbar. Alternativ könnte sich die Einrichtung an die zuständige Verwertungsgesellschaft wenden und mit ihr einen kollektiven Lizenzvertrag abschließen. Denn Verwertungsgesellschaften können mit Dritten Lizenzverträge über diejenigen Werke, zu deren Rechtewahrnehmung sie beauftragt sind, gebündelt abschließen.

Ein Problem ergibt sich jedoch daraus, dass nicht alle Rechteinhaber von einer Verwertungsgesellschaft vertreten werden. Die Werke dieser sogenannten Außenseiter wären also auch nicht von einer Kollektivlizenz erfasst. Das heißt, die Einrichtung müsste überprüfen, ob der betroffene Rechteinhaber einen Wahrnehmungsvertrag mit der Verwertungsgesellschaft geschlossen hat und bei negativem Ergebnis wiederum einen individuellen Lizenzvertrag mit dem Außenseiter aushandeln. Auch hier würde der Aufwand wieder in keinem Verhältnis zum Nutzen stehen. Da das Problem vertraglich nicht gelöst werden kann, bedarf es also einer gesetzlichen Lösung. Diese bestand bisher in Deutschland in Form des § 51 Verwertungsgesellschaftsgesetz (VGG).

II. § 51 VGG

§ 51 VGG löste dieses Problem durch eine gesetzliche Fiktion. Nach dieser wird fingiert, dass Verwertungsgesellschaften, die Rechte der Vervielfältigung und öffentlichen Zugänglichmachung an vergriffenen Werken wahrnehmen, berechtigt sind, auch Rechte an Werken von Außenseitern einzuräumen. Dadurch eröffnet der Gesetzgeber den Weg zu einer kollektiven Lizenz, die auch die Außenseiter mitumfasst. Dies gilt zumindest solange, bis die Außenseiter der Rechtewahrnehmung widersprechen. Lizenznehmer können jedoch nur Bibliotheken, Bildungseinrichtungen, Museen, Archive, und im Bereich des Film- oder Tonerbes tätige Einrichtungen sein. Voraussetzung der gesetzlichen Fiktion ist unter anderem, dass die Werke vor dem Jahr 1966 veröffentlicht wurden und die Nutzung nicht kommerziell erfolgt. Auch betrifft die Regelung nur Printwerke. In den vorherigen Beispielen war bisher immer nur von vergriffenen Büchern die Rede, allerdings können durchaus auch Filme oder Musik vergriffen sein. Letztere fallen bisher nicht unter § 51 VGG.

III. Soulier-Urteil

Der bisherige nationale Lösungsweg wurde in Frage gestellt, als der EuGH über die Vereinbarkeit einer vergleichbaren französischen Regelung mit dem Europarecht entschied

(Urt. v. 16.11.2016 – C-301/15).[1] Der Gerichtshof in Luxemburg entschied, dass eine Lizenzvergabe ohne angemessene vorherige Benachrichtigung der betroffenen Rechteinhaber nicht zulässig sei. Daran fehle es nach der französischen Regelung. Eine solche Praxis greife in die im Unionsrecht zugesicherten Rechte des Urhebers ein. Zwar sei es nicht nötig, dass jeder Rechteinhaber seine ausdrückliche Zustimmung gebe, er müsse aber zumindest darüber informiert werden, dass eine Nutzung erfolgen soll und wie er dieser Nutzung widersprechen kann. Ein öffentlich einsehbares Register erfülle die Informationspflichten noch nicht.

Die vom EuGH geäußerten Bedenken ließen sich auch auf § 51 VGG übertragen, da auch die deutsche Regelung nicht vorsieht, dass die Rechteinhaber einzeln informiert werden. Deshalb war nach dem Soulier-Urteil unklar, inwieweit § 51 VGG noch weiter Anwendung findet.

IV. Art. 8-11 DSM-RL

In der europäischen Urheberrechtsreform nutzte der Gesetzgeber die Gelegenheiten, eine unionsweite Lösung für die durch die Soulier-Rechtsprechung hervorgerufene Rechtsunsicherheit zu finden. Mit den Art. 8-11 DSM-RL hat er eine Rechtsgrundlage für zukünftige nationale Regelungen zur Nutzung von vergriffenen Werken geschaffen.

Art. 8 Abs. 1 DSM-RL ermöglicht nun auf europäischer Ebene weitestgehend das, was bisher nach § 51 VGG erlaubt war. Die Mitgliedstaaten sollen Regelungen erlassen, nach denen Verwertungsgesellschaften Kultureinrichtungen Nutzungslizenzen für vergriffene Werke einräumen dürfen. Dabei soll die Lizenz der für den Bereich zuständigen Verwertungsgesellschaft auch die Werke von Außenseitern erfassen. Diese gesetzliche Erlaubnis zur Lizenzvergabe ist aber an eine Reihe von Voraussetzungen geknüpft: So darf die Nutzung ausschließlich für nicht-kommerzielle Zwecke erfolgen. Außerdem müssen sich die Werke in den Beständen der Einrichtung befinden. Eine solche Bestandsakzessorietät sorgt dafür, dass die Einrichtungen nur einen erweiterten Zugang zu dem schaffen, was sich ohnehin bereits in ihrem Bestand befindet. Eine Erweiterung ihres Bestandes darüber hinaus ist nicht zulässig.

Weiterhin müssen die Verwertungsgesellschaften repräsentativ für die Rechteinhaber der einschlägigen Art von Werken sein. Das bedeutet, dass es nicht genügt, dass eine Verwertungsgesellschaft von einigen Rechteinhabern mit der Wahrnehmung ihrer Rechte für das entsprechende Werk beauftragt wurde. Es muss laut Erwägungsgrund 33 der DSR-RL zumindest eine „beträchtliche Zahl von Rechteinhabern“ der Verwertungsgesellschaft ihr Mandat für die spezifische Nutzung erteilt haben. Diese noch reichlich unscharfe Formulierung bedarf einer näheren Konkretisierung durch den nationalen Gesetzgeber. Für den Fall, dass es an der Repräsentativität der Verwertungsgesellschaft mangelt, hat der Gesetzgeber in Art. 8 Abs. 2 DSM-RL eine Alternative zur kollektiven Lizenz geschaffen. Danach sind die Mitgliedstaaten berechtigt, für solche Fälle gesetzliche Schranken zu erlassen, die die Kultureinrichtungen berechtigen, im begrenzten Rahmen dennoch vergriffene Werke zu nutzen. In diesen Fällen sind sie allerdings nicht zu analogen Vervielfältigungen berechtigt, sondern dürfen die Werke „nur“ auf nicht-kommerziellen Internetseiten zugänglich machen.

Im Hinblick auf die Werkart geht der europäische Gesetzgeber über die bisherige deutsche Regelung hinaus. Zukünftig sollen nicht nur vergriffene Printwerke, sondern vergriffene Werke aller Art lizenzierbar sein bzw. unter die Schranke des Abs. 2 fallen. In Art. 8 Abs. 5 DSM-RL versucht der europäische Gesetzgeber eine grobe Definition aufzustellen, die erklärt, ab wann ein Werk vergriffen ist. Das soll der Fall sein, wenn nach Treu und Glauben davon ausgegangen werden kann, dass das gesamte Werk auf den üblichen Vertriebswegen für die Öffentlichkeit nicht erhältlich ist, nachdem ein vertretbarer Aufwand betrieben wurde, um festzustellen, ob es für die Öffentlichkeit erhältlich ist. Wann dieser vertretbare Aufwand als betrieben gilt, ist allerdings noch nicht näher definiert. Hier wird es in die Verantwortung des nationalen Gesetzgebers fallen, nähere Konkretisierungen zu treffen.

Erlaubt ist neuerdings auch die Erteilung der Lizenz für eine unionsweite Nutzung des Werkes. Diese Neuerung kommt gerade den länderübergreifenden Digitalisierungsprojekten zugute, die im Netz unionsweit ihre Datenbanken zu Verfügung stellen.[2]

1 Siehe hierzu ausführlicher Mörike, Wer schweigt, stimmt nicht zu, DFN-Infobrief 02/2017.

2 Auf solchen Plattformen kann der Zugang zu den einzelnen Werken allerdings nur über eine Verlinkung zur Seite der jeweiligen Einrichtung, in der sich das Werk befindet, geschaffen werden. Der Grund dafür ist auch hier die Bestandsakzessorietät.

V. Fazit und Praxishinweise

Als Google Books 2004 anfing in großem Umfang Bücher zu digitalisieren, griffen sie zuerst auf die Bestände der Hochschulbibliotheken zurück. Ein Großteil der digitalisierten Werke waren auch hier vergriffene Werke. Zwar wurde nach einem endlosen Rechtsstreit entschieden, dass Google Books diese Werke nur ausschnittsweise zur Verfügung stellen darf, aber dennoch rückten diese Werke - insbesondere durch die Suchfunktionen - wieder stärker in das Sichtfeld der Öffentlichkeit. Damit wollte Google allerdings weder der Welt noch den Rechteinhabern etwas Gutes tun, sondern in erster Linie selbst profitieren. Trotzdem wurde durch Googles Vorstoß zum ersten Mal einer breiteren Öffentlichkeit bekannt, welche Möglichkeiten die Digitalisierung für die Reaktivierung dieses ungenutzten Wissens bietet. Wenn in Deutschland Digitalisierungsprojekte realisiert werden sollen, die nicht Partikularinteressen, sondern der Allgemeinheit dienen, müssen daran ebenfalls die Hochschulen mitwirken. Die DSM-RL bietet hierzu die Möglichkeit, indem ausschließlich öffentliche Kultureinrichtungen zur Lizenznahme privilegiert werden. Mitwirken können die Hochschulen dabei sowohl durch Rechtsgestaltung als auch durch Rechtsanwendung.

Als europäische Richtlinie muss die DSM-RL erst noch in nationales Recht umgesetzt werden. Dabei haben die Mitgliedstaaten einen nicht unerheblichen Entscheidungsspielraum, z. B. bei der Definition, ab wann ein Werk als vergriffen angesehen werden kann. Art. 11 DSM-RL hält die Mitgliedstaaten dazu an, die einzelnen Interessenvertreter zu konsultieren, bevor sie festlegen, nach welchen Voraussetzungen ein Werk als vergriffen gilt. Zu diesen Interessenvertretern gehören neben den Rechteinhabern und Verwertungsgesellschaften auch die Einrichtungen des Kulturerbes, zu denen wiederum die Hochschulbibliotheken gehören. Viele Stellungnahmen wurden bereits von einzelnen Interessengruppen verfasst, aber solange der nationale Gesetzgebungsprozess andauert, kann auch noch weiter darauf eingewirkt werden. Eine Überarbeitung des § 51 VGG ist erforderlich, da die Richtlinie in manchen Bereichen enger und anderen weiter als die bisherige Regelung ist.

Zukünftig werden die Hochschulen dann die neuen nationalen Bestimmungen auch anwenden und in eigenen oder überregionalen Digitalisierungsprojekten ihre Bestände an vergriffenen Werken zugänglich machen. Damit dienen sie letztlich ihrem eigentlichen Hauptzweck, der Wissensmehrung.

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