

infobrief recht

7/2021

Juli 2021



Habemus Reform

Größte Reform des Urheberrechts seit zwei Jahrzehnten teilweise in Kraft getreten

Im Hinterzimmer zur Netzsperr

Die neue Clearingstelle Urheberrecht im Internet (CUII)

Ausgelöscht.

Das unberechtigte Löschen von Daten rechtfertigt eine fristlose Kündigung gegenüber dem Arbeitnehmer

Habemus Reform

Größte Reform des Urheberrechts seit zwei Jahrzehnten teilweise in Kraft getreten

von *Justin Rennert*

Die seit Beginn des Gesetzgebungsverfahrens kontrovers und medienwirksam diskutierte EU-Urheberrechtsreform hat nun ihren vorläufigen Abschluss gefunden. Ende Mai passierte das „Gesetz zur Anpassung des Urheberrechts an die Erfordernisse des Digitalen Binnenmarktes“ den Deutschen Bundestag.¹ Am 7. Juni 2021 traten weite Teile des Gesetzes in Kraft, die übrigen Regelungen folgen am 1. August 2021. Wir geben einen Überblick über die Neuregelungen und Änderungen, die Hochschulen besonders betreffen.

I. Hintergrund und Gesetzgebungsverfahren

Die Europäische Kommission hatte bereits im September 2016 im Rahmen ihrer Strategie für einen digitalen Binnenmarkt einen Vorschlag für eine „Richtlinie über das Urheberrecht im digitalen Binnenmarkt“ (kurz: DSM-RL) gemacht. Der Vorschlag war sodann Gegenstand intensiver Diskussionen im Europäischen Parlament und im Rat der Europäischen Union. Der aus Mitgliedern des Rates und des Parlamentes bestehende Vermittlungsausschuss musste einberufen werden und verhandelte ab Oktober 2018 bis zum Februar 2019. Erst am 26. März 2019, mehr als zwei Jahre nach der erstmaligen Befassung des Europäischen Parlamentes mit dem Gesetzesvorschlag, nahm das Parlament den Vorschlag schließlich an. Zwischenzeitlich gingen in Deutschland zehntausende Menschen auf die Straßen, um gegen das geplante Gesetz zu demonstrieren. Bei der bundesweit größten Demonstration im März 2019 in München meldete die Polizei eine Teilnehmerzahl von 40.000 Menschen.² Der Protest richtete sich vor allem gegen den geplanten Artikel 13 des Kommissionsvorschlags (in der schließlich verabschiedeten Richtlinie Artikel 17), der eine urheberrechtliche Verantwortlichkeit für Upload-Plattformen wie YouTube vorsah, wenn auf ihren Plattformen urheberrechtlich geschützte Inhalte hochgeladen werden. Kritiker

und Demonstrierende befürchteten als Konsequenz der Regelung ein sog. Overblocking von Inhalten durch die Upload-Plattformen, mithin eine versehentliche Blockierung auch von Inhalten, die gar nicht urheberrechtlich geschützt sind. Dies würde die Ausübung des Rechtes auf freie Meinungsäußerung im Internet gefährden.

Mit dem Beschluss des Rates der Europäischen Union wurde die Richtlinie gleichwohl im April 2019 verabschiedet. Die Mitgliedstaaten hatten daraufhin bis zum 7. Juni 2021 Zeit, um die nicht unmittelbar in den Mitgliedstaaten geltende Richtlinie in bindendes nationales Recht umzusetzen. Die Bundesrepublik Deutschland setzte die Richtlinie nun in Gestalt des „Gesetzes zur Anpassung des Urheberrechtes an die Erfordernisse des Digitalen Binnenmarktes“ (nachfolgend: Umsetzungsgesetz) um. Das Gesetzespaket bringt Änderungen am Urheberrechtsgesetz (UrhG) und am Verwertungsgesellschaftengesetz (VGG) mit sich. Zudem wird mit dem Urheberrechts-Diensteanbieter-Gesetz (UrhDaG) ein gänzlich neues, eigenständiges Gesetz geschaffen, das die urheberrechtliche Verantwortlichkeit von Upload-Plattformen regelt und Artikel 17 der DSM-Richtlinie umsetzt. Nachfolgend stellen wir die Änderungen mit besonderem Hochschulbezug überblicksweise dar.

¹ <https://www.bundestag.de/dokumente/textarchiv/2021/kw20-de-urheberrecht-binnenmarkt-842596>

² <https://www.sueddeutsche.de/muenchen/demo-muenchen-urheberrecht-1.4380419>

II. Überblick über die einzelnen Regelungen der Reform

Die Einzelregelungen des Umsetzungsgesetzes unterscheiden sich zunächst nach dem Datum ihres Inkrafttretens. Während viele Einzelregelungen bereits am 7. Juni 2021 in Kraft getreten sind, gilt das neue UrhDaG erst ab dem 1. August 2021. Zunächst wird hier auf die ab dem 7. Juni geltenden Vorschriften eingegangen, ein Überblick über das UrhDaG folgt zuletzt.

1. Text- und Data-Mining

Das Umsetzungsgesetz ergänzt die bisherigen Regelungen zum Text- und Data-Mining.³ Seit März 2018 bestand in Gestalt des § 60d UrhG aF bereits eine gesetzliche Erlaubnis für das Text- und Data-Mining zu Zwecken der wissenschaftlichen Forschung. Beim Text- und Data-Mining werden große Mengen von Informationen, die in digitaler Form vorliegen (also z. B. Texte, Töne, Statistiken oder Bilder) mithilfe von Computern automatisiert ausgewertet. Dies geschieht in der Regel unter Verwendung von Algorithmus-basierten Analyseverfahren und erlaubt die Aufdeckung von Strukturen, Trends und Korrelationen innerhalb großer Datensätze. So setzen beispielsweise Versicherungen das Data-Mining ein, um die Häufigkeit und die Wahrscheinlichkeit spezifischer Schadensfälle auszuwerten und so die Versicherungsprämie intelligent anpassen zu können.⁴

Der neue § 44b UrhG führt eine Erlaubnisnorm für das Text- und Data-Mining ein, bei der die Verfolgung von Forschungszwecken nicht mehr erforderlich ist. Gemäß § 44b UrhG ist es nunmehr für jedermann zulässig, Vervielfältigungen von rechtmäßig zugänglichen digitalen oder digitalisierten Werken für das Text- und Data-Mining zu erstellen. Die Daten dürfen beispielsweise auf einer Festplatte gespeichert und kopiert werden, um sie für die Bearbeitung durch den Algorithmus vorzubereiten. Es ist dabei stets Voraussetzung, dass die Werke bereits rechtmäßig zugänglich sind, d.h. beispielsweise frei im Internet verfügbar. Dem Inhaber des Urheberrechts an den in den Daten enthaltenen Werken bleibt allerdings die Möglichkeit, die Vervielfältigung zu untersagen, indem er

einen Nutzungsvorbehalt erklärt. Dies kann beispielsweise in AGB oder im Impressum der eigenen Webseite erfolgen.

Nach wie vor gibt es in Gestalt des § 60d UrhG jedoch eine Spezialregelung für Forschungsorganisationen. Für die wissenschaftliche Forschung erlaubt sie Vervielfältigungen der in den Daten enthaltenen Werke. Zusätzlich erlaubt sie jedoch, die Vervielfältigungen im Anschluss an die Aufbereitung für die Analyse einem abgegrenzten Personenkreis oder einzelnen Dritten auch öffentlich zugänglich zu machen. Privilegiert ist mithin die Bereitstellung der Daten innerhalb eines Teams von Forschenden (also z. B. im Intranet eines universitären Instituts) oder die Begutachtung von Forschungsergebnissen im Rahmen sog. Peer-Review-Verfahren.

Das Umsetzungsgesetz nimmt einige Änderungen an dieser Vorschrift vor. Die wohl wichtigste Änderung ist der Entfall der Vergütungspflicht. Vor dem 7. Juni hatte der Rechteinhaber gegen denjenigen, der Vervielfältigungen oder öffentliche Zugänglichmachungen im Rahmen des Text- oder Data-Ming vornahm, nach Gesetz einen Anspruch auf Zahlung einer angemessenen Vergütung. Nach neuer Rechtslage besteht ein solcher Anspruch nicht mehr. Der nationale Gesetzgeber hat sich sonach an die (unverbindliche) Vorgabe in Erwägungsgrund 17 Satz 2 der DSM-RL gehalten. Weiterhin entfällt die Pflicht, nach erfolgter Vervielfältigung für die einzelnen Werke innerhalb des Datenbestandes eine Quelle angeben zu müssen. Nach alter Rechtslage musste beispielsweise nach der Digitalisierung eines Datensatzes innerhalb der elektronischen Datei der Urheber genannt werden. Schließlich wurde die sehr strenge Beschränkung der Vorschrift auf nicht kommerzielle Nutzungszwecke aufgelockert. Bislang durften Forscher, die von der Erlaubnisnorm Gebrauch machen wollten, ausschließlich nicht kommerzielle Zwecke verfolgen, d. h. keine Gewinne erzielen. Nunmehr ist es ausreichend, wenn zwar Gewinne erzielt werden, diese allerdings sämtlich in die wissenschaftliche Forschung reinvestiert werden. Alternativ reicht es aus, wenn eine Forschungseinrichtung im Rahmen eines staatlich anerkannten Auftrages im öffentlichen Interesse tätig ist. Ist eine Einrichtung gänzlich kommerziell tätig, kann sie sich – wie schon beschrieben – allerdings auf den neuen § 44b UrhG berufen. Ausdrücklich sei an dieser Stelle erwähnt, dass die Spezialregelung für Forschungsorganisationen des § 60d UrhG den neuen § 44b UrhG in ihrem Anwendungsbereich nicht verdrängt. Für reine Vervielfältigungen (nicht jedoch für öffentliche Zugänglichmachungen) kann sich auch ein Forscher

³ Vertiefend Gielen: „Die neue urheberrechtliche Schranke zum Text- und Data-Mining“, DFN-Infobrief Recht 12/2019

⁴ Bitter in Hoeren/Sieber/Holzner MMR-HdB, Teil 15.4 Big Data im Finanz- und Versicherungswesen Rn. 2

auf den § 44b UrhG berufen.⁵ Insofern werden die Risiken für Forschende abgemildert, wenn nicht eindeutig geklärt ist, ob diese im rechtlichen Sinne kommerziell oder nicht kommerziell tätig sind.

2. Digitale Lehre

Eine geringfügige Änderung bewirkt das Umsetzungsgesetz im Rechtsregime zur digitalen Lehre. Nach § 60a UrhG aF war es schon bisher erlaubt, zur Veranschaulichung des Unterrichts und der Lehre an Bildungseinrichtungen zu nicht kommerziellen Zwecken bis zu 15 Prozent eines veröffentlichten Werkes zu vervielfältigen, zu verbreiten, öffentlich zugänglich zu machen oder in sonstiger Weise öffentlich wiederzugeben. Aus Sicht des europäischen Gesetzgebers bestand allerdings ein Mangel an Rechtssicherheit bei grenzüberschreitenden Nutzungen. Wenn also zum Beispiel eine italienische Studentin an einer deutschen Fernuniversität eingeschrieben war und von Italien online die Vorlesungen und Seminare verfolgte, bestand für die Universität die Gefahr, wegen einer Urheberrechtsverletzung nach italienischem Recht in Anspruch genommen zu werden.

Nunmehr schreibt der neue § 60a UrhG in einem neu eingefügten Absatz 3a vor, dass bei Nutzung eines Werkes zur Veranschaulichung des Unterrichts oder der Lehre an Bildungseinrichtungen nur das Recht des Staates am Sitz der Bildungseinrichtung anwendbar ist. Die deutsche Fernuniversität im oben genannten Beispiel kann sich nun also sicher sein, dass sich die urheberrechtliche Zulässigkeit der Werknutzung im Rahmen von Online-Vorlesungen ausschließlich nach deutschem Recht richtet.

3. Nicht verfügbare und vergriffene Werke

Erhebliche Änderungen bewirkt das Umsetzungsgesetz innerhalb der Vorschriften zu vergriffenen Werken. Vergriffene Werke sind solche, die nicht mehr im Handel erhältlich sind, für die aber gleichwohl noch urheberrechtlicher Schutz besteht. Oft befinden sich diese Werke im Bestand von Hochschulen, Bibliotheken, Museen oder Archiven. Im Zuge der fortschreitenden Digitalisierung dieser Einrichtungen gab und gibt es

das erhebliche Bedürfnis, auch vergriffene Werke digital (insb. online) verfügbar zu machen, um das darin enthaltene Wissen nicht in Vergessenheit geraten zu lassen. Problematisch ist dabei, dass die Digitalisierung von Werken in die Rechte des Urhebers eingreift und deswegen eigentlich die Einholung einer Nutzungserlaubnis erforderlich wäre.⁶ Bei vergriffenen Werken gestaltet sich das ausfindig Machen des Rechteinhabers zur Einholung der Nutzungserlaubnis allerdings häufig schwierig. Beispielsweise kann es sein, dass der Verlag, der das Werk veröffentlicht hat, gar nicht mehr existiert oder die Anschrift des Urhebers inzwischen unauffindbar ist.

Seit 2014 existierten daher in Deutschland mit den §§ 51 ff. VGG aF Regelungen, die mittels einer gesetzlichen Vermutungsregelung de facto ermöglichten, dass Verwertungsgesellschaften Nutzungsrechte an Printwerken einräumen, obwohl ihnen die Befugnis hierzu vom Rechtsinhaber nicht übertragen wurde. Bibliotheken oder Archive mussten sich seither statt mit einer Vielzahl potentiell unauffindbarer Rechtsinhaber nur mit einigen wenigen Verwertungsgesellschaften auseinandersetzen.

Dieses Rechtsregime weitet das Umsetzungsgesetz nunmehr erheblich aus. Zunächst fällt die Beschränkung auf Printwerke weg. Gemäß dem neu eingefügten § 52b VGG ist nun jede Werkart (insb. Film- und Musikwerke) erfasst, ohne Rücksicht darauf, ob das Werk in einer Print-Publikation veröffentlicht wurde. So könnten z.B. in Zukunft auch für Werke, die auf Videokassetten im veralteten Format gespeichert sind, Nutzungsrechte vereinfacht erteilt werden. Gleiches gilt für Fotografien, die im Analog-Format vorliegen oder für auf CDs oder Schallplatten gespeicherte Musik- oder Tonaufnahmen.

Weiterhin ersetzt das Umsetzungsgesetz den Begriff der „vergriffenen Werke“ durch den Begriff der „nicht verfügbaren Werke“. Nicht verfügbar ist ein Werk nach dem neuen § 52b Abs. 1 VGG, wenn es der Allgemeinheit auf keinem üblichen Vertriebsweg in einer vollständigen Fassung angeboten wird. Darunter fallen zunächst alle Werke, die schon nach alter Rechtslage als vergriffen galten, d.h. nicht mehr im Handel verfügbar sind. Zudem sind unter der neuen Terminologie aber nun auch Werke erfasst, die zwar irgendwann einmal durch den Urheber veröffentlicht wurden, aber noch nie im Handel erhältlich waren. Hat die jeweilige Einrichtung mit einem ver-

⁵ aml. Begr. BT-Drs. S. 110

⁶ Vertiefend Tiessen: „Vergriffen heißt nicht vergessen“, DFN-Infobrief Recht 01/2020

treibbaren Aufwand ohne Erfolg versucht, ein Angebot des Werkes am Markt aufzufinden, so wird unwiderleglich vermutet, dass dieses vergriffen ist.

Nach wie vor besteht ein Widerspruchsrecht des Rechtsinhabers. Der Widerspruch führt zur Unwirksamkeit der Rechteinräumung. Anders als bisher muss der Widerspruch nicht gegenüber dem Deutschen Patent- und Markenamt (DPMA), sondern gegenüber dem Amt der Europäischen Union für geistiges Eigentum (EUIPO) erfolgen. In diesem Zuge wird auch das bisher gem. § 52 VGG aF beim DPMA geführte Register vergriffener Werke Ende 2025 geschlossen. Auf einem neuen europaweiten Online-Informationsportal des EUIPO müssen Verwertungsgesellschaften gem. § 52 Abs. 1 S. 1 Nr. 4 VGG nun sechs Monate vor Wirksamwerden der Rechteinräumung über das betreffende Werk und die Rechteinräumung an selbigem informieren. Rechtsinhaber können so ihr Werk identifizieren und der Rechteinräumung im Anschluss ggf. widersprechen oder Ansprüche auf Zahlung von anteiligen Einnahmen geltend machen.

Der neue § 52 VGG weist lediglich Kulturerbe-Einrichtungen (also Bibliotheken, Museen und Archive sowie Einrichtungen im Bereich des Tonerbes) als mögliche Profiteure der vereinfachten Nutzungsrechtseinräumung aus. Unter der bisherigen Rechtslage waren Bildungseinrichtungen wie Hochschulen im Gesetz ausdrücklich genannt. Vieles spricht jedoch dafür, dass Hochschulen auch nach wie vor erfasst sind, da diese in der Regel über eingegliederte Bibliotheken oder zumindest Archive verfügen.

Für Hochschulangestellte in Bibliotheken oder Archiven ergibt sich im Ergebnis durch das Umsetzungsgesetz folgende Regel: Haben sie mit einigem Aufwand den Markt nach Angeboten des jeweiligen Werks durchsucht, so dürfen sie sich bis zu einem etwaigen Widerspruch des Rechtsinhabers sicher sein, dass die Verwertungsgesellschaft die richtige Stelle für die Rechteinräumung ist.

4. Verantwortlichkeit von Upload-Plattformen

Im Januar 2020 informierten wir bereits umfassend über die durch die DSM-RL vorgesehene urheberrechtliche Verantwortlichkeit von Upload-Plattformen. Insbesondere setzten

wir uns mit der Problematik von Upload-Filtern auseinander.⁷ An dieser Stelle soll zunächst ein kurzer Überblick über die Umsetzung der europäischen Regelungen durch das UrhDaG erfolgen. Eine detaillierte Aus- und Bewertung der neuen Vorschriften werden wir im Infobrief vornehmen, nachdem das Gesetz am 1. August 2021 in Kraft getreten ist und die praktischen Auswirkungen spürbar geworden sind. Zwar sind Hochschulen, sofern sie selbst Upload-Plattformen betreiben (beispielsweise ein universitätseigenes Videoportal, auf dem Studierende Inhalte hochladen können), gem. Art. 2 Nr. 6 der DSM-RL (umgesetzt in § 3 Nr. 2 UrhDaG) von den Änderungen der DSM-RL ausgenommen, gleichwohl sind sie wie jeder andere Internetnutzer von den Regelungen im praktischen Umgang mit dem Internet betroffen (beispielsweise bei der Nutzung der Plattform „YouTube“ durch die Hochschule zu Zwecken der Öffentlichkeitsarbeit).

Mit Inkrafttreten des UrhDaG am 1. August 2021 werden Upload-Plattformen wie YouTube (nach der Terminologie des UrhDaG „Diansteanbieter“) für von Nutzern hochgeladene Inhalte gem. § 1 Abs. 1 UrhDaG verantwortlich sein. Sie können dementsprechend künftig bei einer Verletzung des Urheberrechts von Rechtsinhabern auf Unterlassung und Schadensersatz in Anspruch genommen werden. Bisher war eine Inanspruchnahme nur möglich, wenn sie Kenntnis von der Rechtsverletzung hatten und trotzdem untätig geblieben sind (d.h. die betreffenden Inhalte nicht von ihrer Plattform entfernt haben).

Die Befreiung der Diansteanbieter von der Möglichkeit zur Inanspruchnahme ist für Diansteanbieter zwar nach wie vor möglich, aber an weitaus strengere Voraussetzungen geknüpft als bisher. Insbesondere müssen sich Diansteanbieter nun laufend darum bemühen, die vertraglichen Nutzungsrechte für geschützte Inhalte zu erwerben. Der nationale Gesetzgeber sieht vor, dass „bestmögliche Anstrengungen“ zum Erwerb der Nutzungsrechte unternommen werden müssen. Insofern ist die Formulierung ggü. der deutschen Fassung der DSM-RL („alle Anstrengungen“) abgemildert. Zu den bestmöglichen Anstrengungen gehört insbesondere die Zusammenarbeit mit Verwertungsgesellschaften, die in der Regel Urheberrechte einer Mehrzahl von Urhebern wahrnehmen.

⁷ Gielen: „First Rule: You Do Not Talk About Uploadfilter“, DFN-Infobrief Recht 01/2020

Weiterhin müssen Diensteanbieter Inhalte umgehend blockieren, sobald der Rechtsinhaber dies verlangt. Unter gewissen Voraussetzungen müssen sie auch dafür sorgen, dass die geschützten Inhalte in Zukunft nicht mehr hochgeladen werden.

Der dadurch entstehenden Gefahr des Overblockings von Inhalten durch den Einsatz automatisierter Identifikations- und Blockierungsverfahren (insb. durch den Einsatz von Upload-Filtern) versucht der deutsche Gesetzgeber auf zweierlei Weise beizukommen: Erstens wird durch Einführung eines Beschwerdeverfahrens sowohl für Nutzer als auch für Rechtsinhaber die Möglichkeit geschaffen, sich (auf Nutzerseite) gegen die Blockierung und (auf Rechtsinhaberseite) gegen die öffentliche Wiedergabe zur Wehr zu setzen. Zweitens werden durch das neu eingeführte Rechtsinstrument der mutmaßlich erlaubten Nutzungen bestimmte Fälle geschaffen, in denen die Diensteanbieter die Inhalte trotz Blockierungsverlangen der Rechtsinhaber zunächst nicht blockieren müssen. Erst nach Einlegung einer Beschwerde durch den Rechtsinhaber kann es dann zur Löschung kommen. Zu diesen Fällen gehört insbesondere die nichtkommerzielle Nutzung kleinster Auszüge von Werken (beispielsweise im Rahmen von Parodien oder Internet-Memes). Wie wirksam die genannten Rechtsinstrumente sind, kann gegenwärtig noch nicht gesagt werden. Ob sie einem aggressiven Overblocking vorbeugen, muss Gegenstand einer Evaluierung nach Inkrafttreten des Gesetzes sein. Jedenfalls hat der deutsche Gesetzgeber den Spielraum der DSM-RL genutzt, die lediglich abstrakt vorgab, dass die neu eingeführte Verantwortlichkeit von Diensteanbietern nicht dazu führen darf, dass Inhalte, die nicht gegen das Urheberrecht verstoßen, blockiert werden.

Bemerkenswert ist schließlich der durch § 4 Abs. 3 UrhDaG vorgesehene Direktvergütungsanspruch von Urhebern gegen den Diensteanbieter. Gerade bei komplexen digitalen Verwertungen gewährleistet das Urhebervertragsrecht nicht automatisch, dass Kreative auch an den Einnahmen beteiligt werden, die verwertende Unternehmen (z.B. Musikverlage) mit der Lizenzierung an Diensteanbieter erzielen. Hat der Urheber das Recht der öffentlichen Wiedergabe einem Dritten eingeräumt, so hat der Diensteanbieter für die Nutzung des Werkes dem Urheber künftig gleichwohl eine angemessene Vergütung zu zahlen. Diensteanbieter können also in die Situation geraten, dass sie dem Dritten (zum Beispiel einem Musikverlag) zunächst Lizenzgebühren für die Einräumung von Nutzungsrechten bezahlen und zusätzlich dem Urheber direkt eine

angemessene Vergütung zahlen müssen. Nach alter Rechtslage genügte die Entrichtung von Lizenzgebühren an den Dritten.

III. Fazit und Auswirkungen für Hochschulen

Die praktischen Auswirkungen der nationalen Umsetzung der DSM-RL durch das Gesetz zur Anpassung des Urheberrechts an die Erfordernisse des Digitalen Binnenmarktes sind immens. Viele Regelungen betreffen Hochschulen unmittelbar. Dazu gehören insbesondere die geänderten Vorschriften zum Text- und Data-Mining und zu nicht verfügbaren Werken. Hier sind sogar kombinierte Anwendungsmöglichkeiten denkbar. Beispielsweise kann es sein, dass eine Hochschulbibliothek ihren Bestand an nicht verfügbaren Werken digitalisieren und dabei gleichzeitig gewisse Muster innerhalb dieses Bestandes erkennen möchte. Die reine Vervielfältigung kann ihr in so einem Fall nach § 60d UrhG erlaubt sein. Für eine anschließende Zugänglichmachung des Bestandes gegenüber der Allgemeinheit kann sie sich für die vereinfachte Lizenzierung an die zuständige Verwertungsgesellschaft wenden. Sofern kein unmittelbarer Hochschulbezug gegeben ist, besteht er jedenfalls mittelbar. Die Vorschriften des UrhDaG zur Verantwortlichkeit von Upload-Plattformen betreffen praktisch jeden Nutzer dieser Plattformen. Immer öfter verwenden auch Universitäten oder universitätseigene Institute Plattformen wie YouTube zur Öffentlichkeitsarbeit oder gar zur Vermittlung von Wissen. Eine hochschulinterne Auseinandersetzung mit den Änderungen durch das Umsetzungsgesetz bietet Chancen und kann insbesondere neue Möglichkeiten der Benutzung geschützter Werke für wissenschaftliche Zwecke aufzeigen.

Im Hinterzimmer zur Netzsperrre

Die neue Clearingstelle Urheberrecht im Internet (CUII)

von Nico Gielen

Das Schreckgespenst der Netzsperrren ist wieder da – diesmal im Gewand der Clearingstelle Urheberrecht im Internet. Ein Zusammenschluss aus Internetzugangsanbietern, führenden Medienunternehmen und der Bundesnetzagentur stellt seit Januar 2021 ein Verfahren zur Verfügung, durch das innerhalb weniger Wochen „strukturell urheberrechtsverletzende Webseiten“ mit einer Netzsperrre belegt werden können. Dies bildet einen geeigneten Anlass, die Relevanz von Netzsperrren herauszustellen und gleichzeitig die neue Organisation zu beleuchten.

I. Einleitung

Netzsperrren sind schon länger Gegenstand hitziger netzpolitischer Diskussionen. 2009 schafften sie es sogar in die allgemeine Presse, weil Ursula von der Leyen als damalige Familienministerin Netzsperrren vorschlug, um den Zugang zu Webseiten mit kinderpornographischen Inhalten zu erschweren. Das entsprechende Zugangerschwerungsgesetz sah vor, dass das Bundeskriminalamt (BKA) gerichtlich ungeprüfte Listen mit Webseiten führen sollte, welche durch Internetzugangsanbieter mit Netzsperrren belegt werden sollten.¹ Dem Gesetz folgte allerdings so viel Kritik, dass zunächst das BKA angewiesen wurde, doch keine Sperrlisten zu führen, bis das Gesetz 2011 wieder vollständig aufgehoben wurde.

An der Diskussion zum Zugangerschwerungsgesetz wird deutlich, welche netzpolitische Sprengkraft das Thema der Netzsperrren in sich birgt. Nichtsdestotrotz wagt sich nun die Clearingstelle Urheberrecht im Internet (CUII) erneut daran und verspricht Rechteinhabern, Netzsperrren innerhalb weniger Wochen errichten zu können. Dies impliziert, dass immer noch ein erheblicher Bedarf nach Netzsperrren besteht.

II. Der Bedarf nach Netzsperrren

Möchte ein Rechteinhaber gegen eine Webseite vorgehen, auf welcher seine Inhalte ohne seine Erlaubnis dargestellt werden, stehen ihm prinzipiell zwei Möglichkeiten offen. Die erste Möglichkeit besteht darin, gegen den Betreiber der Webseite vorzugehen und auf Grundlage des urheberrechtlichen Beseitigungsanspruchs (§ 97 Abs. 1 S. 1 Urheberrechtsgesetz) zu versuchen, eine Löschung der urheberrechtswidrigen Inhalte zu erzielen. Diese Vorgehensweise ist aber meist aussichtslos, wenn sich der Betreiber und die benutzten Server im Ausland befinden.

In solchen Fällen erscheint daher die alternative Möglichkeit, die Internetzugangsanbieter zu einer Netzsperrre zu bewegen, erfolgsversprechender. Eine Netzsperrre erfolgt meist im Domain Name System (DNS), welches die Anfrage eines Nutzers zum Aufruf einer bestimmten Domain in eine IP-Adresse übersetzt, die wiederum einer bestimmten Webseite zugeordnet ist. Diese Übersetzungsleistung kann verhindert werden, indem Internetzugangsanbieter auf ihren Servern für bestimmte Domains die Einträge für die dahinterstehenden IP-Adressen entfernen (DNS-Sperre). Daneben können Internetzugangsanbieter auch gesamte IP-Adressen (IP-Sperre) oder nur einzelne Seiten eines Internetauftritts sperren (URL-Sperre). Netzsperrren führen also nicht zur Löschung der schädlichen Inhalte, sodass sie über andere Zugriffspunkte weiterhin verfügbar bleiben. Damit stellen sie nur die zweitbeste Lösung dar. Nichtsdestotrotz können sie den Zugriff auf die entsprechende Webseite zumindest erschweren.

¹ Hierzu Bröckers/Obex, Zur Umsetzung des Zugangerschwerungsgesetzes in Wissenschaftseinrichtungen, DFN-Infobrief Recht 07/2009, S. 2 ff.

III. Der ordentliche Rechtsweg zur Netzsperrung

Aus dem Unionsrecht folgt, dass Rechteinhaber gegen Internetzugangsanbieter einen Anspruch auf Errichtung einer Netzsperrung geltend machen können. Dies führte der Europäische Gerichtshof (EuGH) in einem Urteil aus dem Jahr 2014 auf Art. 8 Abs. 3 der EU-Richtlinie 2001/29 (InfoSoc-RL) zurück, wonach die Mitgliedstaaten gerichtliche Anordnungen gegen Vermittler ermöglichen müssen, deren Dienste von einem Dritten zur Verletzung urheberrechtlich geschützter Inhalte genutzt werden (Az. C-314/12 – UPC Telekabel).² Hierunter fasste der EuGH auch Internetzugangsanbieter, unterstellte die Modalitäten einer Sperrverpflichtung aber der Ausgestaltung durch die Mitgliedstaaten.

Im Hinblick auf diese unionsrechtlichen Vorgaben entschied der Bundesgerichtshof (BGH) im Jahr 2015, dass die Rechtsgrundlage für einen solchen Sperranspruch im deutschen Recht in der Störerhaftung liege (Urt. v. 26.11.2015, Az. I ZR 3/14 und I ZR 174/14).³ Die Störerhaftung stützt der BGH auf eine analoge Anwendung des § 1004 Abs. 1 Bürgerliches Gesetzbuch, die neben einer Rechtsverletzung voraussetzt, dass der Anspruchsgegner erstens willentlich und adäquat kausal zur Verletzung des geschützten Rechtsguts beiträgt und ihm zweitens zuzumuten ist, die Rechtsverletzung zu unterbinden.

Nach dieser Entscheidung meldete sich 2017 auch der Gesetzgeber zu Wort. Im Bestreben, die Haftungsgefahren beim Betrieb von WLAN zu verringern, brachte dieser eine Gesetzesänderung auf den Weg, die en passant auch die Rechtsgrundlage für Netzsperrungen in Frage stellte.⁴ Zunächst wurde § 8 Abs. 1 S. 2 Telemediengesetz (TMG) eingeführt, wonach Diensteanbieter nicht wegen einer rechtswidrigen Handlung

eines Nutzers auf Schadensersatz, Beseitigung oder Unterlassung einer Rechtsverletzung in Anspruch genommen werden können. Damit wurde die Störerhaftung für WLAN-Betreiber und alle übrigen Diensteanbieter im Sinne des § 8 TMG ausdrücklich abgeschafft. Auch die Anspruchsgrundlage gegen Internetzugangsanbieter zur Errichtung von Netzsperrungen wurde damit beseitigt.

Der Gesetzgeber führte außerdem § 7 Abs. 4 S. 1 TMG ein, der eine Rechtsgrundlage für Sperrverpflichtungen gegen WLAN-Betreiber darstellt. Diese Vorschrift wurde aber ausdrücklich auf WLAN-Anbieter und nicht auf Internetzugangsanbieter zugeschnitten. Somit wäre es für Letztere dabeigebieben, dass die Störerhaftung abgeschafft ist. Damit hätte aber entgegen der Vorgaben des EuGH keine Möglichkeit mehr bestanden, Internetzugangsanbieter zur Errichtung von Netzsperrungen zu verpflichten. Daher entschied der BGH, dass § 7 Abs. 4 S. 1 TMG unionsrechtskonform auszulegen und im Wege der Analogie ebenfalls auf Internetzugangsanbieter zu erstrecken sei (Urt. v. 26.7.2018, Az. I ZR 64/17 – Dead Island).⁵ Daher wird die Rechtsgrundlage von Sperranordnungen gegen Internetzugangsanbieter mittlerweile überwiegend nicht mehr in der Störerhaftung, sondern in § 7 Abs. 4 TMG analog gesehen.

IV. Die neue Abkürzung zur Netzsperrung: Die Clearingstelle Urheberrecht im Internet

Den Initiatoren der CUII schien der durch die Gesetzgebung und Rechtsprechung geebnete Weg zu Netzsperrungen nicht ausgereicht zu haben. Denn nach einer zweijährigen Konsultation von Internetzugangsanbietern, Rechteinhabern, der Bundesnetzagentur (BNetzA) und dem Bundeskartellamt (BKartA) errichteten sie Anfang 2021 mit der CUII ein außergerichtliches Verfahren zur Errichtung von Netzsperrungen für eindeutig urheberrechtsverletzende Webseiten. Zu den Gründungsmitgliedern aufseiten der Internetzugangsanbieter gehören neben der Telekom und Vodafone auch 1&1, Telefónica und Mobilcom-Debitel. Damit sind die größten Unternehmen des deutschen Marktes für Internetzugänge im CUII vertreten. Aber auch auf der Seite der Rechteinhaber sind namhafte Einrichtungen ver-

² Kuta, Bis hierhin und nicht weiter! – EuGH zur Verpflichtung eines Access-Providers zu Netzsperrungen, DFN-Infobrief Recht 06/2014, S. 8 ff.

³ Klein, Den Letzten beißen die Hunde – Bundesgerichtshof öffnet die Tür für obligatorische Netzsperrungen durch Access-Provider, DFN-Infobrief Recht 04/2016, S. 2 ff.; siehe zu den Vorinstanzen Klein, Löst dem Internet die Fesseln! – OLG Hamburg verneint Pflicht eines Access-Providers zur Einrichtung von IP-, URL- und DNS-Sperrungen, DFN-Infobrief Recht 03/2014, S. 9 ff.; Klein, Macht die Schotten dicht – oder doch nicht? – Oberlandesgericht Köln hält Verpflichtung zur Einrichtung von Netzsperrungen durch Internetzugangsanbieter für unzumutbar, DFN-Infobrief Recht 11/2014, S. 5 ff.

⁴ Klein, Wer hat noch nicht, wer will noch mal? – Gesetzgeber schafft Störerhaftung für WLAN-Betreiber ab und führt Sperrverpflichtungen ein, DFN-Infobrief Recht 11/2017, S. 11 ff.

⁵ Baur, Zugang gesperrt! Bitte nicht stören! – Der BGH zur unionsrechtskonformen Auslegung des neuen Telemediengesetzes, DFN-Infobrief Recht 10/2018, S. 2 ff.

treten, wie zum Beispiel Sky, der Börsenverein des Deutschen Buchhandels, die Deutsche Fußballliga und die Motion Picture Association. Sowohl die BNetzA und das BKartA als auch das Bundeswirtschaftsministerium gaben Pressemitteilungen heraus und befürworteten die CUII ausdrücklich.

1. Lenkung durch den Steuerungskreis

Die CUII ist ein Zusammenschluss aus privaten Verbänden, der neben einer verwaltenden Geschäftsstelle aus Prüfungsausschüssen und einem Steuerungskreis besteht.⁶ Der Steuerungskreis ist paritätisch aus Rechteinhabern und Internetzugangsanbietern besetzt und übernimmt eine Lenkungs-funktion. Unter anderem bestimmt er über die anwendbaren Verfahrensregeln und setzt die Höhe der Vergütung der Prüfer fest. Seine Hauptaufgabe besteht darin, drei Pools von Prüfern zu besetzen, aus denen später einzelne Prüfungsausschüsse gebildet werden. Ein Pool soll dabei auf Vorschlag der Rechteinhaber und ein anderer Pool auf Vorschlag der Internetzugangsdienste besetzt werden. Der dritte Pool soll aus unabhängigen Prüfern bestehen.

2. Entscheidung durch den Prüfungsausschuss

Ein Prüfungsausschuss besteht aus einem Vorsitzenden und zwei Beisitzern. Der Vorsitz der Prüfungsausschüsse wird durch ehemalige Richter des Urheberrechtssenats des BGH geführt. Ein Ausschuss prüft erstens, ob eine bestimmte Webseite strukturell urheberrechtsverletzend ist. Nach der Verfahrensordnung der CUII gilt eine Webseite als strukturell urheberrechtsverletzend, wenn sie zumindest auch auf Internetnutzer in Deutschland ausgerichtet ist und auf ihr klare Verletzungen des deutschen Urheberrechtsgesetzes stattfinden. Auf der zweiten Stufe prüft der Ausschuss, ob die Umsetzung einer DNS-Netzsperrung nach der Rechtsprechung des BGH rechtmäßig ist. Insbesondere wird geprüft, ob der Antragssteller zuvor gegen jene vorgegangen ist, die der Urheberrechtsverletzung näher sind, also den Täter der Urheberrechtsverletzung und den Betreiber des verwendeten Servers (sog. Subsidiarität). Die Entscheidung eines Prüfungsausschusses – von denen pro Jahr bis zu 200 ergehen können – müssen einstimmig erfolgen.

⁶ Siehe für die folgenden Ausführungen den Verhaltenskodex und die Verfahrensordnung der CUII, abrufbar unter www.cuii.info.

3. Überprüfung durch die Bundesnetzagentur

Liegt die Entscheidung eines Prüfungsausschusses gegen eine Webseite vor, wird sie der BNetzA weitergeleitet. Diese wiederum soll die Übereinstimmung einer DNS-Netzsperrung mit den unionsrechtlichen Vorgaben zur Netzneutralität bewerten. Diese Vorgaben ergeben sich aus der EU-Verordnung 2015/2120 über Maßnahmen zum Zugang zum offenen Internet (Telecom Single Market Verordnung, kurz: TSM-VO). Mit der Netzneutralität möchte man die Gleichbehandlung aller im Internet übertragenen Datenpakete und hierdurch einen diskriminierungsfreien Zugang zum Internet gewährleisten.⁷ Daher ist eine Blockierung von Datenpaketen und somit auch eine Netzsperrung im Grundsatz verboten. Allerdings sind nach der TSM-VO Ausnahmen vorgesehen. Insbesondere erlaubt Art. 3 Abs. 3 UAbs. 3 lit. a TSM-VO den Internetzugangsanbietern, von dem Leitprinzip der Netzneutralität abzuweichen, wenn dies erforderlich ist, um einer Rechtsvorschrift zu entsprechen. Nach Erwägungsgrund 11 sind damit insbesondere solche Vorschriften angesprochen, welche die Blockierung bestimmter Inhalte vorschreiben. Allerdings wird in diesem Erwägungsgrund ebenfalls betont, dass eine solche Ausnahme nur zur Anwendung kommen darf, wenn dies verhältnismäßig ist und angemessene Verfahrensgarantien gewährleistet sind. Unter diesem Vorzeichen scheint die Einbindung der BNetzA zwar zunächst begrüßenswert. Die BNetzA führt allerdings kein förmliches Verfahren durch, sondern sie gibt lediglich eine unverbindliche und formlose Stellungnahme ab und behält sich ausdrücklich vor, noch ein förmliches Verfahren durchzuführen. In einem Interview hat die BNetzA außerdem offenbart, lediglich eine oberflächliche Prüfung und nur auf Beschwerde hin eine tiefgehende Prüfung vorzunehmen.⁸

4. Umsetzung durch die Internetzugangsanbieter

Wenn die BNetzA ihre formlose Unbedenklichkeitserklärung abgibt, wird diese den Internetzugangsanbietern weitergelei-

⁷ Siehe zur Netzneutralität ausführlich Gielen, Dream on, Telekom! – Das Oberverwaltungsgericht für das Land Nordrhein-Westfalen bekräftigt die Argumentation der Bundesnetzagentur, wonach das Angebot „StreamOn“ der Telekom die Netzneutralität verletzt, DFN-Infobrief Recht 09/2019, S. 2 ff.

⁸ Bündler/Budras, Kommt jetzt das Ende der illegalen Streamingseiten?, F.A.Z. Einspruch v. 10. März 2021.

tet, die sodann verpflichtet sind, die DNS-Sperre unverzüglich zu implementieren. Die Rechteinhaber geben den Internetzugangsanbietern hierfür einen erheblichen Anreiz, indem sie diese in der Verfahrensordnung der CUII für den Fall, dass sich die DNS-Sperre im Nachhinein als rechtswidrig herausstellt, von der Haftung freistellen. Wird versucht, die Internetseite nach Implementierung aufzurufen, wird der Nutzer auf eine Informationsseite der CUII umgeleitet, die den Hinweis enthält, dass die Seite aufgrund von Urheberrechtsverletzungen gesperrt wurde.

5. Rechtsschutzmöglichkeiten

Die Entscheidung der CUII ist nicht zwingend endgültig, sodass immer noch der ordentliche Rechtsweg beschritten werden kann. Allerdings besteht die Einschränkung, dass die Mitglieder der CUII zuvor das interne Beschwerdeverfahren durchlaufen müssen. Sollte unter Einhaltung dieser Voraussetzung ein staatliches Gerichtsverfahren initiiert werden, dürfen die Beteiligten der CUII außerdem nicht einander als Zeugen für Tatsachen benennen. Hiermit, durch andere Vertraulichkeitsvorschriften sowie durch die Anonymität der Prüfer, wird versucht, über das Verfahren der CUII „den Mantel des Schweigens“ zu legen.

Damit kann die Allgemeinheit erst auf eine DNS-Sperre aufmerksam werden, nachdem sie bereits etabliert ist. Der Betreiber einer Webseite sieht sich damit vor vollendete Tatsachen gestellt. Die CUII möchte zwar Stellungnahmen von Internetnutzern entgegennehmen. Da diese am Verfahren aber nicht beteiligt werden, ist ihnen das faktisch nicht möglich. Auch ansonsten haben Internetnutzer wenig Möglichkeiten gegen eine DNS-Sperre vorzugehen. Etwaige Beschwerden können lediglich innerhalb der jeweiligen Vertragsbeziehung mit dem Internetzugangsanbieter geltend gemacht werden.

V. Bewertung der Clearingstelle Urheberrecht im Internet

Die CUII verspricht ein pragmatisches Verfahren. Statt eines jahrelangen Gerichtsprozesses kann man mit dem Verfahren der CUII innerhalb weniger Wochen zu einer Netzsperrung gelangen. Gegenüber dem Gerichtsverfahren ist dies zweifelsohne ein großer Vorteil für die Rechteinhaber. Dem halten Kritiker allerdings einige Nachteile entgegen:

1. Fragwürdige Effektivität

Einer der größten Kritikpunkte liegt darin, dass Netzsperrungen nicht effektiv seien. Sie seien leicht zu umgehen und ihre Effektivität daher fraglich. Tatsächlich kann man mit wenig Mühe einen anderen DNS-Server verwenden und somit eine mit einer Netzsperrung belegte Webseite wieder aufrufen. Außerdem kann eine DNS-Sperre auch durch den Betreiber der Webseite umgangen werden, indem er mit seiner Webseite zu einer neuen Adresse „umzieht“. Vor diesem Hintergrund ist die Kritik an der CUII, welche sich ausschließlich auf DNS-Sperrungen stützt, nachvollziehbar. Gleichwohl kann eine DNS-Sperre die Aufrufzahlen einer Webseite reduzieren, indem technisch weniger versierte Nutzer vom Abruf abgehalten werden und die Hemmschwelle zum Abruf urheberrechtsverletzender Inhalte erhöht wird. Daher stellt eine DNS-Sperre, insbesondere, wenn sie durch die CUII zügig erzielt werden kann, dennoch eine effiziente Alternative zu einem langwierigen Gerichtsprozess dar.

2. Zweifel an privatisierter Rechtsdurchsetzung

Daneben besteht allerdings die Frage, ob es gerechtfertigt ist, das übliche Verfahren zu DNS-Netzsperrungen durch ein privatisiertes Prozedere zu ersetzen. Zwar möchte sich die CUII auch an die Rechtsprechung von EuGH und BGH halten. Diese Rechtsprechung baut allerdings auf der Prämisse auf, dass ein Sperrverfahren im Rahmen eines Verfahrens vor staatlichen Gerichten abläuft. Auch die eingangs genannten Rechtsgrundlagen für Netzsperrungen weisen in diese Richtung. So schreiben die EU-Richtlinien nur vor, dass die Mitgliedstaaten gerichtliche Anordnungen gegen Internetzugangsanbieter ermöglichen müssen. Entsprechend erlaubt auch der deutsche Gesetzgeber mit dem Sperranspruch des § 7 Abs. 4 TMG lediglich gerichtliche Anordnungen.

Dagegen könnte man jedoch halten, dass die genannten Vorschriften zwar gerichtliche Verfahren vorschreiben, aber private Lösungen nicht verbieten. Gleichwohl sollten zumindest grundlegende Verfahrensgarantien gewährleistet werden. Dies ist auch eine Lehre, die man bereits aus der Privatisierung von Domainnamenstreitigkeiten gezogen hat. Diese werden oftmals nach dem ebenfalls privaten Verfahren der Uniform Domain Name Dispute Resolution Policy (UDRP) geführt, das ebenfalls als effiziente Alternative zum ineffektiv empfundenen

nen Gerichtsverfahren gesehen wird. Allerdings wurde der mit dem UDRP-Verfahren einhergehende Pragmatismus auch zum größten Angriffspunkt. Kritiker bemängeln einen Mangel an rechtsstaatlichen Gewährleistungen, der dazu führt, dass die antragsstellenden Markeninhaber gegenüber den Antragsgegnern, also den Domaininhabern, überraschend oft obsiegen.

Die CUII sollte diese Angriffsfläche also nicht bieten, sondern ein faires Verfahren gewährleisten. Vor diesem Hintergrund wirkt jedoch zweifelhaft, dass die Prüfer des CUII-Verfahrens aus Pools gewählt werden, die wiederum durch die Parteien, also die Rechteinhaber und Internetzugangsanbieter, besetzt werden. Der Vorsitzende eines Prüfausschusses wird zwar nicht unmittelbar durch die Parteien, sondern den Steuerungskreis besetzt, allerdings besteht dieser ebenfalls aus Rechteinhabern und Internetzugangsanbietern. Hinzu kommt, dass die Honorare der Prüfer durch die antragsstellenden Rechteinhaber finanziert werden. Diese Verfahrensgestaltung lässt Anreize seitens der Parteien zu, welche die Neutralität der Prüfer gefährden können.

Dagegen könnte man halten, dass es mit dem Schiedsverfahren eine private Verfahrensart gibt, welches in der Zivilprozessordnung (ZPO) sogar gesetzlich anerkannt ist und ebenfalls die Möglichkeit einräumt, dass die Parteien jeweils einen Schiedsrichter benennen (§ 1035 Abs. 3 S. 2 ZPO). Das Verfahren der CUII ist jedoch kein Schiedsverfahren, denn für ein solches müsste der ordentliche Rechtsweg ausgeschlossen werden; das ist – wie oben erwähnt – nicht der Fall. Ein wesentlicher Unterschied zwischen dem CUII-Verfahren und einem Schiedsverfahren besteht dann auch darin, dass den Parteien eines Schiedsverfahrens das Recht zustünde, einen Schiedsrichter abzulehnen, wenn berechtigte Zweifel an seiner Neutralität bestehen (§ 1036 Abs. 2 S. 1 ZPO). Die Verfahrensordnung der CUII räumt ein solches Ablehnungsrecht allerdings nicht ein. Vielmehr gelten die Prüfer danach schlicht als unbefangen. Nach der Verfahrensordnung hätten die Vorsitzenden „die unparteiische Ausübung ihrer Tätigkeit in Justiz, Verwaltung oder Wissenschaft nachgewiesen“. Diese (zweifelloso bestehende) Erfahrung bietet aber kein Garanten dafür, dass im Einzelfall nicht doch ein Interessenkonflikt auftreten kann.

3. Blockierung legaler Inhalte

Oftmals wird kritisiert, dass eine Netzsperrung zu einer Blockierung legaler Inhalte führen könnte. Dies ist auch der Fall, wenn

eine Webseite mit einer Netzsperrung belegt wird, diese Webseite aber auch legale Inhalte aufweist. Allerdings hat der BGH dies ausdrücklich zugelassen. Dahinter steht die Erwägung, dass ein Webseitenbetreiber seiner Inanspruchnahme entgegen könnte, indem er auch einige legale Inhalte öffentlich darstellt. Die Toleranz des BGH geht jedoch nur soweit, wie die legalen Inhalte im Gesamtverhältnis nicht ins Gewicht fallen. Diese Voraussetzung sei noch nicht erfüllt, wenn vier Prozent legale Inhalte gesperrt würden (Urt. v. 26.11.2015, Az. I ZR 174/14). Wo allerdings die magische Grenze liegt, vermochte der BGH nicht zu sagen.

Sollte die CUII diese unbestimmte Grenze – die ein staatliches Gericht ebenso gut anders auslegen könnte als die CUII – überschreiten, könnte daraus auch ein wettbewerbsrechtliches Problem werden. Denn mit den Rechteinhabern befinden sich auch Marktakteure in der CUII, die mit Streaminganbietern im Wettbewerb stehen. Zwar sind Webseitenbetreiber nicht schutzwürdig, solange sie klare Fälle von strukturellen Urheberrechtsverletzungen begehen. Bezogen auf Grenzfälle kann es jedoch problematisch sein, wenn aus einer privaten Initiative heraus Netzsperrungen gegen Wettbewerber gerichtet werden. Daher hängt es maßgeblich davon ab, ob die CUII sich daranhält, ausschließlich gegen Webseiten vorzugehen, die klare und strukturelle Urheberrechtsverletzungen begehen. Sollte die CUII diese – erneut: unbestimmte – Grenze überschreiten, wird sie mit einer Intervention des BKartA rechnen müssen.

VI. Bedeutung für Hochschulen und Forschungseinrichtungen

Das Thema der Netzsperrungen ist auch für den Hochschulbereich wichtig, denn die Hochschulrechenzentren sind Anbieter von Internetzugängen für Studierende und Mitarbeiter. Damit haben sie ein gesteigertes Interesse daran, ob und unter welchen Voraussetzungen Netzsperrungen beansprucht werden können. Bei Hochschulen und Forschungseinrichtungen ist auch stets zu berücksichtigen, dass deren Internetzugänge besonders schutzwürdig sind, da hierdurch Forschung und Lehre ermöglicht wird. Bei einer Grundrechtsabwägung, die vor der Errichtung einer Netzsperrung zwingend erfolgen muss, ist also auch die Forschungs- und Lehrfreiheit des Art. 5 Abs. 3 Grundgesetz zu berücksichtigen. Auch wegen der im Vergleich zu kommerziellen Internetzugangsanbietern relativ kleinen

Nutzerzahl kann eine Netzsperrung von Hochschulrechenzentren unter Umständen abgewehrt werden.

Im Hinblick auf die CUII sind die Internetzugänge, welche über die Rechenzentren der Hochschulen und Forschungseinrichtungen unterhalten werden, ebenfalls von Interesse. Bisher sind bei der CUII zwar nur kommerzielle Internetzugangsanbieter gelistet, sodass die von der CUII gesperrten Webseiten über die Universitätsnetze immer noch abrufbar sind. Gleichwohl ist nicht auszuschließen, dass die CUII auch andere Internetzugangsanbieter zu einer Mitgliedschaft einlädt. In einem solchen Fall sollten die hier dargestellten Vor- und Nachteile sorgsam gegeneinander abgewogen werden.

Ausgelöscht.

Das unberechtigte Löschen von Daten rechtfertigt eine fristlose Kündigung gegenüber dem Arbeitnehmer

von *Nicolas John*

Das Landesarbeitsgericht LAG Baden-Württemberg entschied mit Urteil vom 17. September 2020 (Az.: 17 Sa 8/20), dass die fristlose Kündigung des Arbeitgebers gegenüber seinem Arbeitnehmer wirksam ist, wenn dieser zuvor Daten ohne Rücksprache mit dem Arbeitgeber vom Server des Unternehmens löscht. Insbesondere liege in diesem Verhalten des Arbeitnehmers ein wichtiger Grund für die außerordentliche Kündigung vor. Ob das Verhalten des Arbeitnehmers strafbar ist oder dabei personenbezogene Daten gelöscht werden, ist nicht von zentraler Bedeutung.

I. Hintergrund

Gemäß § 626 Abs. 1 BGB kann der Arbeitgeber seinem Arbeitnehmer fristlos kündigen, wenn ein wichtiger Grund vorliegt. Dieser berechtigt zur Kündigung vor Ablauf der ordentlichen Kündigungsfrist, wenn dem Arbeitgeber unter Berücksichtigung aller Umstände des Einzelfalls und unter Abwägung der Interessen beider Vertragsteile eine Fortsetzung des Arbeitsverhältnisses nicht mehr zumutbar ist. Die außerordentliche Kündigung stellt das schärfste Mittel dar und kann daher nur als letzte Konsequenz erfolgen. Vorher ist im Rahmen einer Verhältnismäßigkeitsprüfung stets zu untersuchen, ob bei einem steuerbaren Verhalten des Arbeitnehmers zunächst eine Abmahnung oder eine ordentliche Kündigung ausreichend gewesen wäre.

II. Sachverhalt

Der klagende Arbeitnehmer war angestellter Key-Account-Manager im Außendienst bei der beklagten Arbeitgeberin. Weil der Arbeitnehmer gegen eine Weisung verstoßen hatte, freitags die Wochenplanung für die folgende Woche vorzulegen, kam es zu einem Gespräch zwischen der Arbeitgeberin und dem Arbeitnehmer. In diesem Gespräch bekundete die Arbeitgeberin ihre Absicht, das Arbeitsverhältnis einvernehmlich beenden zu wollen. Auf einen Aufhebungsvertrag konnten sich die Parteien aber nicht einigen. Am Ende des Gesprächs

verabschiedete sich der Arbeitnehmer bei der Mitarbeiterin der Arbeitgeberin mit den Worten „Man sieht sich immer zweimal im Leben“, bevor er das Betriebsgelände verließ.

Danach erschien der Arbeitnehmer nicht mehr bei der Arbeit, legte eine Arbeitsunfähigkeitsbescheinigung vor und löschte zwei Tage nach dem Gespräch ohne Rücksprache über 3.300 Dateien mit einem Umfang von 7,48 GB aus dem für ihn vorgesehenen Verzeichnis von dem Server der Arbeitgeberin. Zu den gelöschten Daten gehörten unter anderem „Umsatzmeldungen Handelsgruppen 2018“, Vorlagen zur Preisliste (Schweiz), Auswertungen von Daten des Bundesamts für Statistik, Daten zum Handel-Arbeitsschutz, eine Wettbewerbsanalyse, eine Auswertung Analyse Key-Account und ein Excel-Kalkulationstool.

Auf ein Anhörungsschreiben der Arbeitgeberin zu diesem Löschvorgang reagierte der Arbeitnehmer nicht. Daher reagierte die Arbeitgeberin gegenüber dem Arbeitnehmer auf den Vorgang mit einer fristlosen Kündigung, hilfsweise einer ordentlichen Kündigung des Arbeitsverhältnisses. Die Wiederherstellung der gelöschten Daten war der Arbeitgeberin später möglich.

Der Arbeitnehmer erhob gegen diese Kündigung zunächst Kündigungsschutzklage beim Arbeitsgericht (ArbG) Stuttgart und wies darauf hin, dass es sich bei den Daten um „seine Daten“ in „seinem Ordner“ gehandelt habe und diese nicht betriebsnotwendig bzw. nicht mehr erforderlich gewesen seien.

III. Entscheidung

Nachdem das ArbG Stuttgart (Kammer Aalen, Urteil vom 01.10.2019, Az.: 27 Ca 97/19) dem Arbeitnehmer teilweise Recht gab und das Vorliegen eines wichtigen Grundes im Sinne des § 626 BGB verneinte, jedoch die ordentliche Kündigung als wirksam und die Datenlöschung als bloße Nachlässigkeit ansah, urteilte das LAG Baden-Württemberg auf die Berufung des Arbeitnehmers, dass die fristlose Kündigung wirksam sei.

Für das LAG Baden-Württemberg stellt das Löschen der Daten einen wichtigen Grund im Sinne des § 626 Abs. 1 BGB dar. Durch diesen Vorgang habe der Arbeitnehmer arbeitsvertragliche Nebenpflichten erheblich verletzt, insbesondere seine Pflicht, der Arbeitgeberin den Zugriff auf betriebliche Dateien nicht zu verwehren. Dazu gehören Unterlagen, die dem Arbeitnehmer von der Arbeitgeberin zur Verfügung gestellt worden sind und die er während des Arbeitsverhältnisses, beispielsweise durch Schriftverkehr mit Dritten, erlangt hat. Auch selbst angelegte Akten, sonstige Unterlagen und Dateien, mit Ausnahme von privaten Aufzeichnungen, seien zu den betrieblichen Unterlagen zu zählen.

Die vom Arbeitnehmer gelöschten Daten seien von diesem Begriff der betrieblichen Unterlagen erfasst. Aufgrund der Löschung dieser Daten sei nach der Ansicht des LAG Baden-Württemberg eine Fortsetzung des Arbeitsverhältnisses bis zum Ende der Kündigungsfrist für die beklagte Arbeitgeberin unzumutbar. Dem Arbeitnehmer sei ebenfalls ein erheblicher Verschuldensvorwurf zu machen, denn er habe die über 3.300 Dateien nicht versehentlich gelöscht, sondern ganz bewusst, nachdem die Arbeitgeberin ihm mitgeteilt hatte, das Arbeitsverhältnis durch den Abschluss eines Aufhebungsvertrags beenden zu wollen. Angesichts seines Verhaltens müsse seitens der Arbeitgeberin befürchtet werden, dass der Arbeitnehmer in anderen möglichen Konfliktsituationen in ähnlicher Weise reagieren werde.

Eine Abmahnung war nach Auffassung des LAG nicht erforderlich, da der Arbeitnehmer in diesem Fall nicht annehmen könne, dass das unbefugte Löschen von geschäftlichen Daten aus Anlass eines Personalgesprächs von der Arbeitgeberin hingenommen werde. Der Abschied mit den Worten „man sieht sich immer zweimal im Leben“ und das Nicht-Erscheinen zur Arbeit mitsamt der Löschkaktion gleiche einer „Tabula rasa“. Das Gericht findet an dieser Stelle deutliche Worte, der

„Abkehrwille und die Bereitschaft, ‚verbrannte Erde zu hinterlassen‘ [könne] kaum [deutlicher] zum Ausdruck“ gebracht werden.

Nicht entscheidungserheblich war es für das LAG Baden-Württemberg, ob sich der Arbeitnehmer wegen Datenveränderung (§ 303a StGB) oder Computersabotage (§ 303b StGB) strafbar gemacht hat. Ebenso kam es für das Gericht nicht darauf an, ob und mit welchem Aufwand die Daten im späteren Verlauf wiederhergestellt werden konnten oder nicht, und ob diese Daten für den Betriebsablauf tatsächlich von Bedeutung sind.

IV. Fazit und Konsequenzen für Hochschulen

Das Urteil des LAG Baden-Württemberg zeigt anschaulich und ausführlich, dass emotional geleitete Handlungen in schädigender Absicht gegenüber dem Arbeitgeber zu einer fristlosen Kündigung führen können. Überraschend kommt die Entscheidung nicht, schon 2013 urteilte das LAG Hessen (Urteil vom 5.8.2013, Az.: 7 Sa 1060/10), dass eine fristlose Kündigung wegen einer eigenmächtigen Datenlöschung gerechtfertigt sei.¹ Im vorliegenden Fall geht insbesondere die Annahme des Arbeitnehmers, dass er befugt sei, seinen „digitalen“ Arbeitsplatz ohne Grund zu löschen, fehl – denn grundsätzlich stehen sämtliche berufsbezogen erstellte Dateien dem Arbeitgeber zu. Den Beweis, dass es sich um keine betriebsnotwendigen Dateien handelte, erbrachte der Arbeitnehmer im vorliegenden Fall nicht.

Selbst wenn er sich auf den Grundsatz der Datenminimierung der DSGVO berufen hätte, würde dies nicht zu einem anderen Ergebnis führen. Nach Art. 5 Abs. 1 lit. c DSGVO sind personenbezogene Daten nur so lange zu speichern, wie sie für die Zweckerreichung erforderlich sind. Doch neben der Tatsache, dass es sich im vorliegenden Fall vornehmlich um Geschäftsdaten und keine Daten mit Personenbezug handelte, liegt die Entscheidungsbefugnis, welche Daten wann zu löschen seien, ebenfalls bei dem Arbeitgeber.

Hochschulen und Forschungseinrichtungen ist daher anzuraten, ein umfassendes Datensicherungskonzept auf ihren

¹ Zu diesem Urteil im Detail: Kuta, Rechts-Klick, dann löschen ... und schon ist der Arbeitsplatz weg!, DFN-Infobrief Recht 8/2014.

Servern zu implementieren. Damit kann der Gefahr von vorsätzlichen Datenlöschungen wie im vorliegenden Sachverhalt, aber auch dem Risiko versehentlicher Löschungen begegnet werden. Im Notfall kann so auf die (möglichst aktuellen) Backup-Dateien zurückgegriffen werden, um einen nachhaltigen Schaden weitgehend zu vermeiden. Im Übrigen sollten Zugriffsrechte auf Dateien nur erteilt werden, soweit sie für den Arbeitsablauf notwendig sind.

Diese Beschränkung der Zugriffsrechte und Sicherung der Daten spielt auch aus datenschutzrechtlicher Sicht eine relevante Rolle. Denn soweit sich personenbezogene Daten auf dem Server befinden, kann das unbefugte Löschen dieser Daten einen Eingriff in die Integrität und Vertraulichkeit nach Art. 5 Abs. 1 lit. f DSGVO bedeuten. Danach ist die verantwortliche Hochschule oder Forschungseinrichtung durch die Implementierung technischer und organisatorischer Maßnahmen verpflichtet, die personenbezogenen Daten in einer Weise zu verarbeiten, die eine angemessene Sicherheit der Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung, des unbeabsichtigten Verlusts, der unbeabsichtigten Zerstörung oder der unbeabsichtigten Schädigung.

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

Nachdruck sowie Wiedergabe in elektronischer Form, auch auszugsweise, nur mit schriftlicher Genehmigung des DFN-Vereins und mit vollständiger Quellenangabe.