NEU: Podcast der
Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht DFN

12 / 2022
Dezember 2022

Oh du fröhliche Plattformhaftung!

Zur Haftung von Intermediären für urheberrechtswidrige Inhalte

von Johanna Voget

Kopierte Bilder, Videos und Textpassagen – im Online-Bereich erfolgen urheberrechtliche Verletzungen zuhauf. Die Personen hinter den Nutzernamen und Accounts sind oftmals nur mit hohem Aufwand identifizierbar, eine Beseitigung des Verstoßes oder gar das Erlangen von Schadensersatzzahlungen ist daher unsicher. So stellt sich für die Betroffenen die Frage, wann die Betreiber der Plattformen, auf denen die Rechtsverletzung erfolgt ist - wie Youtube, Facebook (Meta), Tiktok und Co. - in Anspruch genommen werden können. Die Forschungsstelle Recht berichtete bereits in der Vergangenheit zu den verschiedenen Regelungen und Entwicklungen zur Plattformhaftung im Bereich des Urheberrechts.[1] Dieser Beitrag soll nun einen Überblick über die verschiedenen Voraussetzungen der Haftung von Plattformbetreibern verschaffen.

I. Hintergrund

Im Bereich der Haftung von Plattformen für Beiträge ihrer Nutzer, die Urheberrechte Dritter verletzen, hat sich die nationale Rechtsprechung in diesem Jahr wesentlich geändert.
Ausgangspunkt hierfür waren die Entscheidungen des Europäischen Gerichtshofs (EuGH) aus 2021 (Urteil v. 22.6.2021 – C-682/18, Youtube und C-683/18, Cyando). Bis zu diesem Zeitpunkt war, trotz weitgehender Harmonisierung des Urheberrechts, die Beurteilung auf nationaler Ebene nach den Grundsätzen der Störerhaftung erfolgt. Mit seinen Urteilen ebnete der EuGH den Weg nicht nur für eine strengere Ausgestaltung der Haftung, sondern auch für eine verstärkte Möglichkeit der Einflussnahme im Bereich der Plattformhaftung durch die europäische Union. Entscheidende Weichenstellungen für die Beurteilung der Haftung sind die Fragen nach dem Vorliegen einer urheberrechtlich relevanten Verwertungshandlung durch das Bereitstellen einer Plattform und der Ausgestaltung der Verkehrs- bzw. Sorgfaltspflichten der Betreiber derselben.

II. Bisher geltendes Prinzip der Störerhaftung

Grundlage für die Frage nach einer Haftung der Plattformbetreiber ist die Einordnung der Tätigkeit derselben im urheberrechtlichen Sinne. Um in die Haftung genommen zu werden, muss also zunächst eine urheberrechtlich relevante Verwertungshandlung vorgenommen werden, die in die Rechte des Urhebers eingreift. Im Rahmen von Online-Sachverhalten kommt eine öffentliche Wiedergabe gem. § 19a Urheberrechtsgesetz (UrhG), auf europäischer Ebene kodifiziert in Art. 3 Abs. 1 der Richtlinie zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (InfoSoc-RL), in Betracht.
Art. 8 Absatz 3 der InfoSoc-RL normiert diesbezüglich, dass Anordnungen auch gegen Dienstleister beantragt werden können, deren Dienste für eine Verletzung verwendet werden. Die Ausgestaltung der Haftung der Dienstleister nach dieser Vorschrift ist aber ausdrücklich den Mitgliedstaaten überlassen.

1 Siehe Tiessen, Wenn zwei sich freuen, haftet der Dritte, DFN-Infobrief Recht 05/2019; McGrath, Kurzbeitrag: Benutzung auf eigene Gefahr – Betreiber haften für ihre Nutzer!, DFN-Infobrief Recht 07/2022.

Dem trug die bisherige nationale Rechtsprechung und Praxis durch das Prinzip der, in Anlehnung an § 1004 des Bürgerlichen Gesetzbuches (BGB) entwickelten, Störerhaftung Geltung. Danach haftet, wer - ohne Täter oder Teilnehmer zu sein - durch sein Verhalten eine Verletzung ermöglicht, bei der Verletzung von Sorgfaltspflichten, allerdings nicht auf Schadensersatz, sondern nur auf Unterlassung.
Die Ausgestaltung dieser Sorgfaltspflicht knüpft inhaltlich an die Regelung des Art. 14 Absatz 1 E-Commerce-RL (ECRL) an. Diese stellt eine Haftungsprivilegierung für Diensteanbieter dar und normiert in diesem Zuge bestimmte Voraussetzungen, nach deren Erfüllung keine Verantwortlichkeit der Diensteanbieter für die Inhalte bzw. gespeicherten Informationen besteht.
Danach darf der Anbieter zunächst keine tatsächliche Kenntnis von der rechtswidrigen Tätigkeit oder Information haben und sich auch keiner Tatsachen oder Umstände bewusst sein, aus denen die rechtswidrige Tätigkeit oder Information offensichtlich wird. Sobald der Diensteanbieter aber Kenntnis von den rechtswidrigen Inhalten erlangt, muss er unverzüglich tätig werden, um die Information zu entfernen oder den Zugang zu ihr zu sperren. Dieses Verfahren zur Einhaltung der Sorgfaltspflichten wird auch als sog. „notice and take down“ und „notice and stay down“ bezeichnet.

Die Plattformbetreiber nahmen nach diesem Verständnis nicht unmittelbar die Verwertungshandlungen aus § 19a UrhG und Art. 3 Abs. 1 InfoSoc-RL vor, sondern wurden, nach Ausübung der Ausgestaltungsmöglichkeit durch Art. 8 InfoSoc-RL, nur haftbar gemacht, wenn sie durch die Nichteinhaltung von Sorgfaltspflichten eine urheberrechtsverletzende Verwertungshandlung durch einen Dritten ermöglichen.

III. Rechtsprechungsänderung hin zur Täterhaftung

In seinen Entscheidungen aus dem letzten Jahr stellte der EuGH entgegen diesem bisherigen Verständnis fest, dass die Betreiber einer Sharehosting-Plattform, auf der Nutzer geschützte Inhalte rechtswidrig öffentlich zugänglich machen können, zwar grundsätzlich keine „öffentliche Wiedergabe“ dieser Inhalte im Sinne des Art. 3 Abs. 1 InfoSoc-RL vornehmen. Eine solche liege aber dann vor, wenn die Diensteanbieter über die bloße Eröffnung der Plattform hinaus dazu beitragen, der Öffentlichkeit unter Verletzung von Urheberrechten Zugang zu solchen Inhalten zu verschaffen. Dies soll zunächst dann der Fall sein, wenn der Betreiber von der rechtsverletzenden Zugänglichmachung eines geschützten Inhalts auf seiner Plattform konkret Kenntnis hat und diesen Inhalt nicht unverzüglich löscht oder den Zugang zu ihm sperrt. Darüber hinaus ist ein solcher Fall gegeben, wenn der Plattformbetreiber weiß oder wissen müsste, dass über seine Plattform im Allgemeinen geschützte Inhalte rechtswidrig öffentlich zugänglich gemacht werden und er nicht die geeigneten technischen Maßnahmen ergreift, die von einem die übliche Sorgfalt beachtenden Wirtschaftsteilnehmer in seiner Situation erwartet werden können, um Urheberrechtsverletzungen auf dieser Plattform glaubwürdig und wirksam zu bekämpfen. Zuletzt nimmt der Dienstanbieter selbst eine öffentliche Wiedergabe vor, wenn er an der Auswahl geschützter Inhalte, die rechtswidrig öffentlich zugänglich gemacht werden, beteiligt ist, auf seiner Plattform Hilfsmittel anbietet, die speziell zum unerlaubten Teilen solcher Inhalte bestimmt sind, oder ein solches Teilen wissentlich fördert. Hierfür kann der Umstand sprechen, dass der Betreiber ein Geschäftsmodell gewählt hat, das die Nutzer seiner Plattform dazu verleitet, geschützte Inhalte auf dieser Plattform rechtswidrig öffentlich zugänglich zu machen.

Nach der Auffassung der europäischen Richter ist der Dienstanbieter also nunmehr unmittelbar nach Art. 3 Absatz 1 InfoSoc-RL verantwortlich, wenn er die in Art. 14 Absatz 1 ECRL angelegten Pflichten verletzt. Eine solche Einordnung der Tätigkeit des Plattformbetreibers als unmittelbare Verwertungshandlung der öffentlichen Zugänglichmachung, entspricht im nationalen Haftungsmodell einer täterschaftlichen Haftung auf Grund einer Verkehrspflichtverletzung. Der EuGH leitet mit anderen Worten aus Art. 3 Absatz 1 InfoSoc-RL Verkehrspflichten ab, deren Verletzung - nicht wie in der bisherigen nationalen Praxis - eine Haftung als Störer, sondern eine täterschaftliche Haftung begründen.

Das wirft die Frage auf: Welche praktischen Auswirkungen zeitigt diese Entscheidung? Durch das Urteil Youtube II (Urteil v. 02.06.2022 - I ZR 140/15), dessen Verfahren eines Musikproduzenten gegen die Youtube LLC und die Google LLC, als alleinige Gesellschafterin von Youtube, den Ausgangspunkt der EuGH Entscheidungen im Wege eines Vorlageverfahrens gebildet hatte, hat der BGH die Entscheidung der europäischen Richter in die nationale Praxis umgesetzt. Das Prinzip der Störerhaftung wurde aufgehoben, an seine Stelle tritt die Haftung der Plattformen als Täter. Herauszustellen ist hierzu jedoch, dass der maßgebliche Anknüpfungspunkt der Intermediärshaftung letztlich unverändert bleibt. Die Plattformbetreiber haften weiterhin nur, wenn sie zumutbare Sorgfaltspflichten verletzen. Folglich müssen

sie grundsätzlich erst dann reagieren, wenn sie in hinreichend deutlicher Form auf eine Rechtsverletzung hingewiesen wurden. Der Rechtsverstoß muss für die Plattformen ohne eingehende tatsächliche und rechtliche Prüfung aufgrund des Hinweises erkennbar sein. Dann erst trifft sie die Pflicht, den verletzenden Inhalt zu löschen und weitere Vorkehrungen gegen gleichartige Verletzungen zu treffen.
Die Folgen bei einer Verletzung dieser Verkehrspflichten sind von nun an aber gewichtiger. Durch die Einstufung als Täter, die unmittelbar die verletzende Verwertungshandlung vornehmen, haften Plattformbetreiber nunmehr eben auch auf Schadensersatz und nicht nur auf Beseitigung des Verstoßes und Unterlassung eines solchen.

Zu bemerken ist an dieser Stelle außerdem, dass der EuGH seine Einflussnahme auf die Einordnung der Haftung der Plattformbetreiber erweitert: Während vorher den Mitgliedstaaten die Ausgestaltung der Haftung überlassen war, unterfällt diese nach den Feststellungen des EuGH nun direkt dem Tatbestand der öffentlichen Wiedergabe nach Art. 3 InfoSoc RL und somit den vom EuGH aufgestellten Voraussetzungen und Auslegungsgrundsätzen. Die Eröffnung der Gestaltungsmöglichkeit des Art. 8 InfoSo-RL kommt in diesem Fall also nicht mehr zum Zuge.

IV. Verhältnis der Entscheidungen zu der Haftung nach Art. 17 DSM RL

Inzwischen wurde die Plattformhaftung im Urheberrecht durch Art. 17 der Richtlinie über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt (DSM RL) speziell geregelt.[2] Dieser sieht in Abs. 4 Buchstabe b und c vor, dass Diensteanbieter hochgeladene Inhalte zuvor auf Verstöße gegen das Urheberrecht überprüfen müssen, um sich nicht selbst für diese haftbar zu machen.
Kern der Proteste gegen und Diskussionen um die neuen Haftungsregelungen stellen die technischen Maßnahmen zur Umsetzung dieser Vorab-Kontrolle, die sog. Uploadfilter, dar: Hierunter werden automatisierte Computerprogramme verstanden, die Daten vor deren Veröffentlichung oder Hochladen nach dezidierten Kriterien kontrollieren und sortieren. Auch Art. 17 DSM RL führt keine allgemeine Pflicht aller Plattformbetreiber zur Vorabkontrolle der hochgeladenen Inhalte ein. Es muss vielmehr berücksichtigt werden, ob der Diensteanbieter alle Maßnahmen ergriffen hat, die ein sorgfältiger Betreiber ergreifen würde, um sicherzustellen, dass auf seiner Website keine nicht genehmigten Werke oder sonstige Schutzgegenstände verfügbar sind, wobei auch bewährte Verfahren in der Branche, die Wirksamkeit der unternommenen Schritte vor dem Hintergrund aller einschlägigen Faktoren und Entwicklungen und der Grundsatz der Verhältnismäßigkeit beachtet werden müssen.
Im Frühjahr dieses Jahres entschieden die europäischen Richter, dass die Regelung des Art. 17 DSM RL nicht gegen die europäischen Grundrechte auf freie Meinungsäußerung und Informationsfreiheit aus Art. 11 EU-Grundrechte-Charta (GRCh) verstößt und somit europarechtskonform ist.[3]

Die dargestellten EuGH-Entscheidungen zur Täterhaftung von Plattformbetreibern und das hierauf basierende nationale Urteil betreffen noch die Rechtslage vor Inkrafttreten dieser Regelung. Gleichwohl haben die Feststellungen des EuGH Auswirkungen auf das nationale Haftungssystem für mittelbare Verletzungshandlungen im Urheberrecht. Denn die hier aufgestellten Grundsätze bleiben auch weiterhin für Fälle der Plattformhaftung relevant, die nicht von dem seit dem 01.08.2021 geltenden Urheberrechts-Diensteanbieter-Gesetz (UrhDaG), welches die DSM RL auf nationaler Ebene umsetzt, erfasst werden. Während Youtube das Paradebeispiel für den Diensteanbieter iSd § 2 UrhDaG ist, ist die Anwendung auf viele andere Plattformen, die nicht so eine große Reichweite haben, nicht vorgesehen.

V. Bedeutung für Hochschulen und wissenschaftliche Einrichtungen

Auch für Hochschulen und wissenschaftliche Einrichtungen ist die Thematik der Haftung von Plattformbetreibern für urheberrechtliche Verletzungen von Belang. Zum einen betreiben wissenschaftliche Einrichtungen zum Teil selbst Plattformen, auf denen Inhalte hochgeladen werden können, sodass die Frage nach einer möglichen Haftung und Verpflichtung zur Kontrollen der Inhalte oder Implementierung technischer Maßnahmen zur Verhinderung des Uploads rechtswidrigen Contents von unmittelbarer Relevanz ist. Zum anderen ist die Rechtsprechung

2 Siehe Gielen, First Rule: Do not talk about Uplaodfilter, DFN-Infobrief Recht 01/2020; Rennert, Habemus Reform, DFN-Infobrief 07/2022; Schaller, Alea iacta est: Uploadfilter bleiben, DFN-Infobrief Recht 08/2022.

von Interesse für den Einzelnen, also auch die Mitarbeiter von Hochschulen und wissenschaftlichen Einrichtungen selbst, die ihr Gedankengut, ihre geistigen Schöpfungen, vor rechtswidriger Verbreitung im Online-Bereich schützen wollen und gegen Verletzungen durch Dritte auf Online-Plattformen vorgehen wollen. Letztlich bleibt die Entscheidung des OLG Hamburg, das nach der Revisionsentscheidung des BGH in Sachen Youtube II erneut zu entscheiden hat, hinsichtlich der konkreten Umsetzung und Ausgestaltung der neuen Täterhaftung im Einzelfall abzuwarten.

Morgen Kinder werden wir klagen

Eine Übersicht zu datenschutzrechtlichen Schadensersatzansprüchen

von Johannes Müller

Die Datenschutzgrundverordnung (DSGVO) sieht das Recht vor, dass Betroffene von Datenschutzverstößen von den Datenverarbeitern Schadensersatz verlangen können. Solche Ansprüche können nicht nur bei der Entstehung von materiellen, sondern auch immateriellen Schäden geltend gemacht werden. Die Voraussetzungen für das Entstehen immaterieller Schäden sind nicht abschließend geklärt und weisen eine enorme Relevanz in der Praxis auf.

I. Das duale Sanktionssystem der DSGVO

Die DSGVO sieht zwei mögliche Wege vor, um Verstöße gegen Datenschutzvorschriften zu sanktionieren. Einerseits kann eine Ahndung durch die zuständige Aufsichtsbehörde erfolgen. Diese kann gemäß Art. 58 Abs. 2 DSGVO Verantwortliche, die Datenschutzverstöße begehen, verwarnen und anweisen, Daten zukünftig datenschutzkonform zu verarbeiten. Neben dieser milden Variante steht der Datenschutzbehörde gemäß Art. 83 DSGVO auch die Möglichkeit zu, Bußgelder gegen Datenschutzverstöße zu verhängen. Diese können gemäß Art. 83 Abs. 4 DSGVO bei einer rechtswidrigen Datenverarbeitung bei bis zu 20 Millionen Euro oder 4 Prozent des Jahresumsatzes liegen, sofern dieser höher ist.[1] Diese Sanktionsmöglichkeit erfolgt ausschließlich durch die öffentliche Hand in Form der jeweiligen Datenschutzaufsichtsbehörde.

Andererseits können Datenschutzverstöße auch durch Schadensersatzansprüche von betroffenen Personen verfolgt werden. Art. 82 DSGVO sieht vor, dass jeder Person, der durch einen Verstoß gegen die DSGVO ein Schaden entstanden ist, einen Anspruch auf Schadensersatz gegen den Verantwortlichen oder Auftragsverarbeiter zusteht. Anders als die Sanktionsmöglichkeit der Bußgeldverhängung durch die Aufsichtsbehörde kann jede natürliche Person, die Opfer eines Datenschutzverstoßes geworden ist, von einem möglichen Schadensersatzanspruch Gebrauch machen. Damit kommt diesem potentiell eine deutlich weitreichendere Wirkung zu, da die Ahndung einerseits nicht davon abhängt, ob die Aufsichtsbehörde sich zum Einschreiten entscheidet und andererseits bei Datenschutzverstößen, die eine Vielzahl von Personen betreffen, auch eine hohe Anzahl von Klägern in Betracht kommt.

II. Die Systematik des datenschutzrechtlichen Schadensersatzanspruches

Art. 82 Abs. 1 DSGVO besagt, dass jede Person, der wegen eines Verstoßes gegen die Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen oder den Auftragsverarbeiter hat. Auch wenn der Wortlaut von jeder Person spricht, sollen lediglich natürliche und nicht auch juristische Personen wie etwa Unternehmen vom Anspruch Gebrauch machen können, da die DSGVO gerade dem Schutz personenbezogener Daten von natürlichen Personen dient. Erforderlich für eine Haftung ist, dass der Verantwortliche Beteiligter am rechtswidrigen Datenverarbeitungsvorgang gewesen ist. Erfolgt die Verarbeitung von Daten nicht durch eine Einrichtung selbst, aber im Auftrag einer Einrichtung, die die relevanten Entscheidungen zur Datenverarbeitung trifft, liegt ein Fall der Auftragsverarbeitung vor. In einem solchen Fall kann grundsätzlich sowohl der Verantwortliche (Auftraggeber) als auch der Auftragsverarbeiter

1 Der Europäische Datenschutzausschuss hat unter folgendem Link Leitlinien zur Berechnung von Bußgeldern veröffentlicht: https://edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf (zuletzt abgerufen am 23.11.2022); vgl. hierzu auch Müller, Bußgeldberechnung für Dummies, DFN-Infobrief Recht 10/2022.

für eine rechtswidrige Datenverarbeitung haften. Hierbei wird jedoch der Auftragsverarbeiter durch Art. 82 Abs. 2 S. 2 DSGVO privilegiert. Er soll lediglich dann haften, wenn er spezielle, für den Auftragsverarbeiter bestehende, Pflichten verletzt oder eine Weisung missachtet, die ihm rechtmäßig vom Verantwortlichen erteilt wurde.

Trotz Verletzung von datenschutzrechtlichen Vorschriften ist ein Schadensersatzanspruch gemäß Art. 82 Abs. 3 DSGVO ausgeschlossen, sofern der Verantwortliche oder der Auftragsverarbeiter nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. „Verantwortlich" meint im Rahmen von Art. 82 DSGVO das Vorliegen von Verschulden. Ist die Einrichtung, die die Datenverarbeitung durchgeführt hat, imstande nachzuweisen, dass sie weder vorsätzlich noch fahrlässig den Schaden herbeigeführt hat, ist sie nicht zum Schadensersatz verpflichtet. Der Schadensersatzanspruch ist folglich verschuldensabhängig. Das Verschulden wird jedoch vermutet, sodass im Falle eines Schadens durch einen Datenschutzverstoß der Anspruch nur dann ausgeschlossen wird, sofern der Datenverarbeiter aktiv nachweist, dass ihm kein Verschulden zur Last fällt.

III. Ersatz von materiellen und immateriellen Schäden

Schadensersatzansprüche dienen, wie bereits der Begriff erkennen lässt, dazu entstandene Schäden interessensgerecht zu kompensieren. Der Schadensersatzanspruch des Art. 82 DSGVO zeichnet sich durch die Besonderheit aus, dass nicht nur materielle, sondern auch immaterielle Schäden ersetzt werden sollen. Die Entstehung materieller Schäden ist greifbar. Denkbar ist in etwa, dass eine Versicherung unter Verstoß gegen Datenschutzbestimmungen Kenntnis von den persönlichen Umständen eines Versicherungsnehmers erlangt und dieser deshalb eine höhere Versicherungsprämie zu zahlen hat. In einem solchen Fall entstünde ein materieller Schaden in Höhe der Differenz der erhöhten Versicherungsprämie und der normalen Versicherungsprämie, die ohne den Datenschutzverstoß zu entrichten gewesen wäre.

Deutlich schwieriger zu fassen sind jedoch mögliche immaterielle entstandene Schäden. Das deutsche Zivilrecht kennt nur in wenigen Fällen die Möglichkeit immaterielle Schäden zu ersetzen, etwa bei der Zufügung körperlicher Schmerzen (Schmerzensgeld) gemäß § 253 Abs. 2 BGB oder bei schwerwiegenden Persönlichkeitsverletzungen. Dieser restriktive Maßstab gilt jedoch nicht für das europäische Datenschutzrecht. Unter welchen Voraussetzungen hier immaterielle Schäden zu ersetzen sind, ist nicht abschließend geklärt und wird sehr unterschiedlich beurteilt. Teilweise wird angenommen, dass ein immaterieller Schaden bereits bei einem unguten Gefühl vorliegen kann, dass bei einer betroffenen Person durch eine rechtswidrige Datenverarbeitung hervorgerufen wird.[2] Folgt man dieser Linie würde dies dazu führen, dass nahezu jede Verarbeitung personenbezogener Daten, die nicht im Einklang mit den Bestimmungen des Datenschutzrechts steht, zu Schadensersatzansprüchen führen wird. Hierdurch würde der datenschutzrechtliche Schadensersatzanspruch die Funktion erhalten, nicht ausschließlich der Kompensation entstandener Schäden zu dienen, sondern auch gleichzeitig Verantwortliche für die Verletzung von Datenschutzvorschriften zu bestrafen und hierdurch auch präventiv vor zukünftigen Datenschutzverletzungen abzuschrecken. Ein solches Verständnis von einem strafenden Charakter des Schadensersatzes liegt dem deutschen Zivilrecht grundsätzlich fern. Auf datenschutzrechtlicher europäischer Ebene, auf der die deutschen zivilrechtlichen Grundsätze wenig Wirkung entfalten, ist er hingegen denkbar. So spricht auch Erwägungsgrund 146 S. 3 der DSGVO davon, dass der Begriff des Schadens weit zu verstehen ist und so ausgelegt werden muss, dass er den Zielen der Verordnung (dem umfassenden Schutz personenbezogener Daten) in vollem Umfang entspricht.

Dieses weite Verständnis von immateriellen Schäden ist jedoch nicht unbestritten. So wird auch in der Wissenschaft teilweise für datenschutzrechtliche Schadensersatzansprüche eine spürbare Persönlichkeitsverletzung gefordert.[3] Hiernach soll nicht jeder Bagatellverstoß zu Schadensersatzansprüchen führen können.

Neben der Fragestellung, ob erst bei einer bestimmten Erheblichkeit ein ersetzbarer immaterieller Schaden entstehen soll, besteht auch Unklarheit bei der Frage, wie genau der entstandene immaterielle Schaden berechnet werden soll. Anders als beim materiellen Schaden hat eine konkrete Vermögenseinbuße nicht stattgefunden. Denkbar wäre, dass einige der Kriterien des Art. 83 Abs. 2 DSGVO, welche die Aufsichtsbehörden bei der Berechnung einer Bußgeldhöhe zu berücksichtigen haben,

2 So etwa Kühling/Buchner/Bergt, Datenschutzgrundverordnung BDSG Kommentar, Art. 82 DSGVO Rn. 18a f.

3 So etwa Franzen/Gallner/Oetker, Kommentar zum europäischen Arbeitsrecht, Art. 82 DSGVO Rn. 22.

auch für die Ermittlung der Höhe des immateriellen Schadens herangezogen werden können. Hiernach könnten etwa die Art, Schwere und Dauer des Verstoßes und auch die Kategorie der betroffenen personenbezogenen Daten zu berücksichtigen sein. Denkbar ist, dass sich in der Zukunft in der Rechtspraxis bestimmte Fallgruppen bilden, für die jeweils bestimmte pauschale Schadensersatzansprüche gelten sollen. Solche Fallgruppen sind etwa bei Urheberrechtsverletzungen üblich.

IV. Rechtsprechung zu immateriellen Schadensersatzansprüchen

Auch in der gerichtlichen Praxis kommt es zu Unterschieden bei der Bewertung von immateriellen Schadensersatzansprüchen. Überwiegend wird hier eine enge Sicht verfolgt, die den Klägern nicht für jegliche Unannehmlichkeiten infolge von Datenschutzverstößen einen Schadensersatzanspruch zusprechen will. So verlangt zwar etwa das Oberlandesgericht Brandenburg in seiner Entscheidung vom 21.06.2021 (AZ 1 U 69/20) keine schwerwiegende Persönlichkeitsverletzung, es betont aber, dass ein tatsächlich entstandener (auch immaterieller) Schaden darzulegen ist. Folglich möchte es nicht allein jeder rechtswidrigen Datenverarbeitung einen Schadensersatzanspruch folgen lassen. In dem Beschluss musste das Oberlandesgericht unter anderem darüber entscheiden, ob die unzulässige Nutzung des Fotos und des Namens einer Person auf einer Webseite zu datenschutzrechtlichen Schadensersatzansprüchen führt.
Ebenso verlangt auch das Oberlandesgericht Bonn in seiner Entscheidung vom 01.07.2021 (AZ 15 O 372/20), dass es für einen Schadensersatzanspruch zu einer spürbaren Beeinträchtigung gekommen sein müsste. Auch das Landgericht Hamburg forderte am 04.09.2020 (AZ 324 S 9/19), dass es zu einer tatsächlichen Persönlichkeitsverletzung gekommen sein muss, die etwa in einer Bloßstellung liegen kann.

Von einer solchen engen Auffassung weichen jedoch auch Gerichte ab. Auffallend ist, dass gerade Arbeitsgerichte großzügiger einen entstandenen immateriellen Schaden annehmen. So hat das Landesarbeitsgericht Baden-Württemberg in seiner Entscheidung vom 25.02.2021 (AZ 17 Sa 37/20) dargestellt, dass bereits in einem unguten Gefühl, dass die eigenen Daten Unbefugten bekannt wurden und auch ohne Erlaubnis weiterverwendet werden könnten, ein immaterieller Schaden zu sehen ist. Der Entscheidung lag die Frage zugrunde, ob die Übermittlung von Beschäftigtendaten in die USA zu Schadensersatzansprüchen führen kann. Zwar lehnte das Landesarbeitsgericht Baden-Württemberg im konkreten Fall einen Schadensersatzanspruch ab, da die Datenübermittlung in die USA selbst rechtmäßig erfolgte. Das Gericht wies dennoch in der Entscheidung auf sein weites Verständnis des immateriellen Schadensbegriffs hin.
Auch das Landesarbeitsgericht Niedersachsen wies in seinem Urteil vom 22.10.2021 (AZ 16 SA 761/20) darauf hin, dass das Überschreiten einer Erheblichkeitsschwelle nicht erforderlich sei, um einen immateriellen Schaden anzunehmen.

Eine rechtssichere Klärung der Frage, unter welchen Voraussetzungen ein immaterieller Schadensersatzanspruch angenommen werden kann, wird erst erfolgen, wenn der Europäische Gerichtshof (EuGH) hierzu entscheidet. Diesem obliegt die verbindliche Auslegung der Vorschriften des Unionsrechts, zu denen auch die DSGVO zählt. Diese Auslegung müssen auch die nationalen Gerichte zwingend berücksichtigen. Besteht Ungewissheit, wie Unionsrecht auszulegen ist, so sind die nationalen (in der jeweiligen Rechtssache höchstinstanzlichen) Gerichte dazu verpflichten, dem EuGH die Auslegungsfrage vorzulegen und dessen Entscheidung abzuwarten. Gegen diese Pflicht hat nach Auffassung des Bundesverfassungsgerichts das Amtsgericht Goslar in seiner Entscheidung vom 27.09.2019 (AZ 28 C 7/19) verstoßen, indem es pauschal davon ausging, erst bei Überschreiten einer Erheblichkeitsschwelle könne ein immaterieller Schaden angenommen werden und diese Frage nicht dem EuGH vorlegte.[4] Momentan liegen mehrere Vorlagefragen dem EuGH vor, in denen nationale Gerichte den EuGH angerufen haben, damit dieser verbindlich entscheidet, welche Voraussetzungen für den Ersatz von immateriellen Schäden gelten.[5] Ebenso hat der EuGH zu entscheiden, anhand welcher Kriterien der entstandene immaterielle Schaden zu berechnen ist. Die diesbezüglichen Entscheidungen sind mit Spannung zu erwarten.

V. Relevanz für Hochschulen

Das datenschutzrechtliche Schadensersatzrecht weist eine enorme Relevanz für Hochschulen auf. Während von der Sanktionsmöglichkeit der Bußgeldverhängung öffentliche Universitäten

4 Hierzu auch Voget, Work Data Balance: Der Beschäftigtendatenschutz, DFN-Infobrief Recht 11/2022.

5 BAG, BeckRS 2021, 29622; OGH Österreich, ZD 2021, 631; LG Saarbrücken, ZD 2022, 162.

als Körperschaften des öffentlichen Rechts grundsätzlich befreit sind und lediglich private Hochschulen und wissenschaftliche Einrichtungen Adressaten von Bußgeldern sein können,[6] können sämtliche Einrichtungen Gegner eines Schadensersatzanspruchs sein. Begehen Universitäten Datenschutzverstöße, von deren Folgen Individuen betroffen sind, besteht in der Folge das Risiko, dass diese von ihnen Schadensersatz verlangen. Im Rahmen von materiellen Schäden kann in der Regel leicht festgestellt werden, in welcher konkreten Höhe Schadensersatz zu leisten ist. Deutlich schwieriger ist die Frage zu beantworten, ob immaterielle Schäden durch einen Datenschutzverstoß entstanden sind. Folgt man hierbei einem sehr weiten Verständnis eines immateriellen Schadensbegriffs kann in jeder gefühlten Unannehmlichkeit ein Schaden gesehen werden. Dieses Verständnis würde dazu führen, dass nahezu jeder Datenschutzverstoß auch einen Schadensersatzanspruch zur Folge haben könnte. Hiernach könnten nahezu alle Datenschutzverstöße durch Universitäten nicht nur Reputationsprobleme, sondern vor allem auch negative finanzielle Folgen mit sich bringen. Aus der Perspektive von Universitäten, die potentiell Datenschutzverstöße begehen könnten, wäre folglich ein engeres Verständnis des immateriellen Schadens wünschenswert, bei dem etwa erst eine Persönlichkeitsverletzung zur Annahme eines ersetzbaren Schadens führen wird. Eine verbindliche Klärung dieser Frage wird erst durch Entscheidungen des EuGHs erfolgen, die dann auch eine hohe Relevanz für Hochschulen aufweisen werden.

6 Uphues, Kuschelkurs hat ausgedient, DFN-Infobrief Recht 04/2019; John, Unus pro omnibus, omnes pro uno, DFN-Infobrief Recht 05/2022; Müller, Bußgeldberechnung für Dummies, DFN-Infobrief Recht 10/2022.

Geschenke bringt das Oberlandesgericht?

Das Oberlandesgericht Karlsruhe lässt die Verwendung von Diensten von US-amerikanischen Tochterfirmen zu

von Nicolas John

Die Nachwirkungen des „Schrems-II"-Urteils des Gerichtshofs der Europäischen Union (EuGH) dauern nach wie vor an. Nicht nur Unternehmen haben täglich mit der datenschutzkonformen Verarbeitung personenbezogener Daten zu kämpfen, auch öffentliche Einrichtungen müssen im Prozess der Digitalisierung viele Abwägungen hinsichtlich des Datenschutzes treffen. Die richtige Auswahl der Software steht da nur am Beginn dieses Prozesses und ist sorgfältig vorzunehmen. Das Angebot der Hersteller ist aber meist überschaubar und einige von ihnen versprechen ausdrücklich, die Daten DSGVO-konform zu verarbeiten. Der Griff zu einem dieser großen Anbietenden erscheint daher logisch. Das Oberlandesgericht (OLG) Karlsruhe hat hier nun für ein wenig Klarheit gesorgt.

I. Hintergrund

Die Digitalisierung in Unternehmen und öffentlichen Einrichtungen wird schon bei der Auswahl der Software von der datenschutzkonformen Verarbeitung personenbezogener Daten dominiert. Neben den entsprechenden Funktionalitäten muss sichergestellt sein, dass die Datenverarbeitungen auf den Servern der Anbietenden den Bestimmungen der Datenschutz-Grundverordnung (DSGVO) entsprechen.

Probleme bereiten insbesondere Softwarelösungen, welche Datenexporte in EU-Drittstaaten vornehmen, wie z.B. in die Vereinigten Staaten (USA). Der EuGH hat mit seinem „Schrems-II"-Urteil hierzu klar Stellung bezogen und das für die Exporte erforderliche EU-US-Privacy-Shield für ungültig erklärt.[1] Grund für diese Entscheidung sind die Befugnisse der US-amerikanischen Ermittlungsbehörden, welche auf die personenbezogenen Daten zugreifen dürfen, ohne dass betroffene Europäer:innen hiergegen ein wirksames Rechtsmittel einlegen könnten. Datenexporte können seither nicht mehr vereinfacht auf Grundlage des nunmehr ungültigen Privacy-Shields in die USA vorgenommen werden.

Der EuGH lässt aber weiterhin die Verwendung sog. Standarddatenschutzklauseln zu, welche zwischen den verarbeitenden Parteien vereinbart werden müssen.[2] Allerdings hebt er dabei hervor, dass Datenexporte unter Verwendung der Standarddatenschutzklauseln nur dann rechtmäßig sein können, wenn sichergestellt ist, dass US-amerikanischen Behörden keinen Zugriff auf die Daten vornehmen können. Ein Mittel hierfür kann z.B. eine verschlüsselte Ablage der personenbezogenen Daten auf den Servern des Softwareanbietenden sein, bei der nur der Verantwortliche den Schlüssel innehält.

Eine andere (und wohl in der Praxis zu präferierende) Lösung kann die ausschließliche Verarbeitung der personenbezogenen Daten auf europäischen Servern sein. Doch die meisten großen Softwareanbietenden kommen aus den USA. Damit bei der Nutzung ihrer Softwarelösungen aber keine Daten in die USA exportiert werden müssen, werden Tochtergesellschaften mit Sitz in der der Europäischen Union (EU) für die Datenverarbeitung eingesetzt. Auf diese Weise können die Anbietenden versprechen, dass keine personenbezogenen Daten in die USA übermittelt werden und die Verarbeitung im Einklang der Vorgaben der

1 Siehe hierzu: Uphues, Ins Wasser gefallen, DFN-Infobrief Recht 8/2020.

2 Siehe hierzu: Wellmann, O ihr gnadenbringenden Datenschutzklauseln, DFN-Infobrief Recht 12/2020; Tiessen, Santa Claus(e) is coming early, DFN-Infobrief Recht 8/2021; John, New Schrems, new Me(crosoft), DFN-Infobrief Recht 2/2022.

DSGVO geschehe. Auch im vorliegenden Sachverhalt hat das anbietende Unternehmen auf eine solche Lösung gesetzt.

II. Sachverhalt

Auf der Suche nach einer digitalen Lösung für das Entlassmanagement ihrer Patient:innen schrieben zwei kommunale Krankenhäuser ein Vergabeverfahren für eine entsprechende Software aus. Als Teil der Ausschreibung war neben bestimmten Kosten unter anderem auch die Erfüllung der Anforderungen der DSGVO und des Bundesdatenschutzgesetzes (BDSG) an die Verarbeitung der personenbezogenen Daten der Patient:innen gefordert.

Auf die Ausschreibung übermittelten mehrere Dienstleisterinnen Angebote ihrer jeweiligen Softwarelösungen. Eine dieser Anbieterinnen übermittelte ein Angebot, welches den Krankenhäusern zusicherte, dass die personenbezogenen Daten ausschließlich von einem luxemburgischen Tochterunternehmen eines US-amerikanischen Konzerns verarbeitet würden. Diese Zusicherung fand durch die Einbeziehung entsprechender vertraglicher Unterlagen statt, einem „GDPR Data Processing Addendum“ und einem „Supplementary Addendum“. Darüber hinaus umfasste die Zusicherung auch die Tatsache, dass der für die Verarbeitung benötigte Server nach der Angebotsbeschreibung in Frankfurt/Main stehen würde und von einer deutschen GmbH betrieben werden. Die anfallenden personenbezogenen Daten würden allein auf diesem Server gespeichert werden.

Weil dieses Angebot aus Sicht der Krankenhausgesellschaften das wirtschaftlichste war, gaben sie im Rahmen des Vergabeverfahrens bekannt, dass darauf der Zuschlag erteilt werden solle.

III. Beschluss der VK Baden-Württemberg

Aufgrund dieser Ankündigung stellte eine konkurrierende Bewerberin einen Nachprüfungsantrag bei der Vergabekammer (VK) Baden-Württemberg. Diese entschied mit Beschluss vom 16. Juli 2022 (Az.: 1 VK 23/22), dass die von den Krankenhausgesellschaften ausgewählte Dienstleisterin von dem Verfahren auszuschließen sei. Die Entscheidung begründete sie mit dem Einsatz des luxemburgischen Tochterunternehmens für die Datenverarbeitungen. Da sie die Tochter eines US-amerikanischen Unternehmens sei, ist die Nutzung der Dienste ohne eine unzulässige Übermittlung der Daten in ein Drittland, also den USA, nicht möglich. Ob diese Datenübermittlung tatsächlich stattfinde, müsse nach Auffassung der VK Baden-Württemberg nicht konkret festgestellt werden. Es reiche bereits das „latente Risiko eines Zugriffs“ durch staatliche oder private Stellen außerhalb der EU aus, um eine datenschutzrechtlich unzulässige Übermittlung zu bejahen.[3] Daran ändere auch der physische Standort des Servers nichts.

Der Einsatz verstoße daher gegen die DSGVO und halte die Vergabeanforderungen nicht ein – die Anbieterin sei daher aus dem Verfahren auszuschließen.

IV. Beschluss des OLG Karlsruhe

Aufgrund der gegen die Entscheidung der VK Baden-Württemberg eingelegten Beschwerde musste sich nun das OLG Karlsruhe mit der Thematik beschäftigen.[4] Dieses bewertete den Sachverhalt nun anders.

Das OLG ist der Auffassung, dass der Einsatz eines Tochterunternehmens eines US-amerikanischen Konzerns nicht automatisch bedeute, dass der Einsatz nicht DSGVO-konform sei. Soweit die bietende Dienstleisterin ein Angebot abgibt, welches die datenschutzkonforme Verarbeitung zusichert, dürfe von den öffentlichen Auftraggebenden davon ausgegangen werden, dass sie ihre vertraglichen Zusagen erfülle. Die Datenschutzkonformität der Verarbeitung personenbezogener Daten dürfe nur angezweifelt werden, wenn sich konkrete Anhaltspunkte hierzu ergeben.

Aus dem vorliegenden Sachverhalt hätten sich diese Zweifel nicht ergeben können. Denn die anbietende Dienstleisterin machte nachweislich eindeutige Zusicherungen, dass die Verträge die Verarbeitung der personenbezogenen Daten der Patient:innen ausschließlich von der luxemburgischen Tochter zulassen. Zudem dürfen die Daten nur auf deutschen Servern verarbeitet werden. Diese Verarbeitungen hielten die Vorgaben der DSGVO ein. Dass das Angebot in der Praxis auch eingehalten wird, durften die

3 VK Baden-Württemberg, Beschl. v. 13.07.2022, Az.: 1 VK 23/22, Rn. 79.

4 OLG Karlsruhe, Beschl. v. 07.09.2022, Az.: 15 Verg 8/22.

Krankenhausgesellschaften auch annehmen, entgegenstehende konkrete Anhaltspunkte seien nicht ersichtlich. Das OLG macht in seinem Beschluss deutlich, dass die Krankenhausgesellschaften *„nicht davon ausgehen [mussten], dass es aufgrund der Konzernbindung zu rechts- und vertragswidrigen Weisungen an das Tochterunternehmen kommen wird bzw. das europäische Tochterunternehmen durch seine Geschäftsführer gesetzeswidrigen Anweisungen der US-amerikanischen Muttergesellschaft Folge leisten wird."*

Aufgrund dieser Feststellung entspräche das Angebot, welchem die Krankenhausgesellschaften den Zuschlag erteilen wollten, den Vorgaben aus der Ausschreibung. Die Anforderungen an Datenschutz und IT-Sicherheit würden entsprechend gewahrt, es liege nach Ansicht des OLG Karlsruhe kein Grund vor, das Angebot aus dem Verfahren auszuschließen.

V. Bedeutung des Beschlusses

Auf den ersten Blick vermag der Beschluss des OLG Karlsruhe nur eine Streitigkeit im Vergaberecht klären. Doch die Ausführungen zu den Anforderungen des Datenschutzes an Software haben weitreichende Konsequenzen. Denn entkoppelt man diesen Fall nun von der Vergabestreitigkeit und der Thematik um Krankenhaussoftware und abstrahiert ihn auf die generelle Verwendung von Software durch öffentliche Einrichtungen, dann ist die Entscheidung des OLG auch für die Auswahl von z.B. Videokonferenzsoftware von Bedeutung.

Im Kern statuiert das OLG Karlsruhe, dass sich öffentliche Auftraggeber darauf verlassen dürfen, dass das vertraglich zugesicherte, datenschutzkonforme Angebot eines (Software-)Dienstleisters auch in der Praxis eingehalten wird.

Wichtig ist bei dieser Thematik nun die Unterscheidung zwischen dem Ausschluss einer Software aus der Auswahlentscheidung und der tatsächlichen Unterbindung der Verwendung der Software. Denn folgt man nun der Auffassung des OLG Karlsruhe, dürfen die Verantwortlichen zumindest auf Zusicherungen der datenschutzkonformen Verarbeitung personenbezogener Daten der Softwareanbietenden vertrauen. Die Entscheidung des OLGs könnte daher den Weg für die Anwendung US-amerikanischer Software wieder etwas ebnen. Die pauschale Behauptung, dass eine US-amerikanische Software aufgrund einer Befürchtung des Datenexportes trotz entgegenstehender Zusagen nicht nutzbar sei, reicht demnach nicht aus.

Davon abzugrenzen ist jedoch der Umstand, wenn konkrete Anhaltspunkte für mögliche Verstöße gegen die Datenschutzvorgaben festgestellt werden. Dann ist auch nach Auffassung des OLG Karlsruhe den Anhaltspunkten nachzugehen und eine mögliche rechtswidrige Verwendung der Software umgehend zu unterbinden.

VI. Auswirkungen auf Hochschulen und Forschungseinrichtungen

Auch Hochschulen sehen sich regelmäßig mit der Auswahl der richtigen Software konfrontiert.[5] Auch wenn der Beschluss des OLG Karlsruhe mit Sicherheit noch nicht das letzte Wort in dieser Thematik sein wird, gibt er auch Hochschulen nun die Freiheit, Software von oder unter Zuhilfenahme von Tochterunternehmen US-amerikanischer Konzerne auszuwählen, wenn der Anbietende die DSGVO-konforme Verarbeitung personenbezogener Daten vertraglich zusichern kann.

Dennoch ist bei der Überprüfung der entsprechenden Software stets auf den konkreten Einzelfall abzustellen. Denn der Beschluss des OLG Karlsruhe kann nicht als genereller „Freifahrtschein" für kritische Softwarelösungen herangezogen werden. Sobald sich konkrete Hinweise ergeben, welche eine datenschutzkonforme Verarbeitung infrage stellen, muss diesen nachgegangen und sie sollten überprüft werden.

So wurde beispielsweise in Berlin jüngst die Freie Universität (FU) von der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) aufgefordert, die Nutzung der Videokonferenzsoftware „Cisco Webex" einzustellen.[6] Auch bei diesem Sachverhalt ist die Behörde nach einer Prüfung der Software im Januar der Ansicht, dass der datenschutzkonforme Einsatz der Software nicht möglich sei.

Sollte die BlnBDI konkrete Anhaltspunkte vorliegen haben, welche die datenschutzkonforme Verarbeitung der Daten in Zweifel

5 Z.B. zur Auswahl von Videokonferenzsoftware siehe: John, Corona is calling, DFN-Infobrief Recht Jahresband 2020/Covid-19, S. 15.

6 Auszüge des Schreibens der BlnBDI: AstA FU, abrufbar unter https://astafu.de/webex-frist (zuletzt abgerufen am 27.10.2022).

ziehen, hilft die Entscheidung des OLG der FU nun auch nicht weiter. Vielmehr muss in einem solchen Fall der datenschutzkonforme Betrieb überprüft und sichergestellt werden oder auf die Verwendung der Software bzw. der datenschutzwidrigen Bestandteile der Software verzichtet werden.

Anders stellt es sich aber in Fällen dar, in denen diese Anhaltspunkte fehlen. Soweit Anbietende von Softwarelösungen die DSGVO-konforme Verarbeitung vertraglich zusichern, dürfen diese Produkte auch von Hochschulen ausgewählt und verwendet werden, auch wenn es sich um Software-Dienstleistende mit US-amerikanischen Mutterkonzernen handelt. Dennoch muss bei der Einrichtung und dem Betrieb der Software fortlaufend sichergestellt sein, dass die datenschutzrechtlichen Anforderungen auch nach der Auswahl der Software eingehalten werden. [7]

Möglicherweise wird die Verwendung von Software US-amerikanischer Anbietenden in naher Zukunft wieder vereinfacht: Die Fragestellung im vorliegenden Fall kommt vor allem deshalb auf, weil Datenexporte derzeit nur auf Standardvertragsklauseln gestützt werden können und damit umfangreiche technische und organisatorische Maßnahmen einhergehen. Diese Umstände werfen daher schnell die Frage auf, ob diese Software überhaupt datenschutzkonform verwendet werden kann. Nun hat der US-amerikanische Präsident Joe Biden eine entsprechende Exekutivanordnung unterzeichnet,[8] welche einen neuen Angemessenheitsbeschluss ins Leben rufen kann. Das sog. „EU-US-Data-Privacy-Framework“ (EUUSDPF) soll nach Ansicht der USA eine „dauerhafte und verlässliche Rechtsgrundlage“ darstellen. Nun muss die Kommission den entsprechenden Angemessenheitsbeschluss fassen. Dieser wird im Frühjahr 2023 erwartet. Je nach Ausgestaltung des Angemessenheitsbeschlusses könnte hierdurch die Verwendung US-amerikanischer Software für Verantwortliche wieder leichter zu rechtfertigten sein.

7 Siehe z.B. Hinweise zur Nutzung von Microsoft 365 mit den neuen Standardvertragsklauseln: John, New Schrems, new Me(crosoft), DFN-Infobrief Recht 2/2022.

8 Pressemitteilung des Weißen Hauses vom 7. Oktober 2022, abrufbar unter https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/ (zuletzt abgerufen am 27.10.2022).

Kurzbeitrag: Erst, wer an jeder Herberge geklopfet hat…

BGH: Netzsperren müssen ultima ratio bleiben

von Justin Rennert

Um Urheberrechtsverletzungen im Internet zu erschweren, kann die in ihren Rechten verletzte Partei gerichtlich eine Sperrung der Webseite mit rechtswidrigem Inhalt erwirken. Die Voraussetzungen für diese Maßnahme waren dabei in der Vergangenheit äußerst umstritten. Nach einer Entscheidung des Bundesgerichtshofs (BGH) (Urt. v. 13.10.2022, Az. I ZR 111/21) herrscht nun Klarheit.

I. Ausgangspunkt

Eine Reihe von Wissenschaftsverlagen hatte in Deutschland Klage gegen die Telekom als Zugangsanbieter (Access-Provider) erhoben und begehrten die Einrichtung einer Zugangssperre (Netzsperre)[1] für die Webseiten verschiedener sog. „Schattenbibliotheken".[2] Diese haben sich darauf spezialisiert, urheberrechtlich geschützte wissenschaftliche Publikationen kostenfrei und ohne jedwede Nutzungsrechte im Internet zur Verfügung zu stellen. Um die Erreichbarkeit dieser Dienste einzuschränken, versuchten die Verlagshäuser die Telekom als Access-Provider gerichtlich zu einer Netzsperre zu verpflichten.

Die Einrichtung einer Netzsperre begehrten die Verlagshäuser auf Grundlage von § 7 Abs. 4 Telemediengesetz. Diese Regelung spricht dem Rechteinhaber eines urheberechtlich geschützten Werkes einen Anspruch auf Sperrung des Zugangs zu den rechtswidrigen Inhalten gegen den Diensteanbieter zu. Schon die Vorinstanz, das Oberlandesgericht (OLG) München[3] hatte festgestellt, dass ein solcher Anspruch ausschließlich das letzte Mittel darstelle. Nur, wenn ein Vorgehen gegen den Webseitenbetreiber (die Schattenbibliotheken selbst) oder die Host-Provider (Dienstleister, der die Erreichbarkeit der Webseite im Internet sicherstellt) absolut aussichtslos ist, kann auf den Anspruch auf Sperrung zurückgegriffen werden. An dieser Subsidiarität des Anspruchs auf Sperrung ließ das vorinstanzliche OLG schließlich auch das Begehren der Wissenschaftsverlage scheitern, da diese sich nicht ausreichend bemüht hätten gegen die Webseitenbetreiber oder die Host-Provider selbst vorzugehen. Dass der Host-Provider in Schweden ansässig ist, stehe dem nicht entgegen, da Schweden EU-Mitgliedstaat sei und somit aufgrund der gemeinsamen unionsrechtlichen Gesetzesgrundlage zumindest auch dort Auskunftsmöglichkeiten bestehen müssten. Dass die Verlage mit dem Host-Provider in Kontakt getreten waren und diesen abgemahnt hatten, reiche nicht aus, da ein gerichtliches Vorgehen ausgeblieben war.

II. Die Entscheidung des BGH

Im Ergebnis schließt sich der BGH mit seiner Entscheidung nun dem Urteil des OLG an. Die Beantwortung der Frage, welche Anstrengungen zur Inanspruchnahme der Beteiligten, die die Rechteverletzung selbst begangen (Webseitenbetreiber), oder zu ihr durch Erbringung von Dienstleistungen beigetragen haben (Host-Provider), angemessen sind, sei eine Frage des Einzelfalls.

---

1 Zur näheren Erläuterung von Netzsperren: Klein, Macht die Schotten dicht – oder doch nicht?, DFN-Infobrief Recht 11/2014; Klein, Den Letzten beißen die Hunde, DFN-Infobrief Recht 4/2016; Gielen, Im Hinterzimmer zur Netzsperre, DFN-Infobrief Recht 7/2021.

2 Siehe hierzu: McGrath, Schattenbibliotheken hinter schwedischen Gardinen?, DFN-Infobrief 9/2022.

3 OLG München, Urteil vom 27.05.2021, 29 U 6933/19, Rn. 57 ff.

In zwei Punkten macht der BGH jedoch allgemeine Vorgaben, die der Rechteinhaber in jedem Fall einzuhalten habe: So seien Rechteinhaber grds. dazu verpflichtet, Ermittlungen bezüglich der vorrangig in Anspruch zu nehmenden Beteiligten anzustellen und diese außergerichtlich in Anspruch zu nehmen. Bleibt das außergerichtliche Vorgehen erfolglos, so müsse der Rechteinhaber jedenfalls gegen innerhalb der EU ansässige Betreiber oder Hostprovider ein Verfahren des einstweiligen Rechtsschutzes anstrengen. Vom Rechteinhaber könne schließlich jedoch nicht verlangt werden, Maßnahmen anzustrengen, die zu einer nicht zumutbaren zeitlichen Verzögerung der Anspruchsdurchsetzung führen oder denen jede Erfolgsaussicht fehlen würde.

Die vorgehende Entscheidung des OLG erweise sich daher laut der Entscheidung der Karlsruher Richter als rechtsfehlerhaft, da sie nicht feststelle, ob den Wissenschaftsverlagen gegen den Host-Provider in Schweden auch tatsächlich die Möglichkeit des einstweiligen Rechtsschutzes zugestanden hätte. Darauf käme es jedoch an, um die Zumutbarkeit der Anstrengung eines Verfahrens feststellen oder ablehnen zu können. Dennoch erweise sich die Entscheidung aus anderen Gründen als richtig, denn die klagenden Verlage müssten zumindest versuchen, vor einem deutschen Gericht mittels einstweiliger Verfügung einen Auskunftsanspruch gegen den schwedischen Host-Provider geltend zu machen.

Mit seinem Urteil bekräftigt der BGH somit die Subsidiarität eines Anspruchs gegen den Access-Provider. Die deutlich näher an der Rechtsverletzung stehenden Webseitenbetreiber oder Host-Provider sind vorrangig in Anspruch zu nehmen, soweit dies dem Rechteinhaber zumutbar ist. Scheitern die Bemühungen im einstweiligen Rechtsschutz, kommt eine Netzsperre gegen den Access-Provider durchaus in Betracht – sie bleibt jedoch ultima ratio.

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

Podcast der Forschungsstelle Recht im DFN

„Weggeforscht“, der Podcast der Forschungsstelle Recht im DFN, informiert knapp und verständlich über relevante juristische Entwicklungen und Fragestellungen im digitalen Umfeld. Neben einem kurzen Newsblock wird in jeder Folge ein aktuelles Thema erörtert.

Er erscheint regelmäßig ein- bis zweimal im Monat auf allen gängigen Podcast-Plattformen.

Link: https://anchor.fm/fsr-dfn