infobrief recht DEN

9 / 2020
September 2020

Mensch gegen Maschine
Zur datenschutzrechtlichen Relevanz von automatisierten Proctoringdiensten bei digitalen Prüfungen

Am Anfang war alle Software frei
Rechtliche Fallstricke im Umgang mit freier und Open Source Software

Du warst mir ja ´ne Marke!
Zum markenrechtlichen Schutz des Begriffs „Webinar“

Mensch gegen Maschine

Zur datenschutzrechtlichen Relevanz von automatisierten Proctoringdiensten bei digitalen Prüfungen

von Owen Mc Grath

Im Zuge der Umstellung der Lehre auf den digitalen Betrieb in den letzten Monaten wurde auch das Prüfungswesen in weiten Teilen den aktuellen Umständen angepasst. Wo Prüfungen nicht unter Einhaltung der erforderlichen Hygiene- und Sicherheitsmaßnahmen durchgeführt werden konnten und können, blieb und bleibt nur der Rückgriff auf alternative Konzepte. Neben Open-Book-Klausuren, mündlichen Einzelprüfungen und Hausarbeiten, scheint sich auch die Prüfung vor dem heimischen Bildschirm durchgesetzt zu haben.

I. Die Notwendigkeit von Überwachungsmaßnahmen

Zur Wahrung der prüfungsrechtlichen Chancengleichheit (bereits grundgesetzlich verankert in Art. 12 und Art. 3 Grundgesetz) erfordern digitale Prüfungen, genau wie ihr analoges Pendant der Präsenzprüfung, den Einsatz von Überwachungsmaßnahmen.[1] Überwachungsmaßnahmen, welche während einer digitalen Klausur via Webcam und ähnlichen Technologien durchgeführt werden, werden auch als Proctoring bezeichnet. Neben dem unmittelbaren sog. Human Proctoring, bei welchem die Prüflinge zeitgleich durch einen Menschen unter Einsatz technischer Hilfsmittel überwacht werden, etablierten sich mit steigender Bedrohung durch das Corona-Virus in Europa Dienste, welche ein automatisiertes Proctoring anbieten. Eine Vielzahl dieser Dienste stammt aus den USA, wo sie auch seit Längerem bereits eingesetzt werden. Im Gegensatz zu digitalen aber menschlichen Überwachungsdiensten ermitteln automatisierte Proctoringlösungen die Wahrscheinlichkeit eines Täuschungsversuches durch die Erfassung und Verarbeitung des Verhaltens des Prüflings mittels eines Algorithmus. Hierbei eingesetzte Mittel erstrecken sich von klassischer Audio- und Videoüberwachung über Bildschirmaufzeichnungen, Raumscans und Identitätsfeststellungen bis hin zu Eye-Tracking, Tastatur-Anschlags-Messungen und tatsächlicher Bildschirmkontrolle. Damit ist den Überwachungsmöglichkeiten jedoch noch kein Ende gesetzt. Viele Dienstleister bieten den Prüfungseinrichtungen eine weitere Fülle an Überwachungsmöglichkeiten, welche nach Bedarf verwendet werden können.
Die erfassten Daten werden simultan zur Prüfung von einem Algorithmus verarbeitet und bewertet. Für den Prüfer selbst ist dann während und auch nach der Prüfung aus den Berechnungen ersichtlich, wie hoch nach dem festgestellten Verhalten die Wahrscheinlichkeit ist, dass der Prüfling einen Täuschungsversuch begangen hat oder zu nichterlaubten Hilfsmitteln gegriffen hat.

Zur sicheren Überprüfungsmöglichkeit werden die Daten der Überwachungsmaßnahmen nicht nur direkt verarbeitet, sondern regelmäßig zusätzlich aufgezeichnet. So ist es dem Prüfenden möglich nach Beendigung der Klausur die errechnete Täuschungswahrscheinlichkeit durch Sichtung der Aufzeichnungen zu verifizieren.

Auch wenn durch das automatisierte Proctoring eine Überwachungsmöglichkeit im E-Prüfungsbereich mit geringem Personalaufwand geschaffen wurde, so bestehen doch einige Bedenken gegen den Einsatz dieser Methode.

1 Zur allgemeinen datenschutzrechtlichen Zulässigkeit von Überwachungsmaßnahmen: Uphues, Der Prüfling – Allein zu Haus, DFN-Infobrief Recht 07/2020.

II. Technische Bedenken

Die mannigfaltigen Überwachungsmöglichkeiten eines durchschnittlichen automatischen Proctoringdienstes scheinen auf den ersten Blick eine hervorragende und vor allem sichere Durchführung von Online-Klausuren zu ermöglichen. Je mehr Parameter überwacht werden, desto mehr Täuschungsversuche werden ausgemerzt. Im Ergebnis verbleibt also eine dem Grundsatz der prüfungsrechtlichen Chancengleichheit entsprechende Variante der digitalen Prüfungen. Bei dieser Betrachtung bleiben allerdings bereits einige technische Aspekte unberücksichtigt.

Auch wenn die Aufdeckungsquote des Algorithmus überdurchschnittlich gut sein sollte, kann er dennoch nicht mit absoluter Sicherheit einen Täuschungsversuch identifizieren und anzeigen. Das Ergebnis der Berechnung wird immer nur eine Tendenz sein. Um diese Tendenz zu bestätigen, ist das aufgezeichnete Material im Anschluss an die Prüfung erneut zu sichten. Hinzu kommt, dass ein unmittelbares Reagieren auf einen potentiellen Täuschungsversuch (bspw. eine Aufforderung zum Raumscan oder zum Abfilmen des Arbeitsplatzes nach verdächtigem Verhalten) bei der nachträglichen Beschau der Aufzeichnungen nicht mehr möglich ist. Einen Täuschungsversuch so sicher zu verifizieren, stellt sich entsprechend problematisch dar. Freilich bestünde die Möglichkeit während einer automatisch überwachten Prüfung auf eine durch das Programm angezeigte Täuschungstendenz direkt zu reagieren und unmittelbar Aufklärungsmaßnahmen zu ergreifen. Die zusätzliche menschliche Durchführung solcher Investigationen widerspricht aber wohl zentral dem Einsatz eines Dienstes, der gerade eine menschliche Überwachung und damit hohen Personalaufwand obsolet machen soll.

Die eingesetzten Maßnahmen dienen darüber hinaus nicht durchweg der unmittelbaren Aufdeckung von Täuschungsversuchen. Teilweise haben sie, nach eigener Aussage eines Proctoringdienstes, nur eine rein abschreckende, psychologische Wirkung. Der Geprüfte soll sich durch einige Instrumente schlichtweg stärker überwacht fühlen, obwohl er es faktisch nicht ist. Auch wenn der psychologische Effekt solcher Maßnahmen und die entsprechende Auswirkung auf die Bereitschaft zur Täuschung nicht abzustreiten ist, so ist die Notwendigkeit solcher Maßnahmen, gerade mit Blick auf die zusätzliche Belastung der Prüflinge, zumindest anzuzweifeln. Ferner stellt die Existenz von solchen „Leerüberwachungen“ die tatsächliche Wirksamkeit der sonstigen eingesetzten Mittel in Frage.

III. Datenschutzrechtliche Bedenken

Abseits der grundlegenden technischen Bedenken ergeben sich auch datenschutzrechtliche Problembereiche. Vor allem die notwendige Aufzeichnung der Überwachungsmaßnahmen, sowie die teilweise herrschende Unbeholfenheit bei der Beachtung der Vorschriften der Datenschutz-Grundverordnung (DSGVO) sorgen für Zweifel an der datenschutzrechtlichen Konformität.

Wie beschrieben macht es die Überprüfbarkeit der Täuschungstendenz notwendig, dass Überwachungsmaßnahmen aufgezeichnet werden. Die Aufzeichnung stellt neben der eigentlichen Überwachungsmaßnahme eine weitere Verarbeitung personenbezogener Daten dar und damit einen für das europäische Datenschutzrecht relevanten Vorgang. Die verstärkte Verarbeitung personenbezogener Daten kann nur rechtmäßig sein, wenn sie auch den Grundsätzen der Datenverarbeitung nach Art. 5 Abs. 1 DSGVO entspricht. Dafür müsste die Verarbeitung nach Art. 5 Abs. 1 lit. c DSGVO besonders auch „dem Zweck angemessen und […] auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“. Die Zwecke der Verarbeitung bei Überwachungsmaßnahmen im Rahmen von E-Klausuren liegen in der Ermöglichung einer chancengleichen Prüfung unter Berücksichtigung der notwendigen Hygiene- und Sicherheitsstandards. Dieser Zweck unterscheidet sich nicht bei verschiedenen Arten der Überwachung. Sowohl menschliche als auch automatische Überwachungen verfolgen den gleichen Zweck. Allerdings ließe sich die zusätzliche Aufzeichnung von Überwachungen und die entsprechende Datenverarbeitung durch den Einsatz unmittelbaren, also menschlichen Proctorings einfach umgehen. Wird direkt durch einen menschlichen Prüfer überwacht, sind Aufzeichnungen der Überwachungsmaßnahmen zur nachträglichen Überprüfung überflüssig. Damit allein ist die Verarbeitung personenbezogener Daten im Rahmen von automatisierten Proctoringdiensten regelmäßig nicht auf das notwendige Maß beschränkt und daher nicht mit den Vorgaben der DSGVO zu vereinbaren.

Zwar ergeben sich auf den ersten Blick durch den Einsatz automatisierter Dienste Personalersparungen. Diese werden im

Ergebnis allerdings durch die notwendige Nachschau der Aufzeichnungen und die Kosten für den Dienst als solches hinfällig. Eine höhere Effizienz oder stärkere Zweckverfolgung lässt sich daher bei einem automatisierten Verfahren nicht erkennen.

Mit der gleichen Argumentation ist auch dem Einsatz von möglichst umfassenden Überwachungsmitteln aus datenschutzrechtlicher Sicht entgegenzutreten. In der Theorie mag die Zuhilfenahme von sehr weitreichenden Überwachungsmaßnahmen zwar zu einer erhöhten Aufdeckungsquote von Täuschungsversuchen führen. Tatsächlich bedeuten diese Instrumente aber nur eine stärkere Belastung der Rechte der Geprüften[2] ohne gesteigerte Effizienz. Das eingesetzte Mittel ist dem Zweck nicht angemessen. Schlicht gesagt: Herkömmliche Überwachungsmaßnahmen reichen aus um eine chancengleiche Prüfung zu gewähren.

Ferner ist bei der Überwachung von E-Klausuren nicht aus dem Blick zu verlieren, welche Situation eigentlich substituiert werden soll. Es geht nicht darum eine totale Überwachung oder die Unmöglichkeit von Täuschungen zu gewährleisten, auch wenn die technischen Möglichkeiten im heutigen Zeitalter geradezu darauf drängen. Vielmehr geht es darum eine der Präsenzklausur vergleichbare Situation zu schaffen und so den gewöhnlichen Prüfungs- und Hochschulbetrieb aufrecht zu erhalten. Eine Vielzahl der Maßnahmen des automatisierten Proctorings scheinen aber über dieses Ziel hinaus zu schießen. Einem Prüfer in Präsenzklausuren ist es nicht möglich Tastaturanschläge (bzw. „Stiftanschläge“) zu messen oder den „Prüfungstisch“ bis ins letzte Detail zu kontrollieren. Ohne starke Konfiguration der automatisierten Dienste erfolgen also eine Vielzahl an überflüssigen und nicht weiter zweckgebundenen, damit nicht-DSGVO-konformen Datenverarbeitungen.

Nebst diesen inhaltlichen Problemen ergibt sich noch ein zentrales organisatorisches datenschutzrechtliches Sorgenkind. Die meisten Proctoringdienste stammen aus den USA. Bisher war der Einsatz an europäischen und vor allem auch deutschen Hochschulen nicht der Regelfall. Der in der Zeit des Corona-Virus‘ virulent gewordenen Problematik der nötigen Überwachung von E-Klausuren wurde zügig durch die Anbieter von Proctoringdiensten durch entsprechende Angebote entgegengetreten. Um möglichst schnell leistungsfähige Konzepte anbieten zu können, stand nicht immer der Datenschutz und die Datensicherheit im Zentrum der Aufmerksamkeit. Folge waren zum Teil mit der DSGVO unvereinbare Konzepte. Zwar werden diese Konzepte ständig aktualisiert und auch in datenschutzrechtlicher Hinsicht nachgebessert. Die Tendenz der anfänglichen Vernachlässigung lässt allerdings nicht auf allgemeine datenschutzrechtliche Konformität hoffen.

Ferner führt die aktuelle Entscheidung des Europäischen Gerichtshofs (EuGH) zum Privacy Shield (Urteil vom 16.7.2020, C-311/18) dazu, dass eine Übertragung von personenbezogenen Daten auf US-amerikanische Server grundsätzlich nicht mehr auf Grundlage des EU-US Privacy Shields möglich ist.[3] Viele der Anbieter von Proctoringdiensten verarbeiten allerdings zumindest Teile der erhobenen Daten auf heimischen Servern in den USA auf Grundlage des Privacy Shields. Zwar ist als Antwort auf das genannte Urteil eine Verlegung der Verarbeitung auf europäische Server zu erwarten. Fraglich ist allerdings, ob eine solche Verlegung tatsächlich vollständig gelingt oder, ob Teile der Verarbeitungen nach wie vor in den Vereinigten Staaten stattfinden werden.

IV. Fazit und Konsequenzen für die Praxis in wissenschaftlichen Einrichtungen

So reizvoll der Einsatz von automatisierten Proctoringdiensten auf den ersten Blick erscheinen mag, so problematisch ist er dennoch zu bewerten. Personaleinsparungen und eine vermeintlich vollständige und unfehlbare Überwachung dürfen nicht über die technischen und datenschutzrechtlichen Bedenken hinwegtäuschen. Bei der Auswahl eines geeigneten Überwachungstools für digitale Klausuren ist nicht außer Acht zu lassen, welche Situation und welcher Überwachungsstandard in einer vergleichbaren Präsenzklausur herrschen würde und inwiefern Eingriffe auf Seiten der Prüflinge hinzunehmen sind. Vorzugswürdig scheinen derzeit unmittelbare menschliche Überwachungsmaßnahmen ohne weitergehende Aufzeichnungen zu sein.

2 Zu der Belastung der Prüflinge genauer: Uphues, Der Prüfling – Allein zu Haus, DFN-Infobrief Recht 07/2020.

3 Vertiefend hierzu: Uphues, Ins Wasser gefallen, DFN-Infobrief Recht 08/2020.

Am Anfang war alle Software frei

Rechtliche Fallstricke im Umgang mit freier und Open Source Software

von Nico Gielen

Die Pandemie und die damit einhergehenden Restriktionen stellen hohe Anforderungen an die Digitalisierung an Hochschulen und Forschungseinrichtungen. Der richtige Einsatz von Software ist damit von zentraler Bedeutung, um die anstehenden Herausforderungen zu bewältigen. Ein besonderes Augenmerk liegt dabei auf Videokonferenzdiensten, mithilfe derer eine digitale Lehre ermöglicht wird. Da hierbei zunehmend auch auf freie und Open Source Software zurückgegriffen wird, soll dies den Anlass für eine Erläuterung und rechtliche Einordnung geben.

I. Historischer Hintergrund

Bis 1970 haben Computerhersteller ihre Software noch kostenlos, mitsamt Quellcode und stets zusammen mit der Hardware ausgeliefert. Dieser freie Umgang mit Software begünstigte die Entstehung einer Hackerkultur an akademischen Universitäten, im Rahmen dessen Programmierer die Software veränderten und untereinander austauschten. Dann aber wurde das Konzept einer Softwarelizenz eingeführt, um fortan die Softwarenutzung rechtlich zu beschränken, ein neues Marktsegment zu etablieren und dieses im gleichen Zuge gewinnbringend zu erschließen. Software wurde nicht mehr zwingend mit der Hardware zusammen und erst recht nicht mit dem Quelltext ausgeliefert. Vielmehr wurde sie nur in maschinenlesbarer Form vertrieben und zudem als Geschäftsgeheimnis klassifiziert. Veränderungen der Software waren fortan rechtlich und praktisch unmöglich. Die ursprünglich freie Software wurde somit proprietär.

Daraufhin zerfiel auch die akademische Hackerszene. Dessen prominentes Mitglied Richard Stallman kündigte daraufhin seinen Arbeitsvertrag am MIT und widmete sich nunmehr einer Gegenbewegung. Er gründete 1985 die Free Software Foundation, dessen Hauptaufgabe die Unterstützung des GNU-Projektes war. GNU ist dabei eine Abkürzung für „GNU's not Unix" und spielt damit auf das Betriebssystem Unix an, das ursprünglich Arbeitsmittel der Hackergemeinde war, dann aber proprietär wurde und ihr damit die Arbeitsgrundlage entzog – mithin ein perfektes Feindbild. Im Rahmen dieses GNU-Projektes wurden fortan diverse Maßnahmen ergriffen, die allesamt darauf gerichtet waren, freie Software zu fördern.

Aus dieser an der Ostküste gegründeten Bewegung spaltete sich jedoch bald darauf an der Westküste eine Gruppe ab. Die im Silicon Valley tätigen Softwareentwickler planten 1998 eine regelrechte Marketingkampagne. Denn sie fürchteten, der Aktivismus des Free Software Movements würde Wirtschaftsvertreter abschrecken und damit das an sich begrüßenswerte Ansinnen der Bewegung gefährden. Daher tadelten sie den Begriff „Free Software" als verwirrend und sprachen sich für einen terminologischen Richtungswechsel aus. Daraufhin wurde der Begriff „Open Source" vorgeschlagen, der sich prompt durchsetzte und ein eigenes Open Source Movement lostrat.

Obgleich sich die inhaltlichen Anforderungen an freie und Open Source Software im Einzelnen unterscheiden mögen, sind sie zu weiten Teilen deckungsgleich. Der Hauptunterschied zwischen den beiden Bewegungen ist vielmehr ideologischer Natur. Das Free Software Movement verband mit freier Software auch eine soziale und freiheitliche Dimension und war damit eng an die politischen Vorstellungen von Stallman geknüpft. Hingegen liegt Open Source eine andere Philosophie zugrunde. Eric S. Raymond, der das Aushängeschild des Open Source Movements werden sollte, verglich Open Source mit einem Basar, auf dem die Öffentlichkeit jede Entwicklung einsehen und an ihr mitwirken kann. Neben diesem kollaborativen Element ist Open Source aber auch weniger politisch

aufgeladen, sondern verfolgt vielmehr einen pragmatischen Ansatz.

II. Definitionsansätze

Wie bereits anklang, bestand Verwirrung hinsichtlich des Begriffs der freien Software. Oftmals wurde sie mit kostenloser Software gleichgesetzt, woraufhin Aktivisten sich genötigt sahen den Slogan „Free as in Freedom, Not Free as in Free Beer!“ zu skandieren. Die offizielle Definition von freier Software wurde von Stallman entwickelt und als „The Four Essential Freedoms of Free Software“ getauft. Eine Software ist in diesem Sinne frei, wenn sie keinerlei Nutzungsbeschränkungen unterliegt; wenn sie studiert und verändert werden kann, wozu der Quellcode einsehbar sein muss; wenn Kopien des Originals sowie von veränderten Versionen verbreitet werden dürfen.

Wann eine Software hingegen Open Source ist, bestimmt sich nach der durch die Open Source Initiative erlassenen Definition.[1] Zunächst wird klargestellt, dass der Begriff nicht gleichbedeutend ist mit einem Zugriff auf den Quellcode. Vielmehr sind zehn Kriterien zu beachten. Dazu gehört, dass die Software unentgeltlich vervielfältigt, bearbeitet und verbreitet werden darf, dass der Quelltext einsehbar ist und dass eine Verbreitung modifizierter Versionen nur unter denselben Lizenzbedingungen erfolgen darf wie das Original. Des Weiteren darf die Software niemanden diskriminieren und die Nutzung der Software darf nicht an einen bestimmten Verwendungszweck oder ein bestimmtes Produkt gebunden werden. Schließlich darf die Nutzung anderer Software nicht beeinträchtigt werden und die Nutzung der Software muss technologieneutral gestaltet sein.

Aufgrund der großen Überschneidung der beiden Definitionsansätze und zur Umgehung dieses Namensstreits wurde mit Free and Open Source Software (FOSS) ein Sammelbegriff geschaffen. Dieser kann zum einen zur proprietären Software abgegrenzt werden. Allerdings wird an den dargestellten Bedingungen auch klar, dass FOSS nicht uneingeschränkt genutzt werden kann. Deswegen ist sie zum anderen zur Public Domain Software abzugrenzen. Ein häufiges Missverständnis bei FOSS besteht auch darin, dass angenommen wird, sie dürfe keinesfalls entgeltlich vertrieben werden. Zentral ist jedoch nur, dass für die Nutzung der Software keine Gebühr anfallen darf. Dies bedeutet nicht, dass für den Verkauf einer bestimmten Programmkopie im Einzelfall nicht doch ein Preis verlangt werden darf. Des Weiteren ist auch eine kommerzielle Nutzung von FOSS nicht prinzipiell ausgeschlossen.

III. Rechtliche Einordnung

Software beschäftigt nicht nur Programmierer, sondern auch Urheberrechtler. Allerdings gehen diese FOSS aus der entgegengesetzten entgegenstehenden Perspektive an. § 69c Urheberrechtsgesetz (UrhG) macht deutlich, dass der Urheber einer Software bestimmte Rechte innehat, wodurch die Nutzung der Software anderen Personen zu einem großen Teil verboten wird. Insbesondere dürfen sie Software ohne eine Erlaubnis des Urhebers nicht vervielfältigen, bearbeiten oder verbreiten. Damit widerspricht das Urheberrecht in einem zentralen Punkt der FOSS, die voraussetzt, dass solche Verbote gerade nicht bestehen.

1. Lizenzvereinbarung

Das Mittel zur Lösung dieses Konflikts ist die Lizenz. Das UrhG nennt sie in § 31 UrhG zwar Nutzungsrecht, ein inhaltlicher Unterschied geht damit aber nicht einher. Die Lizenz ist eine Vereinbarung zwischen dem Urheber der Software und einem Softwarenutzer. Diese wird oftmals dem Quelltext des Programms vorangestellt. Der Nutzer, der sodann eine Vervielfältigung oder eine Verbreitung vornimmt, zeigt sich dadurch mit der Lizenz einverstanden. Das Zustandekommen der Lizenzvereinbarung bedarf also keines direkten Kontakts zwischen Nutzer und Urheber.
Mithilfe dieser Vereinbarung kann der Urheber allerdings nicht auf sein gesamtes Urheberrecht verzichten. Der Grund dafür liegt in der kontinentaleuropäischen Auffassung, dass Urheberrecht nicht nur ein wirtschaftliches Verwertungsrecht ist, sondern damit untrennbar auch eine persönlichkeitsrechtliche und damit im Kern unverzichtbare Verbindung zwischen Urheber und dem Werk einhergeht. Abseits dieses Kernbereichs darf ein Urheber aber über seine eigenen Verbotsrechte verfügen. Er kann damit insbesondere anderen Personen erlauben, seine Software zu vervielfältigen, zu bearbeiten und zu verbreiten.

1 Siehe unter www.opensource.org/osd.

Der Gesetzgeber hat mit § 32 Abs. 3 S. 3 UrhG auch eine Ausnahme von dem Grundsatz geschaffen, dass der Urheber angemessen zu vergüten ist, wenn er die Nutzung seines Werkes erlaubt. Ohne diese sog. Linux-Klausel wäre es mit dem deutschen Urheberrecht nicht vereinbar, dass FOSS unentgeltlich vertrieben wird.

2. Mustertexte

Der Urheber der Software kann mit dem jeweiligen Nutzer eine individuelle Vereinbarung aushandeln. Er kann aber auch – und dies ist der Regelfall – auf eine vorformulierte Vereinbarung zurückgreifen. Dabei kann zwischen allgemeinen und auf bestimmte Bereiche zugeschnittene Lizenzen differenziert werden. Beispielweise sind die GNU Lesser General Public License auf die Programmierung von Programmbibliotheken und die GNU Free Documentation License auf die Weitergabe von Software-Dokumentationen zugeschnitten. Breiter Verwendung erfreuen sich auch Creative Commons-Lizenzen, die für die Lizenzierung von Bildern, Texten und Musik verwendet werden.

Die am häufigsten verwendete Lizenz ist die GNU General Public License (GPL).[2] Sie wurde 1989 von Richard Stallman verfasst und stellt die wohl bekannteste Errungenschaft des oben erwähnten GNU-Projektes dar. Mittlerweile wurde die GPL noch zweimal aktualisiert. Auch in der dritten Version finden sich zwar unwirksame Bestimmungen, da die Lizenz nicht auf das deutsche Recht zugeschnitten ist. Ein Beispiel hierfür ist der zu weitgehende Haftungsausschluss. Im Grundsatz jedoch handelt es sich bei der GPL um eine auch nach deutschem Urheberrecht wirksame Lizenz.
Im Besonderen zeichnet sie aus, dass sie auf dem Prinzip des Copyleft gründet – ein Wortspiel als Gegenüberstellung zum Copyright. Dieses erfordert, dass jegliche Modifikationen der Ursprungssoftware auch der Ursprungslizenz unterworfen werden muss. Damit unterscheidet sie sich in einem zentralen Punkt von anderen Lizenzen wie etwa der Lizenz der Berkeley Software Distribution (BDS). Die einer BSD-Lizenz unterworfene Software, die also nicht dem Copyleft unterliegt, kann damit auch als Vorlage für proprietäre Software dienen.

2 Weitere Beispiele bei Mörike, Der Preis der Freiheit – Zu den Rechten und Pflichten bei der Nutzung „Freier Software“, DFN-Infobrief Recht 04/2017, S. 2 f.

IV. Folge eines Verstoßes

Wenn die in der jeweiligen Lizenz aufgelisteten Bedingungen nicht erfüllt werden, kann das Nutzungsrecht erlöschen. Dadurch ist die Softwarenutzung wieder verboten und der Nutzer urheberrechtlichen Ansprüchen ausgesetzt. Hierzu zählen die Ansprüche auf Ersatz etwaiger Abmahnungskosten (§ 97a Abs. 3 S. 1 UrhG), Unterlassung (§ 97 Abs. 1 S. 1 UrhG) und Schadensersatz (§ 97 Abs. 2 S. 1 UrhG).

Dazu ein Beispiel aus dem Jahr 2016: In diesem Fall hatte eine Hochschule eine unter der GPL angebotene Software bezogen und wiederum auf ihrer Webseite zum Download angeboten. Da sie aber weder den Lizenztext noch den Quellcode zur Verfügung stellte, verstieß sie gegen die GPL und das Nutzungsrecht entfiel. Die Entgegnung der Hochschule, sie habe die Software ihrerseits von einer Seite geladen, die diese Bedingungen nicht erfüllte, ließ das Gericht nicht durchgreifen. Vielmehr treffe die Hochschule eine Prüfpflicht, der sie in diesem Fall nicht nachgekommen sei. Schließlich verurteilte das Landgericht (LG) Bochum die Hochschule wegen Urheberrechtsverletzung einerseits zum Ersatz der Abmahnungskosten und zur Unterlassung, wobei hervorgehoben werden kann, dass bereits der einmalige Verstoß eine für den Unterlassungsanspruch erforderliche Wiederholungsgefahr indizieren soll. Überraschenderweise verurteilte das LG Bochum die Hochschule auch zur Zahlung eines Schadensersatzes (Urteil vom 3.3.2016, Az. I-8 O 294/15).[3]

Nicht zuletzt wegen dieser Überraschung wurde Berufung eingelegt, wodurch das Urteil des LG Bochum vom Oberlandesgericht (OLG) Hamm überprüft wurde (Urteil vom 13.6.2017, Az. 4 U 72/16). Dieses schloss sich dem LG Bochum grundsätzlich an, widersprach jedoch in Bezug auf den Schadensersatz. Es verwies darauf, dass für unter einer GPL vertriebenen Software eben kein Entgelt verlangt werden darf. Daher habe die Nutzung der Software durch die Hochschule keinen objektiven Wert. Mit anderen Worten bestehe kein Schaden, der von der Hochschule ersetzt werden könnte. Da gegen das Urteil des OLG Hamm keine Revision eingelegt wurde, ist ungewiss, ob diese Rechtsansicht auch vor dem Bundesgerichtshof Bestand haben wird.

3 Ausführlicher Klein, Die Grenzen der Freiheit – Landgericht Bochum verurteilt Hochschule zur Zahlung von Schadensersatz wegen Verstoßes gegen die Bedingungen der General Public License, DFN-Infobrief Recht 07/2016, S. 2 ff.

V. Empfehlungen und Fazit

Bereits an den genannten Gerichtsentscheidungen wird deutlich, dass sich auch Hochschulen tunlichst an die Lizenzbedingungen halten sollten, da sie sich ansonsten urheberrechtlichen Ansprüchen aussetzen können. Um die Lizenzbedingungen einzuhalten, ist ein aufmerksames Studium des Lizenztextes unabdingbare Voraussetzung. Im Regelfall wird dieser einen Hinweis auf die Ursprungsquelle der Software erfordern. Darüber hinaus können jedoch auch noch andere Voraussetzungen bestehen, wie die Offenlegung des Lizenztextes und des Quellcodes.

Eine weitere Problematik besteht darin, dass dem vermeintlichen Lizenzgeber unter Umständen die Berechtigung zur Weitergabe der Software fehlt. Daher sind Lizenznehmer dazu angehalten, diese Berechtigung zu überprüfen. Für den Umfang dieser Prüfpflicht gibt es keine starren Vorgaben und sie ist auch stets vom Einzelfall abhängig. Gleichwohl dürfte nur selten das blinde Vertrauen auf die Zusicherung des Softwarelieferanten ausreichen, er sei zur Weitergabe der Software befugt. Zwar dürfte die Annahme naheliegen, dass die Anforderungen an die Prüfpflicht sinken, wenn die Software seit längerer Zeit verfügbar ist und durch anerkannte Distributoren bereits weit verbreitet wurde. Bestehen aber weiterhin Zweifel, sollte gleichwohl sachkundiger Rat eingeholt werden. Sollte es trotz aller Vorsichtsmaßnahmen zu einer Abmahnung kommen, sollte in einem ersten Schritt überprüft werden, ob der Anspruchsteller wirklich Rechteinhaber ist oder dies nur vorgibt zu sein. Wenn die Berechtigung des Anspruchstellers feststeht, sollte die Urheberrechtsverletzung unverzüglich unterbunden werden. Zudem kann die Abgabe einer strafbewehrten Unterlassungserklärung sinnvoll sein, da durch eine solche die für einen Unterlassungsanspruch erforderliche Wiederholungsgefahr entfällt und damit einem teuren Gerichtsverfahren vorgebeugt werden kann.[4]

Diese Überlegungen sollen gleichwohl nicht zu der Annahme verleiten, dass Hochschulen und Forschungseinrichtungen Abstand von FOSS nehmen sollten. Da bei proprietärer Software nicht minder große Herausforderungen bestehen, sollten sie im Gegenteil FOSS mehr in den Fokus nehmen. Dadurch können sie Kosten einsparen und zugleich eine transparente Softwareentwicklung fördern.

4 Hierzu auch Ochsenfeld, Freie Gefahrenquelle – Landgericht Halle zur Reichweiter der Wiederholungsgefahr bei der Verletzung der sogenannten General Public License (GPL), DFN-Infobrief Recht, Jahresband 2015, S. 150 ff.

Du warst mir ja ´ne Marke!

Zum markenrechtlichen Schutz des Begriffs „Webinar“

von Steffen Uphues

In der August-Ausgabe des letztjährigen DFN-Infobriefs erschien ein Text zu den rechtlichen Voraussetzungen zur Eintragung einer Marke am Beispiel „Webinar“ („Du bist mit ja ´ne Marke!“)[1]. Dieser bislang markenrechtlich geschützte Begriff rückte spätestens mit Beginn der Corona-Pandemie endgültig in den Fokus von Bildungsangeboten durch Hochschulen und öffentliche Forschungseinrichtungen. Zuletzt kamen Meldungen auf, es wäre im Zusammenhang mit Webinar-Veranstaltungen zu Abmahnungen mit Hinweis auf den markenrechtlichen Schutz des Begriffes gekommen. Im Folgenden soll dargelegt werden, weshalb der Begriff nicht länger durch das Markenrecht geschützt sein dürfte und etwaigen Abmahnungen folglich die Grundlage entzogen ist.

I. Einführung

Ist ein Begriff markenrechtlich geschützt, stehen dem Markeninhaber nach § 14 Markengesetz (MarkenG) bei rechtswidriger Verwendung des Begriffs einige Anspruchsziele offen. Insbesondere kann er Unterlassung und Schadensersatz geltend machen. Wie im Infobrief „Du bist mir ja ´ne Marke“ schon erläutert wurde, ist ein markenrechtlicher Schutz ein gewerbliches Schutzrecht und deshalb nur dann zu beachten, wenn man im geschäftlichen Verkehr agiert. Öffentliche Hochschulen und Forschungseinrichtungen verfolgen im Regelfall jedoch keine kommerziellen Interessen. Insofern stehen dem Markeninhaber zumeist keine Ansprüche bei einer Verwendung durch diese Einrichtungen zu. Für den Begriff „Webinar“ scheint ein markenrechtlicher Schutz darüber hinaus ganz allgemein nicht mehr relevant.

II. Was steht einem Schutz entgegen?

Für den Begriff „Webinar“ scheint ein markenrechtlicher Schutz darüber hinaus in zweierlei Hinsicht nicht gerechtfertigt zu sein. Zunächst sind die Voraussetzungen für einen Verfall nach § 49 MarkenG gegeben. Damit das Deutsche Patent- und Markenamt (DPMA) die Marke für verfallen erklärt und löscht, sind bereits entsprechende Anträge beim DPMA eingegangen.[2] Daneben erscheint fraglich, ob die Marke vom Inhaber auch geltungserhaltend im Sinne des Markengesetzes verwendet wurde.

1. Verfall nach § 49 MarkenG

In § 49 MarkenG sind verschiedene Konstellationen normiert, die zu einem Verfall des markenrechtlichen Schutzes und in der Folge zur Löschung der Markeneintragung führen können. Zwingende Voraussetzung ist sowohl nach Abs. 1 als auch nach Abs. 2, dass ein Antrag auf Löschung gestellt wird. Mit Blick auf den Begriff „Webinar“ soll sogleich dargestellt werden, weshalb ein Antrag nach § 49 Abs. 2 Nr. 1 MarkenG zu stellen war – der Begriff war nämlich in den letzten Jahren zu einer im allgemeinen Sprachgebrauch geläufigen Bezeichnung für im Internet abgehaltene Seminare geworden.

Zunächst ist jedoch auf die Regelungen aus § 8 Abs. 2 MarkenG hinzuweisen. Diese enthalten verschiedene absolute Schutzhindernisse. Liegt ein solches Schutzhindernis vor, kann ein Begriff nicht als Marke eingetragen werden. Hintergrund ist,

1 Uphues, Du bist mir ja ´ne Marke!, DFN-Infobrief Recht 08/2019.

2 Registernummer: 30316043

dass ein als Marke einzutragendes Zeichen geeignet sein muss, im Register des DPMA so dargestellt zu werden, dass sowohl Behörden als auch Unternehmen den Schutzgegenstand klar und eindeutig bestimmen können. Nach § 8 Abs. 2 Nr. 3 MarkenG sind demnach solche Begriffe, bei denen sich die zu schützende Marke aus Zeichen zusammensetzt, die dem allgemeinen Sprachgebrauch entspringen und auch zur Benennung der relevanten Dienstleistungen gebraucht werden sollen, nicht eintragungsfähig. Aus heutigem Blickwinkel scheint genau das auf den Begriff „Webinar" zuzutreffen. Entscheidend ist für das Vorliegen eines absoluten Schutzhindernisses jedoch der Zeitpunkt der Markenanmeldung. Der Markenrechtsschutz wurde im Jahr 2003 beantragt. Zu diesem Zeitpunkt dürfte der Begriff jedoch noch nicht Einzug in den allgemeinen Sprachgebraucht erhalten haben. Somit lag keine Üblichkeit im Sinne von § 8 Abs. 2 Nr. 3 MarkenG vor. Insofern erfolgte die Eintragung der Marke im Einklang mit dieser Norm. Sofern – wie im vorliegenden Fall – ein markenrechtlich geschützter Begriff erst im späteren Verlauf in den allgemeinen Sprachgebrauch einzieht, kann ein Verfall nach § 49 Abs. 2 Nr. 1 MarkenG beantragt werden.

Ein Antrag nach § 49 Abs. 2 Nr. 1 MarkenG ist darauf gerichtet, die Eintragung einer Marke als verfallen anzuerkennen und löschen zu lassen. Die Bedingung ist, dass sich die Marke zu einer gebräuchlichen Bezeichnung für Dienstleistungen entwickelt hat, was für den Begriff des Webinars zum jetzigen Zeitpunkt anzunehmen ist. Für diesen Umstand muss der Markeninhaber auch verantwortlich sein. Diese Verantwortung kann sich aus einem aktiven Handeln aber auch aus Untätigkeit ergeben. Der Begriff „Webinar" wurde in den letzten Jahren immer häufiger verwendet. Ein darauf gerichtetes Eingreifen des Markeninhabers – etwa in Form von Abmahnungen – ist nicht bekannt. Es wäre ihm durchaus zuzumuten gewesen, von der Verwendung des Begriffs Kenntnis zu erlangen und dagegen vorzugehen. Demzufolge liegen die Voraussetzungen des § 49 Abs. 2 Nr. 1 MarkenG vor.

2. Nichtbenutzung nach § 25 MarkenG

Neben dem Verfall nach § 49 Abs. 2 Nr. 1 MarkenG könnte ein markenrechtlicher Schutz aus einem anderen Grund entfallen sein. Es könnte an einer rechtserhaltenden Nutzung im Sinne von § 26 MarkenG fehlen. Hierzu ist zunächst klarzustellen, dass der Schutz, den das Markenrecht bietet, die wettbewerblichen Freiheiten anderer Parteien einschränkt. Schließlich würde ein markenrechtlicher Schutz des Begriffs „Webinar" bedeuten, dass konkurrierenden Anbietern die Möglichkeit genommen wird, zur Bewerbung der Veranstaltung einen eingängigen und von Interessenten bei der Suche oft eingegebenen Begriff zu nutzen. Diese Einschränkung anderer Parteien ist nur dadurch zu rechtfertigen, dass der Markeninhaber den von ihm geschützten Begriff auch tatsächlich verwendet. Nach § 26 MarkenG muss er die Marke in einer gewöhnlichen und wirtschaftlich sinnvollen Weise nutzen. Andernfalls kann er gemäß § 25 Abs. 1 MarkenG keine Schadensersatz- oder Unterlassungsansprüche gegen andere Verwender des Begriffs geltend machen.

III. Fazit für öffentliche Hochschulen und Forschungseinrichtungen

Aus der Eintragung des Begriffs „Webinar" lassen sich keine Ansprüche mehr gegen etwaige Verwender herleiten. Für die – gerade in der Zeit der Corona-Pandemie – zahlreich angebotenen Online-Veranstaltungen darf also sehr wohl mit dem Begriff „Webinar" geworben werden. Dies gilt für öffentliche Hochschulen und Forschungseinrichtungen umso mehr, da sie zumeist gar nicht erst im geschäftlichen Verkehr agieren und somit der markenrechtliche Schutzbereich schon nicht eröffnet ist.

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