„Weggeforscht“ der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht DFN

2 / 2024
Februar 2024

Blockst du mich, verklag‘ ich dich!

Das Oberlandesgericht Hamburg urteilt zur urheberrechtlichen Zulässigkeit von Adblockern

von Nicolas John

Digitale Anzeigen, Werbevideos vor den Hauptvideos oder Pop-Up-Werbungen kennt jede:r Internetnutzer:in. Aus ihrer Funktion heraus, nicht übersehen zu werden, sind sie meist „auffällig“ platziert. Doch während sich viele Internetnutzer:innen an den Werbeinhalten stören, sind Webseitenbetreibende regelmäßig auf sie angewiesen, um ihren Service günstig oder sogar kostenlos anbieten zu können. Daher ist es nicht verwunderlich, dass das verbreitete Blockieren der digitalen Werbung den Webseitenbetreibenden ein Dorn im Auge ist. Ein Fall dieser Adblocker ging zunächst vor das Landgericht Hamburg[1] und danach in Berufung vor dem Oberlandesgericht Hamburg[2].

I. Hintergrund

Für ein umfassendes Verständnis des Verfahrens ist zunächst grundlegend auf die Technik hinter der digitalen Werbeindustrie sowie auf die Funktionsweise der Blockade von Werbung einzugehen.

1. Werbung auf Webseiten anzeigen lassen

Wenn Webseitenbetreibende Werbung auf ihren Seiten anzeigen wollen, gibt es unterschiedliche Varianten, dies zu tun. Am einfachsten erscheint es, wenn die betreibende Person eine Werbeanzeige auf ihrer Webseite hochlädt und anschließend den Nutzer:innen anzeigt. Allerdings hat diese Form der digitalen Werbung einige Nachteile. Zum einen müssen Webseitenbetreibende sich um die Schaltung jeder Anzeige erneut kümmern. Soll also eine andere Anzeige geschaltet werden, müssen sie die alte entfernen, die neue auf ihrem Server hochladen und neu verknüpfen. Zum anderen bekommen mit dieser Art der Werbemaßnahmen alle Besuchenden der Webseite die gleiche Werbung angezeigt.

Um den Aufwand zu verringern und die Flexibilität zu erhöhen, bietet die Werbeindustrie den Webseitenbetreibenden ein anderes Modell an. Um eine Webseite über Werbung finanzieren zu können, ist es den Betreibenden möglich, einen zusätzlichen Code auf ihrer Webseite einzubinden, um Werbeanzeigen von einem Unternehmen anzeigen zu lassen. Die Werbeunternehmen haben Verträge mit den zu bewerbenden Unternehmen und leiten die Werbungen an die anzeigenden Webseitenbetreibenden weiter. An den Erlösen werden die Webseitenbetreibenden beteiligt. Auf diese Art müssen die Betreibenden nicht mehr selbst die einzelnen Werbeanzeigen schalten. Darüber hinaus lassen diese Werbetools oftmals eine personalisierte, auf die Nutzer:innen zugeschnittene Werbung zu. Damit die unterschiedliche Werbung angezeigt werden kann, greifen die Webseiten auf sog. „AdServer“ von den Werbeunternehmen zu.

2. Werbung auf Webseiten blockieren

Es gibt verschiedene Wege, Online-Werbung und Anzeigen auf Webseiten zu blockieren. Besonders genervte Nutzer:innen, die im heimischen Netzwerk umfassend blocken wollen, können beispielsweise auf „Pi-hole“ zurückgreifen. Dieses Open Source

1 LG Hamburg, Urt. v. 14.01.2022, Az. 308 O 130/19.

2 OLG Hamburg, Urt. v. 24.08.2023, Az. 5 U 20/22.

Programm leitet den Internetverkehr so um, dass Werbeanzeigen nach den Wünschen der Nutzer:innen ausgefiltert werden können. Doch ist der Einrichtungsaufwand bei diesen Programmen umfangreicher.

Wer nicht so viel Zeit in die Blockade von Werbung stecken möchte und nach Werbeblockern, sog. „Adblockern", sucht, wird auch mit einfachen Browser-Plugins fündig. Diese kleinen Zusatzprogramme können ohne großen Aufwand auf dem Computer im Browser installiert werden und arbeiten im Hintergrund, während die Nutzer:innen die Webseiten besuchen. Im nachfolgenden Verfahren ging es um ein solches Adblock-Browser-Plugin.

II. Sachverhalt

Im Verfahren vor dem Oberlandesgericht (OLG) Hamburg (Az.: 5 U 20/22) ist die Beklagte Vertreiberin eines Browser-Plugins zum Blockieren von Werbeanzeigen mit dem Namen „AdBlock Plus". Damit das Programm weiß, welche Anzeigen blockiert werden sollen, arbeitet es mit sog. Filterlisten. Diese enthalten, gespeichert in sog. „Blacklists", Serverpfade bestimmter Online-Server und deren AdServern, also den Servern, mithilfe derer Werbemittel auf Webseiten platziert werden können. Außerdem enthalten sie meist globale Dateimerkmale, durch welche eine große Anzahl von Seiteninhalten aufgrund von Gemeinsamkeiten mit anderen Webseiten blockiert werden können. Die Nutzung dieses Programms führt im Ergebnis dazu, dass die Webseiten auf dem Bildschirm der Nutzer:innen ohne die Werbeeinblendung der in der entsprechenden Blacklist eingetragenen Webseiten von den AdServern angezeigt werden können. Das Programm sorgt dabei auf zwei verschiedenen Wegen dafür, dass bestimmte, als Werbung erkannte Elemente, nicht angezeigt werden. Zum einen wird verhindert, dass die Werbeinhalte von den AdServern durch den Browser abgerufen werden. Die andere Alternative („Element Hiding") führt dazu, dass ein in den Arbeitsspeicher der Nutzer:innen geladenes Werbeelement nicht auf dem Monitor angezeigt, sondern unterdrückt wird.

Die Klägerin, ein Verlagshaus, ist Inhaberin mehrerer Webseiten, die umfangreich die Dienste von AdServern nutzen. Diese Adserver sind auch auf den durch das Programm „AdBlock Plus" genutzten Blacklists gespeichert. Hierdurch wird die Anzeige der Werbungen, wie von dem Plugin beabsichtigt, auf den Webseiten unterdrückt. Da durch die Nichtanzeige der Werbeeinblendungen den Webseitenbetreibenden meist die finanzielle Grundlage vieler Webseiten verloren geht, strebte die Klägerin gerichtliche Maßnahmen gegen die Vertreiberin (die Beklagte) des Programms an. Hierfür machte die Klägerin geltend, dass durch die Nutzung eines Adblockerprogramms Urheberrechtsverletzungen durch Umarbeitung oder Vervielfältigung begangen werden. Sie verlangte daher die Unterlassung der Blockierung der Werbeanzeigen auf ihren Webseiten.

III. Entscheidung

Das Verfahren wurde von der Beklagten zunächst vor dem Landgericht (LG) Hamburg geführt. Mit Urteil vom 14. Januar 2022 hatte zuerst das LG Hamburg (Az. 308 O 130/19) und nun in zweiter Instanz das OLG Hamburg verschiedene Aspekte der Klage thematisiert und schließlich abgewiesen (Urt. v. 24.8.2023, Az. 5 U 20/22).

1. Kein urheberrechtlich geschütztes Computerprogramm

Zuerst einmal könne nach Ansicht des OLG Hamburg offengelassen werden, ob die Dateien, die beim Abruf der Webseiten an die Nutzer:innen übermittelt werden, als Computerprogramm i. S. d. § 69a Urheberrechtsgesetzes (UrhG) geschützt sind. Es scheine laut Urteil allerdings zweifelhaft, denn für die urheberrechtliche Schutzfähigkeit eines Computerprogramms bedürfe es unter anderem der Feststellung, inwieweit das in Rede stehende Programm „keine ganz einfache handwerklich-technische Gestaltung aufweist". Zwar werde für komplexe Computerprogramme eine urheberrechtliche Schutzfähigkeit vermutet. Dies treffe wohl meist auf moderne Webseiten mit technisch voneinander abgrenzbaren Einzelelementen wie Bilder, Texte, Grafiken aber auch Software wie z. B. PHP-Code zu.

Ob aber durch den Einsatz von diesen Softwarebestandteilen in HTML-Dokumenten bei der Webseite insgesamt von einem Computerprogramm ausgegangen werden könne, wurde bislang nicht entschieden. Abzulehnen sei dies nach Ansicht des LG Hamburg und OLG Hamburg jedenfalls dann, wenn die Softwarebestandteile nicht „prägend für den Quellcode der Webseite" sind. Dies sei bei einem Eingriff in einen Programmschutz durch Werbeblocker meist nicht gegeben.

2. Keine unberechtigte Vervielfältigung

Auch liege nach Auffassung des OLG Hamburg keine unberechtigte Vervielfältigung nach dem Urheberrecht i. S. d. § 69c Nr. 1 UrhG vor. Zwar würden beim Abruf der Webseiten die HTML-Datei und weitere Informationen in den Arbeitsspeicher der Nutzer:innen geladen, allerdings erfolge diese Speicherung mit der Einwilligung der Webseitenbetreibenden. Wer eine Webseite bereitstelle, erkläre sich üblicherweise damit einverstanden, dass die entsprechenden Programme von den Servern der Webseitenbetreibenden oder auch Drittservern abgerufen und im Arbeitsspeicher der Nutzer:innen gespeichert würden. Das Anbieten von Webseiten sei gerade darauf ausgerichtet.

Ebenso seien die Nutzer:innen, die die Seite der Webseitenbetreibenden aufrufen und dabei das Adblockerprogramm nutzen, zur Speicherung der Dateien berechtigt. Es komme entweder eine stillschweigende Vereinbarung zwischen Nutzer:innen und Webseitenbetreibenden über die Speicherung der Dateien in Betracht oder eine sog. (schlichte) Einwilligung der Betreibenden. Von einer solchen sei laut der Rechtsprechung auszugehen, „wenn dem (schlüssigen) Verhalten des Berechtigten die objektive Erklärung entnommen werden kann, er sei mit der Nutzung seiner Werke einverstanden". Die freie Nutzung der durch die Webseitenbetreibenden angebotenen Dateien und Informationen ginge zwangsläufig mit einer Vervielfältigung im Arbeitsspeicher einher und sei im Ergebnis als erlaubte Nutzung anzusehen.

Dies gelte ebenso für jene Nutzer:innen, die Adblockerprogramme verwenden, da die Klägerin gerade keine technische Maßnahme getroffen hat, solche Nutzer:innen von dem Besuch der Webseite auszuschließen. Es handle sich daher stets um eine erlaubte Nutzung. Wenn jedoch ein Programm durch den Webseitenbetreibenden eingesetzt werde, durch das Nutzer:innen mit eingeschaltetem Adblockerprogramm von der Nutzung ausgeschlossen werden, fehle es an der Einwilligung. In einem solchen Fall unterbliebe dann allerdings auch die Vervielfältigung im Arbeitsspeicher, wodurch eine Rechtsverletzung ebenfalls ausgeschlossen sei.

3. Keine Umarbeitung

Außerdem stelle nach Ansicht des OLG Hamburg das anschließende Ausblenden der Werbeanzeigen keine Umarbeitung i. S. d. § 69c Nr. 2 UrhG dar. Zwar habe das Adblockerprogramm eine Auswirkung auf die Datenstruktur, die vom Browser erzeugt würde, es handle sich dabei aber nicht um Umarbeitungen i. S. d. Urheberrechts. Die übermittelten Dateien würden durch das Programm nicht geändert, es komme lediglich zu Eingriffen in den Ablauf des Programms. Diese seien jedoch nicht vom Begriff der Umarbeitung umfasst. Das einfache „Nichtladen" einzelner Funktionen oder Elemente eines Computerprogramms sei nicht als Umarbeitung anzusehen. Schlichte Beeinträchtigungen bzw. Abänderungen des vom Urheber angedachten Programmablaufs (bspw. durch das Nichtausführen von einzelnen Funktionen, also hier das Nichtladen der Werbeinhalte) fielen nicht in den Anwendungsbereich des Urheberrechts an Computerprogrammen, denn es werde damit nicht die „Ausdrucksform des Computerprogramms" beeinträchtigt.

4. Webseite ist kein geschütztes Werk

Zwar lässt das Gericht die Frage offen, ob mit der Webseite ein geschütztes Werk in Form eines sog. Multimediawerks vorliege. Diesbezüglich kam die klagende Partei ihrer verfahrensrechtlichen Darlegungslast nicht ausreichend nach. Allein aus dem vorgetragenen Umstand, dass Texte, Bilder, Grafiken oder Videos etc. kombiniert worden seien, folge jedoch nicht zwingend, dass die erforderliche „hinreichende Schöpfungshöhe" erreicht sei. Es sei nur als Standardlösung anzusehen.

Doch selbst bei der Annahme eines geschützten Werkes sei nach Auffassung des Gerichts die oben genannte (schlichte) Einwilligung der Webseitenbetreibenden zu beachten und ein möglicher Eingriff daher gerechtfertigt. Es liege somit auch an dieser Stelle keine Rechtsverletzung vor, welche einen Unterlassungsanspruch begründen könne.

IV. Fazit

Die Urteile des LG Hamburg sowie des OLG Hamburg zeigen anschaulich, dass die Verwendung von Adblocksoftware keine urheberrechtlich zu beanstandende Rechtsverletzung darstellt. Die Gerichte gehen dabei in ihren Urteilen auch tief auf die technische Ebenen des Webseiten- und Adblock-Aufbaus ein, um den Bogen zum Urheberrecht zu spannen.

Dennoch hat das OLG Hamburg leider die urheberrechtlich spannende Frage, ob die Webseite der Klägerin selbst als

urheberrechtlich schutzfähiges Werk angesehen werden kann, aufgrund des mangelnden Parteivortrags offengelassen. Klar ist aufgrund eines vergangenen Urteils des LG Hamburg lediglich, dass eigenständige Skripte innerhalb einer Webseite einen urheberrechtlichen Schutz beanspruchen können. Diese waren im vorliegenden Sachverhalt aber gerade nicht betroffen. Auch die in der juristischen Literatur diskutierte Möglichkeit, Webseiten als Datenbanken dem urheberrechtlichen Schutz zuzuführen, wird vom OLG Hamburg nicht aufgegriffen.

Darüber hinaus erinnert der Sachverhalt um die Nutzung von Adblocksoftware an die Verwendung von Cheatsoftware bei Computerspielen[3]. Doch während Adblockerprogramme nur auf den Programmablauf einwirken, greift eine Cheatsoftware unmittelbar in die Teile des Computerprogramms (das Computerspiel) ein. Auch wenn die urheberrechtliche Diskussion daher scheinbar mit ähnlichen Argumenten geführt wird, sind die Komplexe um Adblocksoftware und Cheatsoftware getrennt voneinander zu bewerten.

Obwohl das Urteil somit die Verwendung von Adblocksoftware in Form von Browser-Plugins als urheberrechtlich zulässig erachtet, bleibt weiterhin eine Vielzahl an relevanten Fragen offen, die auch für die Webpräsenz von Hochschulen und Forschungseinrichtungen Bedeutung entfalten können.

Im Übrigen ist das Verfahren mittlerweile vor dem Bundesgerichtshof (BGH) als Revisionsinstanz anhängig. Allerdings ist zu erwarten, dass er lediglich die im Verfahren aufgeworfenen Fragen thematisieren wird. Darüber hinausgehende Fragen werden wohl weiterhin noch nicht geklärt werden können.

3 Hierzu Palenberg, Cheat happens, DFN-Infobrief Recht 6/2023.

Die gewählte Rufnummer ist leider bereits vergeben

Der BGH zum Namensschutz bei Domaingrabbing

von Klaus Palenberg

Der Bundesgerichtshof (BGH, Urteil vom 26.10.2023 – I ZR 107/22) hat eine aktuelle Entscheidung zu den Voraussetzungen einer unberechtigten Namensanmaßung durch Registrierung und Nichtfreigabe einer Internetdomain gefällt. In Fällen des sogenannten „Domaingrabbings" geht es häufig um die Frage, wann die „Reservierung" einer Domain rechtsmissbräuchlich ist. Im vorliegenden Fall ging es dabei vor allem um die namensrechtlichen Probleme des Domaingrabbings. Gleichzeitig werden durch diesen Beitrag die marken- und wettbewerbsrechtlichen Fragen des Themas beleuchtet.

I. Das Geschäftsmodell „Domaingrabbing"

In Deutschland werden sämtliche Domains mit der Endung „.de" (de-Top-Level-Domain) von der DENIC eG verwaltet. Dadurch wird sichergestellt, dass es jede de-Domain nur einmal gibt. Diese Einzigartigkeit führt allerdings dazu, dass eine bestimmte Domain für Institutionen, die mit dieser Domain in Verbindung gebracht werden wollen, einen erheblichen Mehrwert darstellen kann. So hat beispielsweise der DFN-Verein ein großes Interesse daran, dass Nutzende bei Eingabe von „dfn.de" in ihren DNS-Resolver auf der Homepage des Deutschen Forschungsnetzes landen und nicht etwa auf der des Data Feminism Networks.

Dieses Bedürfnis wollen sich einige findige Geschäftsleute zunutze machen. Beim sogenannten „Domaingrabbing" werden bzw. wurden bestimmte Domains bei den zuständigen Stellen wie der DENIC registriert, um sie später weiterzuverkaufen. Dass dieses Geschäftsmodell tatsächlich trägt, zeigen einige spektakuläre Verkäufe von besonders eingängigen Domains. Der teuerste Verkauf einer Domain bis zum Jahr 2022 in Höhe von 30,18 Millionen Dollar wurde für die Domain „PrivateJet.com" getätigt.[1] Auch der zweithöchste Verkauf brachte 30 Millionen Dollar ein.[2] Unter den 30 teuersten Verkäufen aller Zeiten bis zum Jahr 2022 finden sich neben Firmennamen wie „Tesla" vor allem allgemeine Begriffe wie „Hotels", „Healthinsurance", „Toys" oder „Whisky".[3] Auch aktuell werden noch erkleckliche Beträge für Domains bezahlt. So wurde im Jahr 2022 für „call.com" noch ein Betrag in Höhe von 1,6 Millionen Dollar fällig.[4] De-Domains brachten im Jahr 2022 bis zu 163.740 Dollar („termin.de").[5]

1 https://de.statista.com/statistik/daten/studie/1351062/umfrage/die-teuersten-domains-aller-zeiten-weltweit/ (zuletzt abgerufen am 05.12.2023).

2 https://de.statista.com/statistik/daten/studie/1351062/umfrage/die-teuersten-domains-aller-zeiten-weltweit/ (zuletzt abgerufen am 05.12.2023).

3 https://de.statista.com/statistik/daten/studie/1351062/umfrage/die-teuersten-domains-aller-zeiten-weltweit/ (zuletzt abgerufen am 05.12.2023).

4 https://de.statista.com/statistik/daten/studie/169729/umfrage/top-10-der-teuersten-domainverkaeufe/ (zuletzt abgerufen am 05.12.2023).

5 https://de.statista.com/statistik/daten/studie/1329833/umfrage/teuerste-de-domains-in-deutschland/ (zuletzt abgerufen am 05.12.2023).

Doch auch abseits dieser besonders prägnanten Domains besteht ein bedeutender Absatzmarkt für Domains, sodass auch weiterhin viele Domains „reserviert" sind. Auch weniger aussagekräftige Domains, wie etwa „dl.de", brachten im Jahre 2022 immerhin noch bis zu 23.710 Dollar.[6] Dabei kostet eine Registrierung einer de-Domain laut DENIC-Preisliste vergleichsweise günstige 116 Euro, die Verwaltung für ein Jahr 58 Euro.[7]

II. Das Urteil des Bundesgerichtshofs

1. Der Hintergrund des Verfahrens

Angesichts dieser Preise und der damit unter Umständen überzogenen Erwartungshaltung bei den „Verkäufern" überrascht es nicht, dass immer wieder Fälle von Domaingrabbing vor den Gerichten landen. Dabei geht es aber in der Regel nicht um die aufgerufenen Preise der Domaingrabbenden, sondern vielmehr um Herausgabeansprüche an der streitigen Domain. So beanspruchen in der Regel Firmen oder Personen diejenigen Domains, die sich aus ihrem Namen bilden lassen.

2. Der Sachverhalt

So war es auch in dem vor dem BGH verhandelten Fall. Die Klägerin firmierte unter dem Namen „energy COLLECT GmbH & Co. KG" als Inkassodienstleister für Energieversorgungsunternehmen. Allerdings benutzte sie diesen Namen erst seit Sommer 2020. Bereits im April 2010 hatte aber der Beklagte, ein Rechtsanwalt, die Domains „energycollect.de" und „energy-collect.de" bei der DENIC auf seinen Namen registriert.

Diese Domains nutzte der Beklagte ausschließlich als Weiterleitung auf die Website eines Unternehmens, dessen Vorstand er war. Inhalte wurden unter den Domains nicht angezeigt. Das Unternehmen, auf dessen Website weitergeleitet wurde, war ebenfalls ein Inkassounternehmen für die Energieversorgungsbranche und firmierte unter dem Namen „on-collect solutions AG". Die URL der Website des Unternehmens lautete „www.on-collect.de".

3. Die Entscheidung

In der Entscheidung des BGHs ging es in erster Linie um namensrechtliche Ansprüche der Klägerin. Nach § 12 BGB kann jeder bei unbefugter Verwendung seines Namens durch einen anderen verlangen, dass diese Beeinträchtigung beseitigt wird und künftige Beeinträchtigungen unterlassen werden.
Dies setzte in diesem Fall voraus, dass der energy COLLECT GmbH & Co. KG ein Namensrecht zustand, was mit der hinreichenden originären Unterscheidungskraft des Firmenbestandteils „energy COLLECT" gegeben war.
Auch ein unbefugter Namensgebrauch durch den Beklagten bejahte der BGH. Ihm stehe kein eigenes Namens- oder Kennzeichenrecht an der Bezeichnung „energy COLLECT" zu. Denn ein solches folge nicht bereits aus der Registrierung der Domain. Das fremde Namensrecht der Klägerin gebrauchte der Beklagte, indem er die Registrierung der Domain mit dem fremden Namensbestandteil aufrechterhielt. Damit schließe er den eigentlichen Namensträger von der Nutzung seines eigenen Namens unter dieser Top-Level-Domain aus. Dieser Gebrauch erfolgte auch unbefugt, da der Namensträger diesen nicht gestattet hatte.
Durch die Registrierung einer Domain bei der DENIC wird lediglich ein schuldrechtliches Benutzungsrecht gegenüber der DENIC eG erworben. Nicht damit verbunden ist hingegen Eigentum oder ein sonstiges absolutes Recht, das ähnlich einer Inhaberschaft an einem Immaterialgüterrecht verdinglicht ist.

Dem Beklagten stehe nach Ansicht des BGHs auch deshalb kein eigenes Namensrecht an der Bezeichnung „energy COLLECT" zu, weil er die Domain allein zur Weiterleitung mittels URL-Redirect auf eine andere Seite benutzte. Darin sieht der BGH eine ausschließliche Nutzung als Adressbezeichnung ohne Kennzeichnungsfunktion. Wie eine Telefonnummer solle die so genutzte Domain zwar den Zugang zu der anderen Website eröffnen, ihn aber nicht namentlich bezeichnen. Zudem enthalte die Website keine Inhalte, sondern stelle allein eine Art technische Durchgangsstation dar, um auf die andere Website zu gelangen.

Dahingegen hätten Domainnamen, die zu einer mit Inhalten gefüllten, aktiv verwendeten Website führen, neben der Adressfunktion in der Regel auch eine Kennzeichnungsfunktion für die auf der Website angebotenen Waren und Dienstleistungen.
Durch die Weiterleitung auf eine Website eines anderen

6 https://de.statista.com/statistik/daten/studie/1329833/umfrage/teuerste-de-domains-in-deutschland/ (zuletzt abgerufen am 05.12.2023).

7 https://www.denic.de/preisliste (zuletzt abgerufen am 06.12.2023).

Unternehmens bei Eingabe der streitgegenständlichen Domain werde der eigentliche Namensträger, die Klägerin, mit der Website eines anderen Unternehmens in Verbindung gebracht, obwohl sie tatsächlich nichts mit ihr zu tun habe. Darin sieht der BGH hier eine Zuordnungsverwirrung.

Der eigentliche Knackpunkt in diesem Fall lag in der Tatsache begründet, dass die Klägerin ihre Firma erst circa zehn Jahre nach der Domainregistrierung durch den Kläger gewählt hatte. Dementsprechend gab es zum Zeitpunkt der Domainregistrierung auch kein entgegenstehendes Namensrecht der Klägerin.
Insofern war die Domainregistrierung im Jahre 2010 namensrechtlich unbedenklich. Problematisch war deshalb allein die Aufrechterhaltung der Registrierung bei der DENIC durch den Beklagten, also die Nichtfreigabe der Domain an die Klägerin. Diese Nichtfreigabe wäre wiederum unproblematisch gewesen, wenn der Beklagte die Domain auch aktiv genutzt hätte. Hätte er also eigene Inhalte auf der Website angeboten, die unter „energycollect.de“ erreichbar war, hätte er die Registrierung problemlos aufrechterhalten dürfen.

Da die Domain aber allein zur Weiterleitung genutzt wurde, stellte der BGH hier eine umfangreiche Abwägung der Interessen der Klägerin und des Beklagten an. Aufseiten der Klägerin sieht der BGH eine erhebliche Beeinträchtigung ihrer schutzwürdigen Interessen darin, dass die Internetadresse „energycollect.de“ nur einmal vergeben werden könne und damit bereits mit der Registrierung eine ausschließende Sperrwirkung eingetreten sei. Ohne eine Freigabe durch den Beklagten ist es der Klägerin nicht möglich, die von ihr gewünschte Domain für die Homepage ihres Unternehmens entsprechend ihres Firmennamens zu wählen.
Auf der anderen Seite habe aber auch der Beklagte mit der Registrierung der Domain eine gewisse Rechtsposition erlangt, die nun durch die Wahl des Firmennamens durch die Klägerin entfallen soll. Hinsichtlich dieser Rechtsposition stellt der BGH noch einmal klar, dass es sich dabei um ein relativ wirkendes vertragliches Nutzungsrecht handle. Das bedeutet, dass derjenige, der eine Domain bei der DENIC registriert, erwarten darf, dass er allein diese Domain benutzen darf und kein anderer sie ein zweites Mal registrieren darf. Dieses Nutzungsrecht ist zwar kein Eigentum, sei aber eine eigentumsfähige Rechtsposition des Domaininhabers, die nach Art. 14 Abs. 1 Satz 1 GG geschützt sei.
Deshalb seien die zu berücksichtigenden Interessen aufseiten des Domaininhabers auch nicht auf rein namens- oder kennzeichenrechtliche Interessen beschränkt, wenn diese Rechtsposition vor der Entstehung des widerstreitenden Namens- oder Kennzeichenrechts entstanden sei. Vielmehr spielen auch insbesondere wirtschaftliche Interessen des Domaininhabers eine maßgebliche Rolle.

So könne der Beklagte ein erhebliches Interesse an der weiteren Nutzung der Domain zur Weiterleitung allein deshalb haben, um damit die Trefferquote und das Ranking der Zielseite in Suchmaschinen zu erhöhen. Deshalb sei ein reiner Weiterleitungsgebrauch einer Domian nicht automatisch rechtsmissbräuchlich, sondern kann unter Umständen berechtigt sein.
Selbst die Registrierung und Aufrechterhaltung einer Domain allein mit einer Verkaufsabsicht (das eigentliche Domaingrabbing) hält der BGH für nicht ohne Weiteres rechtsmissbräuchlich. Der Handel mit Domainnamen sei grundsätzlich zulässig und somit grundrechtlich nach Art. 12, 14 GG geschützt und daher auch nicht rechtsmissbräuchlich, solange keine Namens- oder Kennzeichenrechte mit der Registrierung oder Nutzung verletzt werden.

In diesem Zusammenhang erinnert der BGH daran, dass derjenige, der einen Firmennamen als Unternehmenskennzeichen auswählt, sich vorab darüber informieren kann, ob eine entsprechende Domain bereits vergeben ist oder nicht. So könne er in der Regel ohne größere Probleme auch auf ein anderes Unternehmenskennzeichen oder eine andere Top-Level-Domain (wie etwa „.com“ oder „.net“) ausweichen.
Eine abschließende Entscheidung konnte der BGH in diesem Fall noch nicht treffen, weshalb er die Sache zur endgültigen Entscheidung an die Vorinstanz, in diesem Fall das Oberlandesgericht (OLG) Karlsruhe, zurückverwiesen hat.

Exkurs: Revisionsentscheidungen
Im deutschen Zivilprozessrecht wird bei Rechtsmitteln zwischen der Berufung und der Revision unterschieden. In einem Berufungsverfahren geht es häufig um Tatsachenfragen, sodass eine erneute Beweiserhebung z. B. durch Zeugenvernehmungen erfolgt. Bei einer Revision hingegen geht es allein um die Klärung von Rechtsfragen, wozu keine erneute Beweiserhebung nötig ist. Gerichtsverfahren, die vor dem BGH landen, wurden zuvor bereits in mindestens einer Instanz vor einem anderen Gericht verhandelt. Sämtliche Tatsachen, die für die vorherigen Gerichte entscheidend waren, sind also bereits geklärt. Deshalb verhandelt der BGH keine Berufungen, sondern Revisionen. Teilweise kann er sich in seinen Verfahren auf die bereits festgestellten Tatsachen berufen und Sachverhalte selbst abschließend bewerten. In anderen Fällen bleiben allerdings bestimmte Tatsachenfragen unbeantwortet, sodass der BGH noch keine

abschließende Entscheidung treffen kann. Dies ist insbesondere dann der Fall, wenn die Vorinstanz eine weitgehend abweichende Rechtsansicht im Vergleich zur Entscheidung in der Rechtsfrage durch den BGH vertreten hat. Dann sind auf einmal ganz andere Tatsachen für die endgültige Entscheidung wichtig als aus Sicht der Vorinstanz. Da diese aber nur die Tatsachenfragen geklärt hat, die sie für ihre Entscheidung beantwortet haben musste, und der BGH keine Tatsachenfragen klären darf, kann keine abschließende Entscheidung getroffen werden. In einem solchen Fall verweist der BGH den Fall zurück zur Vorinstanz, um die offenen Tatsachenfragen zu klären und anschließend, unter Berücksichtigung der Rechtsauffassung des BGHs, eine endgültige Entscheidung zu treffen.

Mit seiner Zurückverweisung an das OLG Karlsruhe hat er diesem dementsprechend seine Rechtsansicht für diesen Fall mit auf den Weg gegeben. Nach Ansicht des BGHs könne sich die Klägerin regelmäßig nicht auf ein schutzwürdiges Interesse berufen, da ihr Namens- und Kennzeichenrecht erst nach der Registrierung der Domain entstanden sei. Allein, falls aufseiten des Beklagten kein billigenswertes Benutzungsinteresse bestehe, könne ein Rechtsmissbrauch angenommen werden und sich das Namens- und Kennzeichenrecht der Klägerin durchsetzen. Dies sei angesichts der vom Beklagten geltend gemachten wirtschaftlichen Interessen nach derzeitigem Tatsachenstand zuungunsten des Beklagten nicht zu unterstellen.

Damit bleiben der Vorinstanz insbesondere zwei Dinge zur Klärung. Bestehen beim Beklagten tatsächlich weiterhin die geltend gemachten wirtschaftlichen Interessen an der Weiterleitung oder sind diese mittlerweile entfallen. Und zweitens, ob den Beklagten andere rechtsmissbräuchliche Motive getrieben haben, wodurch die Interessenabwägung zugunsten der Klägerin ausfallen könnte. Dies könnte etwa der Fall sein, wenn er die Domain allein aufrechterhielte, um die Klägerin in irgendeiner Form an der Ausübung ihrer Geschäfte zu hindern.

III. Weitere rechtliche Schutzmöglichkeiten gegen Domaingrabbing

Neben den soeben anhand des Urteils des BGHs dargestellten namens- und kennzeichenrechtlichen Schutzmöglichkeiten können sich auch Ansprüche aus anderen Rechtsgebieten im Zusammenhang mit Domaingrabbing ergeben.

1. Markenrechtlicher Schutz

Nach § 14 Abs. 2 Gesetz über den Schutz von Marken und sonstigen Kennzeichen (MarkenG) könnte sich für den Inhaber einer Marke[8] ein Herausgabe- bzw. Unterlassungsanspruch gegen den Domaininhaber ergeben. Hiernach ist es unter bestimmten Voraussetzungen für Dritte verboten, ein mit der Marke identisches oder ähnliches Zeichen im geschäftlichen Verkehr zu nutzen. Hierfür müsste allerdings das Zeichen für diejenigen Waren oder Dienstleistungen genutzt werden, die mit denjenigen Waren oder Dienstleistungen identisch oder ähnlich sind, für die die Marke eingetragen wurde, sodass Verwechslungsgefahr besteht (§ 14 Abs. 2 Nr. 1, Nr. 2 MarkenG). Für Domains bedeutet dies, dass die bloße Registrierung einer Domain oder die Nutzung derselben ohne Bezug zu den Waren und Dienstleistungen des Markeninhabers keine markenrechtliche Verletzungshandlung darstellt. Eine solche liegt lediglich vor, wenn die Domain für ähnliche Dienstleistungen genutzt wird wie die eingetragene Marke und hierdurch eine Verwechslungsgefahr besteht.

2. Sittenwidrige Schädigung durch Domaingrabbing

Ein Anspruch gem. §§ 826, 226, 1004 BGB kann insbesondere auch beim Domaingrabbing zum Tragen kommen. Dazu müsste in dem Verhalten des Domaininhabers eine vorsätzliche sittenwidrige Schädigung gegenüber dem Domaininteressenten zu sehen sein. Allerdings ist nicht jede Registrierung eines Domainnamens ohne Nutzungsabsicht automatisch sittenwidrig. Insbesondere Gattungsbegriffe (z. B. „Welt“ oder auch „Mahngericht“) sind als Domainnamen grundsätzlich keinen rechtlichen Schranken unterworfen. Es gilt insoweit allein das Prinzip der Priorität: Der Vorteil, der demjenigen zukommt, der als erster die Registrierung eines beschreibenden Domainnamens erwirkt, kann nicht als sittenwidrig angesehen werden.

Die Sittenwidrigkeit kann sich aber in Ausnahmefällen aus dem Hinzukommen anderer Umstände ergeben, etwa wenn die

8 Zu den rechtlichen Voraussetzungen zur Eintragung einer Marke siehe bereits Uphues, Du bist mir ja ‚ne Marke!, DFN-Infobrief Recht 08/2019.

Reservierung der Domain vorrangig mit Behinderungszweck erfolgt und ein eigenes schützenswertes Interesse des Reservierenden nicht erkennbar ist. Das Oberlandesgericht München (OLG München, Urteil vom 2.4.1998, Az.: 6 U 4798/97) hat den Willen zur Behinderung eines Dritten etwa für den Fall bejaht, dass jemand mehrere reservierte Domains besitzt, die gleichwohl allesamt seit mehreren Jahren noch ohne Inhalt sind, sodass er die eine umstrittene ohne Weiteres freigeben könnte, dies aber wegen der vom ihm gewünschten Sperrwirkung nicht tut.

3. Wettbewerbsverstoß bei Domaingrabbing

In Betracht kommt daneben auch ein wettbewerbsrechtlicher Anspruch nach §§ 3 i.V.m. 4 Nr. 4 Gesetz gegen den unlauteren Wettbewerb (UWG). Dieser setzt eine unlautere geschäftliche Handlung voraus. Eine solche liegt insbesondere vor, wenn ein Mitbewerber gezielt behindert wird.

Eine Behinderung i. S. d. § 4 Nr. 4 UWG kann sich bereits daraus ergeben, dass die gewünschte Top-Level-Domain nicht bei der DENIC registriert werden kann. Allerdings gilt dies nur bei unterscheidungskräftigen Domainnamen und nicht bei Gattungsbegriffen.

Ob diese Behinderung gezielt i. S. d. § 4 Nr. 4 UWG erfolgt, bestimmt sich danach, ob die Registrierung und das Halten des Domainnamens rechtsmissbräuchlich erfolgt. Hierzu reicht es nicht aus, dass der Anmelder die Domain allein zu dem Zweck registriert hat, sie später im Wege einer Lizenzerteilung oder einer Übertragung weiterzugeben. Dies ist insbesondere der Fall, wenn das entsprechende Unternehmenskennzeichen erst nach der Registrierung in Gebrauch genommen wurde. Vielmehr kommt es auf eine Abwägung der Interessen im Einzelfall an. Sie kommt aber beispielsweise in Betracht, wenn sich der Mitbewerber extra verschiedene Schreibweisen einer Unternehmensbezeichnung registrieren lässt.

4. Gemeinsamkeiten

Sämtliche Ansprüche gegen das Domaingrabbing haben eine Gemeinsamkeit. Soweit die rechtsgebietsspezifischen Voraussetzungen vorliegen, bedarf es zusätzlich eines rechtsmissbräuchlichen Verhaltens. Daher muss die Registrierung ein vorwerfbares Verhalten darstellen, mit dem der Domaininhaber die Domaininteressenten bewusst schädigen oder sie behindern möchte. Eine reine Gewinnerzielungsabsicht durch den Weiterverkauf einer Domain genügt da nicht. Erst wenn daneben noch weitere Umstände treten, hat ein Vorgehen gegen Domaingrabbende Aussicht auf Erfolg.

IV. Folgen für die Hochschulen

Im Falle einer Unternehmensgründung oder auch beim Start eines neuen Projekts stellt sich den verantwortlichen Personen die Frage nach dem Namen. Dabei sollte auch stets die Vermarktung im Internet mitberücksichtigt werden. Zentrales Element in diesem Zusammenhang ist die Wahl einer ansprechenden, aber zugleich aussagekräftigen Domain, die bestenfalls auch gleich den Namen des Unternehmens/Projekts beinhaltet. Dabei sollte sich nicht darauf verlassen werden, die passende Domain nach der Gründung dann auch bei der DENIC registrieren lassen zu können. Tatsächlich ist es nicht unwahrscheinlich, dass gerade die gewünschte Domain bereits vergeben ist. Wie die obige Darstellung zeigt, gibt es in diesen Fällen oftmals auch keine Möglichkeiten, die Freigabe gerichtlich zu erzwingen.

Deshalb sollte die Wahl der Domain bereits bei der Namenssuche mitbedacht werden und bestenfalls aufeinander abgestimmt sein. Dafür ist eine vorherige Abfrage bei der DENIC möglich, um zu klären, ob die gewünschte Domain noch verfügbar ist. Dabei kann es sich unter Umständen lohnen, sich selbst frühzeitig die entsprechenden Domains zu reservieren. Dies ist im Zweifelsfall deutlich günstiger, als die Domain im Nachhinein einer/m Domaingrabbenden teuer abzukaufen.
Steht der Name des Unternehmens oder Projekts bereits fest und stellt sich dann heraus, dass die entsprechende Domain bereits vergeben ist, kann anhand der oben dargestellten Maßstäbe im Einzelfall geprüft werden, ob eine Freigabe ausnahmsweise doch gerichtlich erzwungen werden kann. Hierbei sind die Gesamtumstände insbesondere aufseiten der Domaingrabbenden zu betrachten und festzustellen, ob sich hieraus ein Rechtsmissbrauch ableiten lässt.
Alternativ bietet auch die DENIC den sogenannten DISPUTE-Eintrag gegen rechtswidriges Domaingrabbing als Schutzmöglichkeit an. Dabei weist sie jedoch daraufhin, dass dieses Verfahren nicht dazu führt, dass der Antragsteller unmittelbar Inhaber der entsprechenden Domain wird. Vielmehr verhindert dieses Verfahren in erster Linie, dass der bisherige Domaininhaber die Domain auf einen anderen übertragen kann.

Vertrauen ist gut – Überwachung ist besser?

Chatkontrolle zur Bekämpfung des sexuellen Missbrauchs von Kindern

Von Johanna Voget

Der Vorschlag der Europäischen (EU) Kommission für eine Verordnung zur „Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern“[1] löste eine Flutwelle an Debatten aus. Die Auseinandersetzung zieht sich nunmehr bereits seit 18 Monaten in die Länge, eine Einigung ist nicht in Sicht. Zuletzt hat der EU-Innenausschuss im November 2023 gegen den Entwurf in seiner ursprünglichen Form gestimmt.[2] Dieser Beitrag widmet sich dem Hintergrund des Gesetzgebungsvorhabens, seiner Ausgestaltung und der formellen sowie materiellen Kritik daran.

I. Hintergrund des Vorschlags

Eingebracht wurde der Verordnungsentwurf zur Eindämmung des sexuellen Missbrauchs von Kindern bereits im Jahr 2022 von EU-Innenkommissarin Ylva Johansson. Grund für das Gesetzgebungsvorhaben ist, dass allein 2021 weltweit 85 Millionen Bilder und Videos registriert worden sein sollen, die sexuellen Missbrauch von Kindern darstellen. Die Kommission geht zudem von einer wesentlich höheren Dunkelziffer aus. Hinzu kommt die begründete Vermutung, dass die Fälle von sexuellem Missbrauch an Kindern während der Pandemie signifikant zugenommen haben. Unter Verweis auf Angaben der Internet Watch Foundation nimmt die Kommission für das Jahr 2021 – im Vergleich zum Vorjahreswert – einen Anstieg um 64 Prozent an.[3]

II. Regelungen des Entwurfs

Der Vorschlag beinhaltet zunächst die Gründung eines eigenständigen EU-Zentrums für die Verhütung und Bekämpfung sexuellen Kindesmissbrauchs in Den Haag, das mit den nationalen Behörden in der Durchführung und Durchsetzung des materiellen Rechts eng zusammenarbeiten soll.[4]

Inhaltlich sieht der Vorschlag eine Reihe von Pflichten für die Anbieter von Hosting- und Kommunikationsdiensten vor. Diese reichen von umfänglichen Pflichten zu Risikoanalyse, Risikominimierung und Risikoberichten über die Detektion und Meldung bis hin zur Entfernung von „child sexual abuse material“ und der Zugangssperrung als ultima ratio. Der Anwendungsbereich erfasst nicht nur (audio-)visuelle Darstellungen des Missbrauchs, sondern schließt auch die Anbahnung zu sexuellen Zwecken, das sogenannte Grooming, als Vorstufe ein.

Als kindesmissbräuchlich identifizierte Nachrichten sollen für eine Verdachtsprüfung an das neue EU-Zentrum weitergeleitet werden. Das EU-Zentrum wiederum prüft die Meldungen und leitet bei weiterer Bestätigung des Verdachts die Informationen an Europol oder nationale Sicherheitsbehörden weiter.[5]

---

1 COM (2022) 209 final.

2 https://www.tagesschau.de/ausland/europa/chatkontrolle-eu-kindesmissbrauch-102.html (zuletzt abgerufen am 18.12.2023).

3 Vgl. zu den Zahlen und Fakten: ZD-Aktuell 2022, 01251.

4 ZRP 2022, 191 (191).

5 ZRP 2022, 191.

Internet-Dienste wie Messenger, z. B. WhatsApp oder Signal, E-Mail-Provider oder Social-Media-Plattformen sollen danach gesetzlich gezwungen werden, die privaten Inhalte ihrer Nutzenden zu scannen und darin nach Darstellungen von Missbrauch zu suchen.[6]

Fachleute gehen davon aus, dass das sogenannte „Client-Side-Scanning" die einzige technische Möglichkeit bleibt, mit der Anbieter die Vorschläge der EU umsetzen können. Dabei werden Inhalte von Nachrichten direkt auf dem Gerät gescannt – noch bevor sie verschlüsselt verschickt werden.[7]

Im Ergebnis wäre also die digitale Kommunikation sämtlicher Nutzender unterschiedslos und verdachtsunabhängig von einer Überwachung betroffen. Erfasst wären jegliche Informationen – auch sensible Daten – aus allen Lebensbereichen der Nutzenden. Anbieter müssten dafür sorgen, dass die mittlerweile für private Kommunikation weitgehend etablierte Ende-zu-Ende-Verschlüsselung aufgebrochen wird.

III. Kritik

1. Materielle Kritik

Der Vorschlag wird in breiten Kreisen – insbesondere unter Beachtung der bisherigen Rechtsprechung des EuGHs zur Vorratsdatenspeicherung – für grundrechtswidrig gehalten.[8] Bedenken bestehen insbesondere hinsichtlich der Art. 7, 8 und 11 der gem. Art. 51 Abs. 1 anwendbaren Grundrechtscharta (GRCh). [9]

Kritik wurde bereits vor Veröffentlichung des Vorschlags laut: Am 17.3.2022 wurde ein offener Brief an die politisch Verantwortlichen adressiert, der von dutzenden namhaften Vereinigungen wie etwa der European Digital Rights (EDRi), dem Deutschen Anwaltverein (DAV) oder der Deutschen Vereinigung für Datenschutz (DVD) unterschrieben wurde.[10]
Der DAV befürchtet zum Beispiel „fatale Folgen für den Berufsgeheimnisschutz", da auch etwa die sichere und vertrauliche Kommunikation von Anwält:innen und Mandant:innen nicht mehr gewährleistet werden könnte. Zudem stelle der Vorschlag ein Sicherheitsrisiko dar, da die Mechanismen zur Entschlüsselung und dem Auslesen von Inhalten auch von kriminellen Dritten ausgenutzt oder Geräte kompromittiert werden könnten. Die tatsächlichen Gefährder könnten hingegen einfach ins unkontrollierte Darknet ausweichen.

Die Datenschutzkonferenz (DSK) hat darauf hingewiesen, dass es sich bei der vorgesehenen Chatkontrolle um eine unverhältnismäßige und anlasslose Massenüberwachung handele, die nicht mit den Grundrechten auf Achtung des Privat- und Familienlebens, der Vertraulichkeit der Kommunikation und zum Schutz personenbezogener Daten vereinbar sei.[11]

Breite Kritik am Vorhaben wird auch von Kinderschutzexpert:innen, Betroffenen von Kindesmissbrauch, Vertreter:innen der Polizei, europäischen Regierungen, UN-Beamten, Wissenschaft, Unternehmen, Wirtschaftsverbänden sowie Nichtregierungsorganisationen geäußert.[12]

Grund dafür ist insbesondere die prognostizierte Fehlerquote von etwa drei bis fünf Prozent bei strafrechtlich relevanten Meldungen sowie von zwölf Prozent bei Scans auf „Grooming-Inhalten".[13]

---

6 https://netzpolitik.org/2023/chatkontrolle-abstimmung-auch-im-eu-innenausschuss-verschoben/?via=nl#netzpolitik-pw (zuletzt abgerufen am 18.12.2023).

7 https://netzpolitik.org/2023/anlasslose-massenueberwachung-deutsche-datenschutzkonferenz-lehnt-chatkontrolle-rundweg-ab/?via=nl#netzpolitik-pw (zuletzt abgerufen am 18.12.2023).

8 ZRP 2022, 191 (191); ZD-Aktuell 2022, 01240.

9 ZRP 2022, 191 (192).

10 https://edri.org/wp-content/uploads/2022/03/Civil-society-open-letter-Protecting-rights-and-freedoms-in-the-upcoming-legislation-to-effectively-tackle-child-abuse.pdf (zuletzt abgerufen am 18.12.2023).

11 https://netzpolitik.org/2023/anlasslose-massenueberwachung-deutsche-datenschutzkonferenz-lehnt-chatkontrolle-rundweg-ab/?via=nl#netzpolitik-pw (zuletzt abgerufen am 18.12.2023).

12 https://netzpolitik.org/2023/chatkontrolle-abstimmung-auch-im-eu-innenausschuss-verschoben/?via=nl#netzpolitik-pw (zuletzt abgerufen am 18.12.2023).

13 becklink 2025720.

Sämtliche Internetnutzende stünden durch den Vorschlag unter Generalverdacht und die große Zahl an Falschmeldungen drohe die Ermittlungsarbeit der Strafverfolgungsbehörden wesentlich zu beeinträchtigen. Zukünftig könnte die Fehlerquote durch eine KI-basierte Chatkontrolle reduziert werden, die nach dem gegenwärtigen Stand der Technik jedoch noch nicht umsetzbar sei.[14] Daher stelle sich die Chatkontrolle für die tatsächlichen Ermittlungen zur Verhinderung und Verfolgung von Kindesmissbrauch letztlich als ein ungeeignetes Werkzeug dar.[15]

Angesichts der heftigen Kritik lehnen mittlerweile sämtliche ressortzuständigen Bundesministerien den Vorschlag zur Chatkontrolle ab.[16]

Dabei bezieht sich der Gegenwind jedoch in erster Linie auf die vorgeschlagenen Mechanismen (Chatkontrolle), die Einrichtung einer europäischen Behörde wird insbesondere auch vom Kinderschutzbund Bundesverband begrüßt.[17]

Die EU-Innenkommissarin verteidigt den Entwurf mit dem Zweck und der Wirkung der geplanten Schutzmaßnahmen. Der Wissenschaftliche Dienst kam hingegen in einer Untersuchung zu dem Ergebnis, dass die Wirkungen nicht so weitreichend wären, wie von Johansson wohl angenommen.[18]

2. Formelle Kritik

Auch das Vorgehen im Rahmen des bisherigen Gesetzgebungsverfahrens, insbesondere durch Ylva Johansson selbst, steht in der Kritik.

So soll sie in Verbindung zu Lobbyverbänden, die sich aufgrund von wirtschaftlichen Interessen für die Einführung der Chatkontrolle einsetzen, stehen. Dieser Vorwurf basiert darauf, dass sie sich bei einer Werbeaktion einer Lobbyorganisation als Unterstützerin auf einem Pressefoto gezeigt hatte. Darüber hinaus ist ein mit der Chatkontrolle befasster Mitarbeiter von Johansson gleichzeitig Mitglied in einer dieser Organisationen.

Aus diesem Grund soll auch die einbezogene Expertise bei der Erarbeitung der Verordnung sehr einseitig gewesen sein. Während nur wenige Vertreter:innen der Wissenschaft beteiligt wurden, sollen viele Vorschläge vonseiten der umstrittenen Organisation „Thorn“ eingebracht worden sein. „Thorn“ verkauft unter anderem Software zur Erkennung von Dateien, die Darstellungen von sexualisierter Gewalt zeigen.[19]

Darüber hinaus wird ihr vorgeworfen, im September 2023 Werbung für die Verordnung auf Twitter/X durch sog. „politisches Microtargeting“ betrieben zu haben.[20] Diesbezüglich hat der EU-Datenschutzbeauftragte eine Voruntersuchung eingeleitet.

IV. Aktueller Stand und Änderungsvorschläge

Für das Zustandekommen des Gesetzgebungsvorhabens ist eine Einigung von EU-Parlament, Ministerrat und der EU-Kommission auf eine gemeinsame Position erforderlich.

Der Ausschuss für bürgerliche Freiheiten (LIBE) im EU-Parlament hat daher im Oktober einen Kompromissvorschlag auf den Weg gebracht.[21]

Dieser sieht zunächst zentral vor, dass die Aufdeckungsanordnungen an Anbieter von Kommunikations- und Hostingdiensten zum Scannen der Inhalte ihrer Nutzenden nach Hinweisen auf

14 ZRP 2022, 191 (193).

15 becklink 2026110.

16 becklink 2024976; ZRP 2022, 191 (191).

17 becklink 2026308.

18 becklink 2026754.

19 https://netzpolitik.org/2023/geheime-liste-wie-der-sicherheitsapparat-die-chatkontrolle-praegt/ (zuletzt abgerufen am 18.12.2023).

20 Microtargeting ist eine umstrittene Werbemethode, die die EU-Kommission selbst strenger regulieren will, dazu: https://netzpolitik.org/2022/politische-werbung-die-zukunft-des-microtargeting-in-der-eu/#netzpolitik-pw (zuletzt abgerufen am 18.12.2023).

21 https://netzpolitik.org/2023/einigung-im-eu-parlament-steht-bevor-chatkontrolle-nur-bei-verdacht/?via=nl#netzpolitik-pw (zuletzt abgerufen am 18.12.2023).

Darstellungen sexualisierter Gewalt gegen Kinder und Anbahnungsversuche einem Richtervorbehalt unterliegen sollen.

Darüber hinaus sollen solche Anordnungen nur noch für spezifische Gruppen von Nutzenden – etwa bei Chatgruppen – möglich sein und den begründeten Verdacht erfordern, dass eine Verbindung zu Missbrauchsmaterial besteht.

Des Weiteren soll die Kommunikation, bei der eine „Ende-zu-Ende-Verschlüsselung" eingesetzt wurde, von der Chatkontrolle ausgenommen sein.

Im Rat der EU-Mitgliedstaaten zeichnet sich allerdings auch unter Berücksichtigung des Kompromissvorschlags noch keine Einigung ab.[22]

Nach aktuellen Angaben zweifelt das EU-Parlament nun an einem rechtzeitigen Zustandekommen des geplanten Vorhabens.[23] Die derzeitigen Übergangsregelungen zum freiwilligen Scannen nach Inhalten sexualisierter Gewalt gegen Kinder laufen zum 3. August 2024 aus. Die EU-Kommission hat daher vorgeschlagen, diese um zwei Jahre zu verlängern. Die Regelungen erlauben es, dass Plattformen wie Facebook oder Anbieter von Cloudspeichern freiwillig nach „bekanntem" Material suchen.

V. Bedeutung für Hochschulen und Forschungseinrichtungen

Das Vorhaben betrifft auch Hochschulen und Forschungseinrichtungen insofern, als dass jegliche Kommunikation der Studierenden, Lehrenden und Mitarbeitenden von der Chatkontrolle in seiner ursprünglich vorgeschlagenen Form erfasst wäre. Gerade im Gesundheitssektor, zum Beispiel in Fällen digitaler Sprechstunden beim Arzt, kann durch den Austausch von Abbildungen von Körperteilen ein Fall von unbekanntem Material, der in die Fehlerquote der Kontrolle eingeht, begründet werden. Es bleibt abzuwarten, in welcher Form die Chatkontrolle in diesem Jahr Eingang in die Praxis findet und welche Auswirkungen sie zeitigt.

22 https://netzpolitik.org/2023/einigung-im-eu-parlament-steht-bevor-chatkontrolle-nur-bei-verdacht/?via=nl#netzpolitik-pw (zuletzt abgerufen am 18.12.2023).

23 https://netzpolitik.org/2023/chatkontrolle-eu-kommission-zweifelt-an-einigung-und-geht-mit-zwischenloesung-in-die-verlaengerung/ (zuletzt abgerufen am 18.12.2023).

DFN Infobrief-Recht-Aktuell

Digital Services Act:

Ab dem 17. Februar 2024 wird der Digital Services Act (DSA) volle Gültigkeit beanspruchen. Schon seit dem 16. November 2022 sind Regelungen des DSA in Kraft. Inhaltich werden Neuregelungen zur Haftungsprivilegierung von Internetprovidern und Dienste-anbietern eintreten sowie Bestimmungen, die zu einer größeren Transparenz und Sorgfalt im Umgang mit sozialen Netzwerken führen sollen. Neu ist dabei u.a. die Schaffung eines Digitalen-Dienste-Koordinators in jedem Mitgliedstaat. Die Bundesnetzagentur ist als zentrale Koordinierungsstelle für die digitalen Dienste in Deutschland vorgesehen.

Digitale-Dienste-Gesetz:

Durch den Entwurf des Digitale-Dienste-Gesetzes (DDG) sollen die Vorgaben des DSA auf nationaler Ebene umgesetzt werden. Dabei werden bisher geltende nationale Regelungen, die in Zukunft aufgrund der Bestimmungen des DSA neu auszurichten sind, abgelöst. Das DDG soll parallel zum DSA für den 17. Februar 2024 in Kraft treten.

EUid-Brieftasche:

Der Europäische Rat und das Parlament haben sich im November vorläufig über eine europäische Identität (eID) geeinigt. Die Verordnung wurde mit dem Ziel überarbeitet, einen sicheren und vertrauenswürdigen Zugang öffentlicher und privater Online-Dienste mit der EUid-Brieftasche zu nutzen. Der digitale Führerschein, ärztliche Rezepte und die Möglichkeit der Kontoeröffnung können dadurch verwaltet werden.

Hier erhalten Sie den Link zur Presserklärung:
https://www.consilium.europa.eu/de/press/press-releases/2023/11/08/european-digital-identity-council-and-parliament-reach-a-provisional-agreement-on-eid

EuGH vom 21. Dezember 2023: Zum Umgang mit Gesundheitsdaten, die durch den Arbeitgeber erhoben werden und damit verbundenen Schadensersatzansprüchen

Gesundheitsdaten, die im arbeitsrechtlichen Zusammenhang erhoben werden, unterliegen einem erhöhten Schutz. Die Ausnahmeregelungen des Art. 9 Abs. 2 DSGVO sind anwendbar. Ein bei der Verarbeitung dieser Daten entstehender Schadensersatzanspruch nach DSGVO soll jedoch nicht eine Bestrafungsfunktion beinhalten, sondern als Ausgleich dienen.

Nachfolgend erhalten Sie den Link zur Entscheidung:
https://curia.europa.eu/juris/document/document.jsf?text=&docid=280768&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=8124112

Kurzbeitrag: Auftragsverarbeitungsvereinbarung, wechsle dich!

Berliner Datenschutzbehörde erklärt die Nutzung von Cisco Webex seitens der FU Berlin nun doch für zulässig

von Klaus Palenberg

Noch 2022 hatte der Berliner Datenschutzbeauftragte der Freien Universität Berlin (FU Berlin) die Nutzung der Videokonferenzplattform Webex des US-Konzerns Cisco untersagt. Nach vertraglichen Anpassungen und einem Personalwechsel bei der Datenschutzbehörde hat die neue Berliner Datenschutzbeauftragte nun aber keine Einwände mehr gegen die Weiterverwendung der Software.

I. Probleme bei der Nutzung von Cisco Webex

Die Frage, ob und wie Software von US-Konzernen in der Europäischen Union datenschutzkonform genutzt werden kann, beschäftigt die nationalen und europäischen Datenschutzbehörden schon seit längerem. Nachdem die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) bereits 2020 eine Orientierungshilfe zur datenschutzkonformen Nutzung von Videokonferenzsystemen veröffentlichte,[1] geriet auch das Videokonferenzportal Webex des US-Konzerns Cisco in den Blick der Datenschutzaufsichtsbehörden. Die Anbieter gelten nämlich, sofern sie personenbezogene Daten verarbeiten, als Auftragsverarbeiter i. S. d. DSGVO.

Daraus folgt, dass die Verantwortlichen, also öffentliche und nicht-öffentliche Stellen, die deren Angebote nutzen wollen, mit den Anbietern eine Auftragsverarbeitungsvereinbarung treffen müssen. Schließlich sind die Verantwortlichen nach Art 5 Abs. 2 DSGVO für die datenschutzkonforme Datenverarbeitung rechenschaftspflichtig und müssen, auch etwa durch die Auswahl ihrer Auftragsverarbeiter, die Einhaltung der gesetzlichen Vorschriften gewährleisten. Die Anbieter, wie beispielsweise Cisco, nutzen zu diesem Zweck Standard-Auftragsverarbeitungsvereinbarungen. Diese sind jedoch nach Ansicht einiger Datenschutzaufsichtsbehörden nicht mit der DSGVO vereinbar, da es ihnen insbesondere an Transparenz hinsichtlich der Datenverarbeitung für eigene Zwecke mangele. Um die Systeme datenschutzkonform nutzen zu können, bedarf es deshalb Vereinbarungen zwischen den Verantwortlichen und den Auftragsverarbeitern, die von den Standard-Vereinbarungen abweichen. Dass solche abweichenden Vereinbarungen möglich sind und Erfolg haben können, bewiesen kürzlich Cisco und die FU Berlin.

II. Die Nutzung von Cisco Webex an der FU Berlin

Schon seit 2020 nutzt die FU Berlin für hybride Formate in Lehre, Forschung und Verwaltung das Videokonferenzportal Webex. 2021 kamen allerdings datenschutzrechtliche Bedenken bezüglich dieser Praxis auf. Der damalige kommissarische Landesdatenschutzbeauftragte Volker Brozio kam zu dem Ergebnis, dass der Einsatz der Software umgehend zu stoppen sei. Zu diesem Zeitpunkt habe es keine rechtskonforme Möglichkeit zum Betrieb des Systems gegeben, obwohl die Hochschule nach eigener Aussage damals bereits diverse Maßnahmen für einen sicheren Einsatz der Videokonferenzsoftware ergriffen habe. Seit diesem Zeitpunkt verhandelten die FU Berlin, Cisco und die Berliner Datenschutzaufsichtsbehörde, unter welchen

1 https://www.tlfdi.de/fileadmin/tlfdi/gesetze/orientierungshilfen/oh-videokonferenzsysteme_final.pdf (zuletzt abgerufen am 18.12.2023).

Bedingungen ein Einsatz von Webex möglich sei. Zuletzt hatte der damalige Berliner Landesdatenschutzbeauftragte noch im August 2022 die FU Berlin aufgefordert, die Nutzung von Cisco Webex umgehend zu beenden.[2]

Im November 2023 hat nun die neue Berliner Datenschutzbeauftragte Meike Kamp das Verfahren abgeschlossen und kommt zu dem Schluss, dass der Einsatz von Cisco Webex seitens der FU Berlin nach zähem Ringen doch zulässig sei.[3] Diese veränderte Beurteilung der Datenschutzkonformität begründet sie insbesondere damit, dass die FU Berlin die vertragliche Auftragsverarbeitungsvereinbarung mit Cisco angepasst habe. So beruhe die aktuelle Datenverarbeitung durch Cisco auf einer neu verhandelten vertraglichen Grundlage, die unter anderem eine Übertragung von personenbezogenen Daten der Nutzenden an Cisco ausschließe. Zudem sei nach intensiver Prüfung und auch bei einem Vor-Ort-Termin bei der FU Berlin keine unzulässige Offenlegung personenbezogener Daten von den Nutzenden festgestellt worden. Die Berliner Landesdatenschutzbeauftragte beurteilt daher die zuvor festgestellten datenschutzrechtlichen und technischen Defizite als beseitigt. Auch der Europäische Datenschutzbeauftragte (EDSB) erklärte die angepasste Nutzung bereits im Juli für vereinbar mit den rechtlichen Vorgaben nach der DSGVO. Der US-Konzern Cisco selbst brüstet sich mit seinen datenschutzrechtlichen Anstrengungen der vergangenen Jahre. So sei es bei dem System etwa möglich, die Daten vollständig in der EU zu halten.

Ganz ohne Gegenstimmen bleibt die neue Auftragsverarbeitungsvereinbarung zwischen der FU Berlin und Cisco jedoch nicht. Der Allgemeine Studierendenausschuss (AStA) der FU Berlin, der auch schon zuvor auf einen Wechsel zu datensparsameren Alternativen wie Jitsi oder Big Blue Button gedrängt hatte, hält weiterhin die Nutzung von datenschutzfreundlicheren Open-Source-Angeboten für angebracht.[4] Auf eine diesbezügliche Nachfrage des AStAs verwies die Berliner Datenschutzbehörde auf das Fehlen einer dahingehenden rechtlichen Verpflichtung der FU Berlin und auf ihr eigenes Ermessen hinsichtlich des datenschutzrechtlichen Prüfungsumfangs.

III. Bedeutung für Hochschulen

Die Anpassung der Auftragsverarbeitungsvereinbarung zwischen Cisco und der FU Berlin und die Entscheidung der Berliner Landesdatenschutzbeauftragten zeigt, dass Software von US-Anbietern von Hochschulen in datenschutzkonformer Weise genutzt werden kann, sofern durch Vereinbarungen, die von den Standard-Verarbeitungsvereinbarungen abweichen, das datenschutzrechtliche Schutzniveau hinreichend gesteigert wird. Hierbei kann z. B. auch die Handreichung der DSK hinsichtlich Microsoft 365[5] Orientierung bieten.[6] Dass Cisco sich mit diesen abweichenden Vereinbarungen einverstanden erklärte, bedeutet jedoch nicht zwangsläufig, dass auch andere US-Konzerne wie etwa Microsoft zu derartigen Zugeständnissen bereit sind. Die aktuelle Entscheidung der Berliner Datenschutzbeauftragten zeigt aber, dass sich entsprechende Anstrengungen lohnen können und dies von den Datenschutzaufsichtsbehörden auch honoriert wird.

---

2 https://www.heise.de/news/Trotz-Datenschutz-Ultimatum-FU-Berlin-will-Cisco-Webex-vorerst-weiter-nutzen-7254870.html (zuletzt abgerufen am 18.12.2023).

3 https://www.fu-berlin.de/presse/informationen/fup/2023/fup_23_268-webex/index.html (zuletzt abgerufen am 18.12.2023).

4 https://astafu.de/node/583 (zuletzt abgerufen am 18.12.2023).

5 Handreichung für die Verantwortlichen zum Abschluss einer Auftragsverarbeitungsvereinbarung gem. Art. 28 Abs. 3 DSGVO mit Microsoft für den Einsatz von „Microsoft 365", abzurufen unter handreichung_ms_365_clean_formatiert_stand-24.08.2023.pdf (nrw.de) (zuletzt abgerufen am 18.12.2023).

6 Hierzu ausführlich Palenberg, Unterm Christbaum liegt 'ne Handreichung, DFN-Infobrief Recht 12/2023.

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 Universität Münster, 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