Newsletter IP/IT

September 2023

Inhalt

Europäisches Parlament einigt sich auf Position zur KI-Verordnung

I. Hintergrund

Das Europäische Parlament hat sich am 14. Juni 2023 auf eine gemeinsame Position zur KI-Verordnung geeinigt. Damit kann der Trilog beginnen, in dem die EU-Kommission, der Rat und das Europäische Parlament eine finale Fassung der KI-Verordnung verhandeln wollen. Damit könnte das weltweit erste umfassende gesetzliche Regelwerk zur Verwendung von Künstlicher Intelligenz Ende 2023 verabschiedet werden.

II. Positionen des Europäischen Parlaments

In den vergangenen Monaten hat das Europäische Parlament darum gerungen, eine einheitliche Position zur KI-Verordnung zu erarbeiten. Wesentliche Streitpunkte waren insbesondere die Frage, ob und inwieweit Künstliche Intelligenz (KI) eingesetzt werden darf, um Personen mit Hilfe einer biometrischen Fernidentifizierung in Echtzeit zu identifizieren. Praktisch wird dieser Anwendungsfall bei der Frage relevant, ob die Sicherheitsbehörden diese Technologie einsetzen dürfen, um z. B. bei einer Videoüberwachung in öffentlichen Räumen Personen zu identifizieren, gegen die ermittelt wird. Zu diesem Zweck identifiziert ein Algorithmus die erfassten Gesichter und gleicht diese mit dem Bestand einer Datenbank ab. Am Berliner Bahnhof Südkreuz lief hierzu bereits ein Modellversuch, in dem diese Technologie erprobt wurde. Das konservative Lager im Europäischen Parlament wollte eine solche KI jedenfalls in bestimmten Fällen zur Aufklärung schwerer Straftaten zulassen, während das eher linke Lager diese Technologie verbieten möchte. Das Europäische Parlament hatte zwischenzeitlich eine gemeinsame Position erlangt, die kurz vor der Sitzung am Mittwoch durch einen Änderungsantrag des konservativen Lagers noch ins Wanken gebracht wurde. Nunmehr hat sich das Europäische Parlament jedoch darauf geeinigt, dass die biometrische Fernidentifizierung in

Echtzeit verboten werden soll. Unter engen Voraussetzungen soll es aber möglich sein, die Aufzeichnung im Nachhinein mit Hilfe von KI zu analysieren.

III. Position zur Klassifizierung von KI und den sich daraus ergebenden Rechtsfolgen

Ferner hat sich das Europäische Parlament damit beschäftigt, in welchem Rahmen der Einsatz von KI zukünftig grundsätzlich erfolgen soll. Der ursprünglich von der EU-Kommission erstellte Entwurf der KI-Verordnung sieht vor, dass KI-Systeme in vier Kategorien eingestuft werden. An die Klassifizierung sind dann weitere Rechtsfolgen geknüpft, die Vorgaben zur bloßen Kenntlichmachung des Einsatzes von KI, der Zertifizierung sowie in bestimmten Fällen bis hin zu einem Verbot enthalten. Verboten sind KI-Systeme, die ein *unannehmbares Risiko* darstellen. Auf der zweiten Stufen stehen KI-Systeme, die ein *hohes Risiko* mit sich bringen. Auf der dritten Stufe sind KI-Systeme, von denen ein *eingeschränktes Risiko* ausgeht. Schließlich erfasst die vierte Stufe KI-Systeme, die ein *minimales oder gar kein Risiko* mit sich bringen. Die meisten KI-Systeme dürften, jedenfalls nach derzeitiger Definition in Art. 6 des Entwurfs des Europäischen Parlaments, in der Praxis also wohl als Hochrisiko KI-Systeme eingestuft werden.

Das Europäische Parlament hat sich nun dahingehend positioniert, dass KI-Systeme zur Emotionserkennung in den Bereichen Strafverfolgung, Bildung, Grenzkontrolle und am Arbeitsplatz als verbotene KI eingestuft werden. Ebenso sollen KI-Systeme für das sog. „predicitive Policing“ verboten werden.

Weiter hat sich das Europäische Parlament darauf geeinigt, dass Betreiber von Hochrisiko KI-Systemen vor deren Einsatz eine Folgenabschätzung durchführen sollen. Das Instrument ist der aus dem Datenschutzrecht stammenden Datenschutzfolgenabschätzung entlehnt und besagt, dass im Vorfeld die Auswirkungen des zukünftigen Einsatzes der KI zu bewerten sind. Ziel ist es, dass die Betreiber durch die Folgenabschätzung selbst Maßnahmen ergreifen, um das von dem KI-System ausgehende Risiko zu reduzieren. Grundsätzlich ist dieses Vorgehen sinnvoll. Allerdings zeigt sich schon bei der Datenschutzfolgenabschätzung, dass das Vorgehen das gewünschte Ziel nicht erreicht, wenn jeder Verantwortliche verpflichtet ist, für bestimmte, standardisierte Verarbeitungen (z. B. Microsoft Office 365) eine eigene Datenschutzfolgenabschätzung durchführt. Dies führt zu einem unnötigen Dokumentationsaufwand in den Unternehmen. Sinnvoller erscheint es, in diesen Fällen zentral eine Folgenabschätzung durchzuführen und die zu ergreifenden Maßnahmen zentral vorzuschlagen. Das einzelne Unternehmen könnte sich dann darauf beschränken, die Folgenabschätzung lediglich für Abweichungen vom Standard zu ergänzen.

IV. Auch ChatGPT und Co. werden erfasst

Wichtig ist zudem, dass das Europäische Parlament einen Vorschlag eingebracht hat, wie sog. Foundation Models zukünftig reguliert werden sollen. Dabei geht es um die Regulierung von KI-Modellen, die für verschiedene Zwecke eingesetzt werden können. Aktuell prominentestes Beispiel ist GPT, die Grundlage für ChatGPT. Der Vorschlag des Europäischen Parlaments sieht vor, dass die Anbieter von Foundations Models bestimmte, aber nicht alle Pflichten erfüllen müssen, die auch Anbieter von Hochrisiko KI-Systemen treffen.

V. Nächste Schritte

Im Anschluss an die Sitzung des Europäischen Parlaments haben unmittelbar die Trilog-Verhandlungen begonnen. Es wird erwartet, dass insbesondere die Fragen rund um den Einsatz von KI-Systemen zur biometrischen Echtzeitüberwachung auch in den Trilog-Verhandlungen umfassend diskutiert werden wird. Das gleiche dürfte für die Regelung zu den Foundations Models gelten.

VI. Kritische Punkte

Das EU-Vorhaben, weltweit die erste Regulierung für künstliche Intelligenz zu schaffen, ist ambitioniert. Vorbild ist hierbei sicherlich die DSGVO, die mittlerweile als Vorbild für eine Datenschutzregulierung auf der ganzen Welt geworden ist. Ob dieser Erfolg auch mit der KI-Verordnung einhergehen wird, darf allerdings bezweifelt werden.

Ziel der Regulierung ist es, sowohl Risiken, die damit einhergehen, dass Künstliche Intelligenz eingesetzt wird, zu reduzieren und die Bürger und die Gesellschaft in Europa vor den Folgen zu schützen. Zum anderen soll die Regulierung aber auch dazu dienen, diese Technologie in der EU zu fördern. Betrachtet man die – im Verhältnis zu den USA und China – eher gering ausgeprägte wirtschaftliche Erfolgsgeschichte der EU in diesem Bereich, stellt man sich die Frage, warum sich die KI-Verordnung vor diesem Hintergrund primär mit Verboten und Auflagen befasst, und kaum Regelungen enthält, die einen Anreiz dafür setzen, Künstliche Intelligenz in der EU zu entwickeln und als Produkt oder Service auf den Binnenmarkt zu bringen.

Wesentliche Voraussetzung für den Einsatz von Künstlicher Intelligenz ist die Verfügbarkeit von Daten, um die Modelle

damit trainieren zu können. Die EU arbeitet an verschiedenen Gesetzesvorhaben, die Maschinendaten leichter verfügbar machen sollen. Gleichzeitig setzt die KI-Verordnung sehr hohe (und in Teilen nicht zu erfüllende Anforderungen) an die Datensätze, mit denen KI-Systeme trainiert werden. Dahinter steht die Überlegung, dass ein sog. Bias in KI-Systemen vermieden werden soll. Gleichzeitig fehlen Regelungen, die es erlauben, personenbezogene Daten für Zwecke der künstlichen Intelligenz zu verarbeiten. Es bleibt bei den Regelungen der DSGVO und wird damit auf eine Einwilligungslösung oder eine Interessenabwägung, mit allen rechtlichen Unsicherheiten hinauslaufen. Hier wäre es wünschenswert, wenn der Gesetzgeber Regelungen erlässt, die die Interessen der Unternehmen, aber auch der Bürger angemessen in Ausgleich bringen – also eine Interessenabwägung im Gesetz.

Schließlich scheint es die Tendenz zu geben, dass alle KI-Systeme als KI-Systeme mit einem hohen Risiko klassifiziert werden. Damit treffen die Unternehmen umfassende Pflichten beim Einsatz von Künstlicher Intelligenz. Wünschenswert wäre es, wenn der Gesetzgeber in dieser Kategorie eine ausbalanciertere Lösung vorschlagen würde. Der Eindruck, dass die KI-Verordnung ausbalancierte Regelungen anhand der Klassifizierung trifft, wird dadurch verwischt. Sinnvoller wäre es, hier zudem nicht nur anhand der KI-Systeme, sondern auch der Leistungsfähigkeit der betroffenen Unternehmen zu unterscheiden.

Es bleibt abzuwarten, ob und auf welche gemeinsame Position sich die Beteiligten im Rahmen des Trilog einigen werden.

Angemessenheitsbeschluss der EU-Kommission für die USA und Verlautbarungen der Aufsichtsbehörden

I. In Kürze

Die Europäische Kommission hat am 10. Juli 2023 ihren Angemessenheitsbeschluss für den Datenschutzrahmen zwischen der Europäischen Union („EU“) und den USA, das „Trans-Atlantic Data Privacy Framework“ („DPF“), angenommen. Der DPF legt fest, dass die Vereinigten Staaten im Verhältnis zur EU ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die aus der EU an US-Unternehmen übermittelt werden. Voraussetzung ist, dass die US-Unternehmen an dem DPF teilnehmen und unter dem DPF zertifiziert sind. Mit der Annahme des Angemessenheitsbeschlusses können EU-Unternehmen nun grundsätzlich personenbezogene Daten an zertifizierte US-Unternehmen übermitteln, ohne noch weitere zusätzliche Datenschutzgarantien umsetzen zu müssen.

II. Hintergrund

Die Übermittlung von personenbezogenen Daten in Länder außerhalb der EU (sog. Drittländer) ist nach der Datenschutzgrundverordnung („DSGVO“) nur zulässig, wenn geeignete Datenschutzgarantien bestehen. Aufgrund von Angemessenheitsbeschlüssen der Europäischen Kommission können personenbezogene Daten frei und sicher aus dem Europäischen Wirtschaftsraum (EWR) in ein Drittland übermittelt werden, ohne dass weitere Bedingungen oder Genehmigungen erforderlich sind. In den letzten drei Jahren gab es für die USA keinen gültigen Angemessenheitsbeschluss, nachdem der Europäische Gerichtshof (nachfolgend „EuGH“) die beiden Vorgängerabkommen Safe Harbour („Schrems I”) und den Privacy Shield („Schrems II”) nach Klagen des österreichischen Datenschutzaktivisten Max Schrems für unwirksam erklärte. Das DPF soll nun als Nachfolgemodell wieder Rechtssicherheit im Drittlandtransfer in die USA schaffen.

III. Trans-Atlantic Data Privacy Framework

Mit dem DPF werden verbindliche Garantien geregelt, um den vom EuGH geäußerten Bedenken Rechnung zu tragen. Dabei werden die Rechte von EU-Bürgern erheblich ausgeweitet und ein neues zweistufiges Rechtsbehelfsverfahren eingeführt. Ziel ist u. a. die EU-Daten vor unberechtigten Zugriffen durch die US-Nachrichtendienste zu schützen. So ist vorgesehen, dass sich US-Nachrichtendienste verpflichten, den Zugriff auf Daten von EU-Bürgern auf das zum Schutz der nationalen Sicherheit erforderliche und verhältnismäßige Maß zu beschränken. EU-Bürger können eine Beschwerde

beim „Civil Liberties Protection Officer", dem Bürgerrechtsbeauftragten der US-Nachrichtendienste, einreichen. Die Entscheidung des „Civil Liberties Protection Officer" kann zudem vor dem neu geschaffenen „Data Protection Review Court" anfochten werden.

IV. Zertifizierung als Anwendungsvoraussetzung

Unternehmen können sich nur dann auf den DPF berufen, wenn der jeweilige Datenimporteur, an den personenbezogene Daten übermittelt werden, auch unter dem DPF zertifiziert ist. Dies müssen Unternehmen in der EU vorab prüfen. Das US-Department of Commerce veröffentlicht – wie auch seinerzeit für die Vorgängerabkommen Safe Harbour und Privacy Shield – online eine entsprechende Liste (EU-US-DPF-Liste), anhand welcher überprüft werden kann, ob die betreffende Organisation zertifiziert ist. Für den Fall, dass der Empfänger über keine Zertifizierung verfügt, bleibt es bei der notwendigen Anwendung der Standardvertragsklauseln („SCC"). Allerdings kann dann aller Voraussicht nach im Rahmen der Durchführung des Transfer Impact Assessments („TIA") auf eine intensive Prüfung des Vorliegens von ausreichenden Zusatzgarantien durch den Verweis auf den Angemessenheitsbeschluss verzichtet werden.

V. Rechts(un)sicherheit

Rechtssicherheit bietet das DPF nur so lange, wie ein „angemessenes Schutzniveau" in den USA gewährleistet ist und der EuGH das DPF nicht für unwirksam erklärt. Der NOYB-Vorsitzende Max Schrems, der beide vorherigen Angemessenheitsbeschlüsse vor dem EuGH erfolgreich angegriffen hatte, bereitet sich bereits jetzt auf die erneute Anfechtung beim EuGH vor. Sollte der Fall dem EuGH noch dieses Jahr vorgelegt werden, wäre eine endgültige Entscheidung voraussichtlich nicht vor 2025 zu erwarten. Zu berücksichtigen ist dabei, dass der EuGH in der Vergangenheit den Privacy Shield mit sofortiger Wirkung für ungültig erklärt und den Unternehmen keine Frist für den Wechsel zu einem alternativen Übermittlungsmechanismus eingeräumt hat.

VI. Aktuelle Verlautbarungen der Aufsichtsbehörden

Inzwischen gibt es erste Verlautbarungen der Aufsichtsbehörden, die jedoch kein einheitliches Bild zeichnen. Die Datenschutzkonferenz („DSK") hat am 4. September 2023 mit den Anwendungshinweisen zum Angemessenheitsbeschluss erste Erläuterungen zur neuen Rechtslage veröffentlicht. Neben allgemeinen Informationen erteilt die DSK insbesondere an einzelnen Stellen konkrete Hinweise zu den Vorgaben an den Datentransfer. Insbesondere weist die DSK darauf hin, dass mit der Zertifizierung eines US-Datenimporteurs nicht der Datentransfer jeglicher Daten erfasst sei. Beschäftigtendaten seien etwa nur dann von der Zertifizierung eines US-Datenimporteurs erfasst, wenn der Eintrag des US-Datenimporteurs in der EU-US-DPF-Liste den Eintrag „HR-Data" in der Rubrik „Covered Data" enthält. Überdies enthalten die Erläuterungen der DSK weitreichende Hinweise für betroffene Personen in Bezug auf die Rechtsschutzmöglichkeiten gegen die Nichteinhaltung der Grundsätze des DPF (die DSK benennt etwa die verschiedenen zuständigen Beschwerdestellen und Organisationen innerhalb der USA und der EU). Zusätzlich bekräftigt die DSK im Rahmen ihrer Hinweise, dass neben dem Angemessenheitsbeschluss keine weitere Legitimation für den Datentransfer in die USA notwendig ist und bei Durchführung des TIA die im Angemessenheitsbeschluss ausgeführten Bewertungen berücksichtigt werden können.

In eine etwas andere Richtung geht ein ebenfalls am 4. September veröffentlichtes Papier des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit („TLfDI"). In dieser Verlautbarung weicht der TLfDI ausdrücklich vom Votum der DSK ab und weist erneut auf bestehende Risiken beim Datentransfer in die USA hin. Anders als die DSK legt der TLfDI den Unternehmen nahe, zunächst eine Entscheidung des EuGH abzuwarten.

VII. Praktische Hinweise

Wer in Zukunft nicht gezwungen sein will, ad hoc auf politische Entscheidungen der EU-Kommission, des EuGH oder der US-Regierung zu reagieren, setzt beim Einsatz von US-Anbietern am besten nicht nur auf den Angemessenheitsbeschluss, sondern ergreift vorsichtshalber auch weitere Maßnahmen, wie z. B. den Abschluss der SCCs als alternativer Transfermechanismus, oder prüft, ob andere Rechtsgrundlagen den Transfer rechtfertigen können (Art. 49 DSGVO). Bestehende SCCs sollten daher zunächst nicht ersetzt werden, da offen ist, ob und wie lange das DPF in Kraft bleibt. Hierfür spricht auch die uneinheitliche Auffassung innerhalb der Aufsichtsbehörden. Die Überprüfung und Bewertung des eigenen Datentransfers an US-Dienstleister im Rahmen der Durchführung eines TIAs ist weiterhin zu empfehlen. Dieses bleibt ein wertvolles Instrument, um sicherzustellen, dass diese die notwendigen Datenschutzanforderungen vollständig erfüllen. Auch Übermittlungen in Drittstaaten mit angemessenem Datenschutzniveau bedürfen einer Rechtsgrundlage für die Datenverarbeitung nach Art. 6 DSGVO oder

9-DSGVO bzw. des BDSG. Das DPF ist zudem kein Freibrief für jegliche Datenübermittlung in die USA. Es gibt Sonderregelungen, wie bspw. bei der Verarbeitung von Gesundheitsdaten. Das DPF macht zudem den Abschluss von Auftragsverarbeitungsverträgen oder Joint-Controller-Vereinbarungen nicht obsolet. Verschaffen Sie sich auch einen Überblick über Subunternehmer Ihrer US-Vertragspartner, die ggf. nicht nur in den USA, sondern in China oder Indien ihren Sitz haben. Auch mit diesen sind vertragliche Regelungen und ausreichende Garantien zu vereinbaren, die den Transfer von Daten legitimieren. Der Hinweis auf einen Angemessenheitsbeschluss bei einem Drittlandtransfer ist gemäß Art. 13 Abs. 1 lit. f) DSGVO verpflichtend. Auch bei der Angabe der Empfänger der übermittelten Daten muss darüber informiert werden, ob diese unter das DPF fallen. Und auch die Verarbeitungsverzeichnisse im Sinne des Art. 30 DSGVO, die einen US-Datentransfer dokumentieren, müssen durch die Angabe des Angemessenheitsbeschlusses als Rechtsgrundlage für den Datentransfer ergänzt werden.

Keyword- Advertising: Nutzung einer fremden Marke

I. Auf den Punkt.

Die Nutzung einer Marke oder eines Unternehmenszeichens als gebuchtes Keyword bei einer Suchmaschine beinhaltet nicht zwangsläufig die Verletzung von Markenrechten. Dies bestätigte jüngst das OLG Braunschweig, wobei es maßgeblich auf die Sicht des verständigen Internetnutzers abstellt. Dieser müsse anhand der Werbeanzeige erkennen können, dass die angebotenen Waren und Dienstleistungen nicht von der Inhaberin der Marke stammen.

II. Hintergrund

Der 2. Zivilsenat des Oberlandesgerichts Braunschweig (OLG Braunschweig, Urt. v. 9.2.2023 – 2 U 1/22) hatte sich mit der Berufungsklage eines Unternehmens auseinanderzusetzen. Die Berufungsklägerin betreibt ein Vergleichsportal für Kreditvermittlungsangebote im Internet und hatte Werbeanzeigen bei der Suchmaschine Google im Rahmen des Keyword Advertising geschaltet. Beim Keyword-Advertising können Dienstleister bestimmte Begriffe bei dem Betreiber einer Suchmaschine buchen, damit ihre Werbeanzeigen bei Eingabe des Suchbegriffes in der Liste der Suchergebnisse erscheinen. Die Berufungsklägerin hatte als Keyword den Begriff „smava“ eingetragen. Die Werbeanzeigen der Berufungsklägerin, wurden daraufhin in der Liste der Suchergebnisse an zweiter Stelle unter der Anzeige der Smava GmbH gezeigt, welche gleichzeitig Inhaberin der Wortmarke „smava“ ist. Die Smava GmbH, ebenfalls Betreiberin eines Online-Vergleichsportals für Ratenkredite, sah darin eine Verletzung ihrer Markenrechte und eine unlautere Werbung. Der Klage auf Unterlassung und Feststellung der Schadenersatzpflicht gab das Landgericht Braunschweig weitestgehend statt.

III. Die Entscheidung

Die gegen diese Entscheidung gerichtete Berufung hatte Erfolg. Das Oberlandesgericht Braunschweig wies die Klage mit Urteil vom 9. Februar 2023 ab. Zwar sei eine markenrechtliche Doppelidentität im Sinne des § 14 II 1 Nr. 1 MarkenG, also eine Übereinstimmung sowohl gegenüberstehender Zeichen als auch Waren und Dienstleistungen, durch Nutzung der Marke als Keyword gegeben, die Verletzung einer Marke oder Unternehmenskennzeichnung läge jedoch nur vor, wenn eine der Funktionen der Marke durch die Anzeige beeinträchtigt würde.

Eine solche Beeinträchtigung sei vorliegend nicht gegeben. Anhand der Werbeanzeige könne der verständige Nutzer der Suchmaschine erkennen, dass die beworbene Dienstleistung nicht von der Markeninhaberin stamme. Die Kennzeichnung als „Anzeige“ über dem Text sowie das Fehlen einer Nennung der verteidigten Marke als Begriff reiche hierbei aus, um eine abweichende betriebliche Herkunft der angebotenen Dienstleistung zu verdeutlichen. Eine Verletzung durch Verwendung der bekannten Marke „ohne rechtfertigenden Grund in unlauterer Weise“ läge ebenfalls nicht vor. Es handele sich bei der Werbung um den Vorschlag einer Alternative zum Angebot der Inhaberin der Marke.

IV. Unser Kommentar

Im Wesentlichen bestätigt die Entscheidung die bisherige Rechtsprechung von BGH und EuGH. Besonderes Augenmerk widmet der BGH der Frage, ob das Keyword-Advertising eine der Funktionen der Marke, insbesondere die Herkunftsfunktion, beeinträchtigt. In den bislang ergangenen Entscheidungen fand bei dieser Einschätzung regelmäßig Berücksichtigung, inwiefern der verständige Nutzer der Suchmaschine eine Werbeanzeige von einem echten Suchergebnis unterscheiden kann. Nach den Grundsatzentscheidungen des BGH und EuGH wurde die Abgrenzung der Werbeanzeigen durch Darstellung in einem deutlich gekennzeichneten „Werbeblock“ vorausgesetzt. Das OLG lässt nunmehr auch eine Abgrenzung mit hinreichenden grafischen Mitteln ausreichen. Zwangsläufig wird sich mit Gewöhnung des verständigen Internetnutzers an eine übliche Anzeigenstruktur der Anforderungsmaßstab an die Kenntlichmachung als Anzeige im Laufe der Zeit verändern. Es empfiehlt sich somit in jedem Einzelfall individuell die Ausgestaltung der Anzeige zu untersuchen und eine entsprechende Einschätzung zu treffen.

OLG München: Zum Mangel einer Software bei fehlender Funktionsfähigkeit auf einzelnen Betriebssystemen

I. Hintergrund

Erwirbt eine Person oder ein Unternehmen eine Software, stellt sich nicht selten die Frage nach der zu gewährleistenden Beschaffenheit einer Software. Die Beschaffenheit wird meistens in Verträgen festgelegt, jedoch ist dies gesetzlichen Grenzen unterzogen. Besondere Bedeutung kann dabei dem Aspekt zukommen, ob eine Software in Kombination mit einem bestimmten Betriebssystem funktionsfähig ist. Das OLG München hatte in einem aktuellen Verfahren zu entscheiden, ob die fehlende Funktionsfähigkeit auf dem Betriebssystem des Kunden einen Sachmangel im Sinne des § 434 BGB bedeutet.

II. Sachverhalt

Die Klägerin des Rechtsstreits vor dem OLG München (OLG München, Urt. v. 17.11.2021 – 7 U 5822/20 = MMR 2022, 216) ist ein Unternehmen, das Software unterschiedlicher Anbieter vertreibt. Die Beklagte ist ein Unternehmen in der Immobilienbranche. In einer Online-Präsentation stellte die Klägerin der Beklagten eine Software zur Immobilienverwaltung vor. Im Anschluss schrieb die Klägerin der Beklagten ein Angebot für die zeitlich unbegrenzte Überlassung der Software („Softwarekauf“). Im Angebot befand sich auf der letzten Seite der Hinweis, dass die Software nur mit bestimmten Server Betriebssystemen von Microsoft verwendet werden kann.

Die Beklagte, die ausschließlich Apple Geräte (Betriebssystem MacOS) verwendet, rügte gegenüber der Klägerin, dass die Software bei ihr nicht funktionstüchtig sei und erklärte den Rücktritt vom Kaufvertrag. Mit ihrer Klage begehrte die Klägerin nun die Erfüllung ihrer Forderung auf Kaufpreiszahlung für die Software. Die Beklagte behauptete, dass die Klägerin ihr in einer – unstreitig durchgeführten – Online-Präsentation zugesichert habe, dass die Software auch auf dem Betriebssystem MacOS liefe.

Das Landgericht gab der Klage statt und verurteilte die Beklagte antragsgemäß zur Zahlung des Kaufpreises. Hiergegen legte die Beklagte Berufung ein. Zur Behauptung, dass Software grundsätzlich unter allen gängigen Betriebssystemen liefe, beantragte die Beklagte die Einholung eines Sachverständigengutachtens.

III. Entscheidung

Das OLG München wies die Berufung der Beklagten im Wesentlichen zurück. Die Beklagte sei von Ihrer Zahlungspflicht durch ihre Rücktrittserklärung nicht befreit worden, da es einem wirksamen Rücktritt bereits an einem Sachmangel im Sinne des § 434 Abs. 1 BGB a.F. fehle.

1. Keine Beschaffenheitsvereinbarung

Es sei keine Beschaffenheitsvereinbarung im Sinne des § 434 Abs. 1 S. 1 BGB a.F. geschlossen worden.

Von der Behauptung der Beklagten, dass die Klägerin ihr in der Online-Präsentation zugesichert habe, dass die Software auf dem Betriebssystem MacOS liefe, konnte sich das Gericht nicht überzeugen. In den hierzu vom Gericht erhobene Zeugenaussage ergab sich lediglich die Behauptung seitens der von der Beklagten benannten Zeugen, dass Vertreter der Klägerin angegeben hätten, dass in Kürze ein Zusatzmodul erhältlich sei, wodurch die Software auch auf MacOS betriebsfähig sei. Nach Ansicht des Gerichts ließ sich hieraus bereits kein Versprechen einer Beschaffenheit herleiten. Demgegenüber verwies das Gericht ausdrücklich auf den Zusatzhinweis aus dem Angebot, in dem auf die kompatiblen Betriebssysteme hingewiesen wurde.

2. Eignung zur im Vertrag vorausgesetzten Verwendung

Es liege auch kein Sachmangel nach § 434 Abs. 1 S. 2 Nr. 1 BGB a.F. vor. So eigne sich die Software für die nach dem Vertrag vorausgesetzte Verwendung. Dabei gehe es um die konkrete Nutzung der Kaufsache durch den Käufer, die die Parteien zwar nicht vereinbart, aber übereinstimmend unterstellt haben. Bei der Ermittlung dieser Verwendung seien neben dem Vertragsinhalt die Gesamtumstände des Vertragsabschlusses heranzuziehen. § 434 Abs. 1 S. 2 Nr. 1 BGB a.F. ziele mit dem Merkmal der „nach dem Vertrag vorausgesetzten Verwendung“ nicht auf konkrete Eigenschaften der Kaufsache ab, die sich der Käufer vorstellt, sondern darauf, ob die Sache für die dem Verkäufer erkennbare Verwendung (Nutzungsart) durch den Käufer geeignet sei (BGH, Urt. v. 20.3.2019 - VIII ZR 213/18, Rn. 25 f.). Zweck der Verwendung sei der Einsatz für die Immobilienverwaltung gewesen. Eine fehlende Eignung der Software habe die Beklagte nicht vorgetragen. Die Verwendung auf dem Betriebssystem MacOS sei demgegenüber eine konkrete Eigenschaft, die sich die Beklagte vorgestellt habe. Allerdings sei diese nicht im Verwendungszweck enthalten gewesen.

3. Eignung zur gewöhnlichen Verwendung

Die Software sei auch nicht nach § 434 Abs. 1 S. 2 Nr. 2 BGB a.F. mangelhaft gewesen, da sie sich für die gewöhnliche Verwendung eigne und eine Beschaffenheit aufweise, die bei Sachen der gleichen Art üblich sei und die der Käufer nach der Art der Sache erwarten könne. Die Software eigne sich bereits für die gewöhnliche Verwendung, da sie für den Zweck der Nutzung, die Immobilienverwaltung, brauchbar sei. Die Software weise auch die übliche Beschaffenheit auf, die ein Käufer erwarten könne. Dem Gericht sei aus jahrelanger Befassung mit Streitigkeiten im Softwarebereich bekannt, dass die Funktionsfähigkeit einer Software auf allen gängigen Betriebssystemen nicht üblich sei. Aufgrund eigener Sachkunde des Gerichts bedürfe es daher des von der Beklagten beantragten Sachverständigenbeweises nicht.

IV. Unser Kommentar

Die Entscheidung des OLG München ist grundsätzlich zu begrüßen, da hierzu bislang keine gerichtliche Einordnung erfolgt war. Trotz der Neufassung des § 434 BGB zu Beginn des Jahres 2022 dürfte diese Einordnung bis auf Weiteres Bestand haben. Es stellt demnach keinen Mangel dar, wenn eine Software nicht auf allen gängigen Betriebssystemen läuft. Die Software entspricht dem erwartbaren Zustand, wenn sie für ihren Zweck grundsätzlich geeignet ist. Es ist derweil nicht so, dass Software immer auf allen Betriebssystemen funktionsfähig ist. Aus diesem Grund kann der Käufer die Funktionsfähigkeit auf allen Betriebssystemen beim Softwarekauf nicht erwarten.

Außergewöhnlich ist die Feststellung des Gerichts aus eigener Sachkunde, dass Software üblicherweise nicht auf allen Betriebssystemen verwendbar ist und das Gericht hierzu auf die Erhebung eines Sachverständigenbeweises verzichtet hat. Nach dem Urteil ist davon auszugehen, dass Käufer zukünftig nicht erwarten können, dass eine Software auf allen Betriebssystemen funktionsfähig ist. Dennoch ist weiterhin aus Gründen der Rechtssicherheit anzuraten Beschränkungen der Kompatibilität von Software mit bestimmten Betriebssystemen oder anderweitige Einschränkungen der Software in Leistungsbeschreibungen und Vertragsdokumenten hinreichend kenntlich zu machen.

DNS-Sperre – ein praxistaugliches Verteidigungsmittel im Kampf gegen Verletzung von Urheberrechten?

I. Hintergrund

Inhaber von Urheberrechten sehen sich oftmals hohen Herausforderungen ausgesetzt, sofern sie gegen Webseiten-Betreiber vorgehen wollen, die rechtswidrig Inhalte ins Netz stellen. Grund ist, dass die verantwortlichen Betreiber häufig unerreichbar im Ausland sitzen oder namentlich nicht bekannt sind. Vor diesem Hintergrund liegt es nahe, an „greifbare" Dritte, wie etwa den Host-Provider oder den Access-Provider heranzutreten, um die Rechtsverletzung zu unterbinden. Das Gesetz sieht als Instrument die Domain-Name-System-Sperre (DNS-Sperre) gemäß § 7 Abs. 4 Telemediengesetz (TMG) vor.

II. Funktionalität einer DNS-Sperre

Die DNS-Sperre knüpft an das Domain-Name-System an, das den direkten Datenverkehr im Internet unterstützt, indem es Domainnamen mit Webservern verbindet. Im Wesentlichen übersetzt DNS eine benutzerfreundliche Domainanfrage – wie z. B. www.luther-lawfirm.com – mit einer computerfreundlichen Server IP-Adresse – wie z. B. 10987654321. Aufgrund dieser Funktion wird DNS oftmals auch als „Telefonbuch des Internets" bezeichnet. Betreiber von DNS-Servern können als Access-Provider für bestimmte Domains die Auskunft sperren. Infolgedessen wird dem Internetznutzer dann keine oder eine andere Website mit der Nachricht, dass die aufgerufene Website nicht mehr verfügbar sei, angezeigt.

III. Vorgaben an eine DNS-Sperre nach § 7 Abs. 4 TMG

Bereits 2015 hatte der Bundesgerichtshof (BGH) in einem Grundsatzurteil zur „Störerhaftung von Access-Providern" ausgeführt, dass Access-Provider erst in Anspruch genommen werden können, wenn eine Inanspruchnahme der näher an der Rechtsgutverletzung stehenden Content- und Host-Provider scheitere oder keine Erfolgsaussicht habe. Mithin haftet der Access-Provider gegenüber dem tatnäheren Beteiligten ausschließlich subsidiär. Das durch den BGH entwickelte „Subsidiaritätserfordernis" fand 2017 auch Eingang in § 7 Abs. 4 TMG: Demnach kann ein Access-Provider erst in Anspruch genommen werden, wenn für den Rechtsinhaber „keine andere Möglichkeit [besteht], der Verletzung des Rechts abzuhelfen". Vor dem Hintergrund der unbestimmten Formulierung, die zur Interpretation einlädt, stellt sich die Frage, ob die DNS-Sperre zur Abwendung von Urheberrechtsverletzungen in der Praxis tatsächlich ein scharfes Schwert darstellt oder letztlich ein Verteidigungsmittel mit stumpfer Klinge ist.

IV. Die BGH-Entscheidung vom 13. Oktober 2022

Mit Urteil vom 13. Oktober 2022 (Az. I ZR 11/21) hat der BGH die Voraussetzungen für eine DNS-Sperre, insbesondere unter Berücksichtigung des Subsidiaritätserfordernisses, näher konkretisiert:

1. Der Sachverhalt

Die Klägerinnen, bestehend aus mehreren Wissenschaftsverlagen, beantragten einen Telekommunikationsdienstleister als Access-Provider zu verpflichten, eine DNS-Sperre für bestimmte Domainnamen (wie etwa „LibGen“ und „Sci-Hub“) einzurichten. Die Webseiten vertrieben wissenschaftliche Artikel und Bücher, an denen die Klägerinnen ausschließliche Nutzungsrechte hatten. Die der Klage vorangegangenen und durch die Klägerinnen durchgeführten Ermittlungen verliefen größtenteils erfolglos. Ein in Schweden ansässiger Host-Provider wurde außergerichtlich abgemahnt, reagierte jedoch nicht auf Notifizierungs- und Abmahnschreiben.

2. Die Begründung

Der BGH sah das Subsidiaritätserfordernis vorliegend nicht als erfüllt an: Weder sind die Klägerinnen gegen den schwedischen Host-Provider im Rahmen des einstweiligen Rechtsschutzes vorgegangen, noch haben sie eine entsprechende Erfolglosigkeit dargelegt. Vorliegend wäre es den Klägerinnen zumindest zumutbar und geboten gewesen, vor einem deutschen Gericht im Wege der einstweiligen Verfügung einen Auskunftsanspruch gegen den schwedischen Host-Provider geltend zu machen, um an weitere Erkenntnisse bzw. Ermittlungsansätze über den Rechtsverletzter zu gelangen. Ein Auskunftsanspruch gem. § 101 Urheberrechtsgesetz (UrhG) ist in Fällen von offensichtlicher Rechtsverletzung im einstweiligen Rechtsschutz ausnahmsweise zulässig, vgl. § 101 Abs. 7 UrhG.

a) Konkretisierung des Subsidiaritätserfordernisses

Nach dem BGH muss der Rechtsinhaber zunächst alle zumutbaren Maßnahmen gegen den Betreiber als unmittelbarer Rechtsverletzter oder/und den Host-Provider, der durch die Erbringung einer Dienstleistung zur Rechtsverletzung beiträgt und daher näher an der Rechtsverletzung steht, ausschöpfen. Der Erschöpfung zumutbarer Maßnahmen steht es gleich, wenn diesen im Vorhinein jede Erfolgsaussicht fehlt.

b) Zumutbare Maßnahmen

Welche Maßnahmen für den Rechtsinhaber zumutbar sind, ist nach dem BGH eine Frage des Einzelfalls. Im Regelfall gehören dazu (jeweils im zumutbaren Umfang):

- eigene Nachforschungen zur Ermittlung von vorrangig in Anspruch zu nehmenden Beteiligten, wie Betreiber und Host-Provider. Dies umfasst auch die Einschaltung staatlicher Ermittlungsbehörden im Wege der Strafanzeige oder die Vornahme privater Ermittlungen durch Detektive oder darauf spezialisierte Unternehmen, soweit wirtschaftliche Ressourcen vorhanden sind;
- außergerichtliche Inanspruchnahmen bekannter Betreiber und Host-Provider auf Entfernung der urheberrechtsverletzenden Inhalte;
- gerichtliche Verfahren des einstweiligen Rechtsschutzes gegen innerhalb der Europäischen Union ansässige Betreiber und Host-Provider. Bei Staaten außerhalb der Europäischen Union muss das Vorhandensein gleichwertiger Rechtsschutzmöglichkeiten im Einzelfall geprüft werden, wobei an die vom Antragsteller zu erbringende Darlegungslast keine überzogenen Anforderungen gestellt werden dürfen.

Die Grenze des Unzumutbaren ist da erreicht, wo weitere Maßnahmen zu einer untragbaren Verzögerung der Anspruchsdurchsetzung führen würden. Dies sei etwa bei der Durchführung eines Hauptsacheverfahrens über mehrere Instanzen der Fall.

c) Fehlende Erfolgsaussicht

Bezüglich der Frage, ob den zumutbaren Maßnahmen im Vorhinein jede Erfolgsaussicht fehlt, ist der Rechtsinhaber als Antragsteller grundsätzlich darlegungs- und beweispflichtig. Der Berufung der Revision auf eine tatsächliche Vermutung aufgrund allgemeiner Lebenserfahrung erteilte der BGH eine Absage: Die Revision hatte hierzu vorgetragen, dass sich die Betreiber „strukturell urheberrechtsverletzender Internetseiten“ durch anonymisierende Schutzmaßnahmen gegen die Inanspruchnahme absichern würden, sodass den Maßnahmen – wie etwa in Form von privaten Ermittlungen und der Durchsetzung von Auskunftsansprüchen – von Anfang an jede Erfolgsaussicht fehlte. Der BGH lehnte die Annahme einer tatsächlichen Vermutung ab, da sich an den Begriff „strukturell urheberrechtsverletzender Internetseiten“ kein Satz der alltäglichen Lebenserfahrung knüpfen lasse, der eine entsprechende Schlussfolgerung zulasse. Dies folge insbesondere aus der Konturlosigkeit des Begriffs „strukturell urheberrechtsverletzender Internetseiten“. Auch stellte der BGH infrage, ob die Anknüpfung an eine tatsächliche Vermutung überhaupt zu einer Erleichterung der Anspruchsdurchsetzung führen könne. Dem stehe der zu erwartende umfangreiche Vortrag zur Darlegung der Tatsache entgegen, dass es sich um eine „strukturell urheberrechtsverletzende Internetseite“ handele.

Allerdings könne sich eine Erfolglosigkeit aus früheren Maßnahmen – wie einem in anderem Zusammenhang durchgeführten Verfahren des einstweiligen Rechtsschutzes gegen

denselben Host-Provider – ergeben. Offen bleibt dagegen die zeitliche Dimension, innerhalb derer noch von einem Zusammenhang mit vorangegangen Verfahren gegen denselben Host-Provider ausgegangen werden kann.

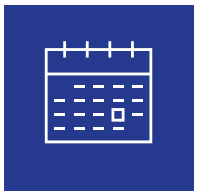
V. Unsere Praxishinweise

Das Urteil führt die Rechtsprechungslinie des BGH konsequent und entgegen anderslautenden Stimmen in der Literatur fort: Die DNS-Sperre bleibt das letzte Mittel, um einer Urheberrechtsverletzung abzuhelfen. Der Rechtsinhaber muss zunächst alle zumutbaren Maßnahmen ausschöpfen, bevor er einen Access Provider in Anspruch nehmen kann. Insbesondere sollte zunächst eine einstweilige Verfügung gegen tatnähere Beteiligte angestrengt werden, sofern diese einen Sitz in der EU haben. Dies umfasst auch den Versuch, eine Drittauskunft im Rahmen des einstweiligen Rechtsschutzes vor einem deutschen Gericht geltend zu machen. Dies dürfte in der Zukunft sicherlich die sachgerechte Vorgehensweise sein. Dabei ist die einstweilige Verfügung rechtzeitig einzuleiten. Andernfalls fehlt es an einem Verfügungsgrund und der zögerliche Rechtsinhaber verliert seinen Anspruch gegen den Access-Provider, da das Subsidiaritätserfordernis nicht mehr eingehalten werden kann. Bei außereuropäischen Sachverhalten muss insbesondere geprüft werden, ob gleichwertige Rechtsschutzmöglichkeiten bestehen, hierbei müssen insbesondere internationale Abkommen in den Fokus genommen werden.

VI. Fazit

Im Ergebnis ist festzuhalten, dass eine DNS-Sperre – aufgrund der restriktiven Voraussetzungen – nur als letztes Mittel der Verteidigung in Betracht kommt. Ob dies nun ein Verteidigungsmittel mit scharfer oder stumpfer Klinge ist, hängt vom Einzelfall ab; denn letztlich gilt, dass auch eine mit Erfolg erkämpfte DNS-Sperre nicht unbedingt den erhofften Erfolg bringen wird. Die Schwäche von DNS-Sperren ist, dass sie mehr oder weniger leicht zu umgehen sind. Zum einen bleibt die Website über die Eingabe der IP-Adresse weiterhin aufrufbar. Zum anderen kann der Domain-Name leicht abgeändert werden, sodass die Website über eine Suchmaschine weiterhin auffindbar bleibt. Ferner ist DNS dezentralisiert aufgebaut, sodass Internetnutzer mithilfe einer Konfiguration ihres Routers auch Anfragen an die DNS-Server anderer Betreiber in Drittstaaten senden können. Nicht zuletzt bei lokalen DNS-Sperren bleibt die Möglichkeit der Umgehung durch Nutzung eines VPN-Tunnels.

Veranstaltungen, Veröffentlichungen und Blog



Eine Übersicht mit unseren Veranstaltungen finden Sie hier.

Eine Liste unserer aktuellen Veröffentlichungen finden Sie hier.

Unseren Blog finden Sie hier.

Impressum

Verleger: Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 0
Telefax +49 221 9937 110, contact@luther-lawfirm.com
V.i.S.d.P.: Dr. Michael Rath, Partner
Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 25795
michael.rath@luther-lawfirm.com

Bildnachweis: AdobeStock/stnazkul: Seite 1; AdobeStock/Jackie Niam: Seite 3; AdobeStock/Sikov: Seite 6 AdobeStock/Blue Planet Studio: Seite 9; AdobeStock/tippapatt: Seite 10; AdobeStock/klss777: Seite 12;

Haftungsausschluss

Obgleich dieser Newsletter sorgfältig erstellt wurde, wird keine Haftung für Fehler oder Auslassungen übernommen. Die Informationen dieses Newsletters stellen keinen anwaltlichen oder steuerlichen Rechtsrat dar und ersetzen keine auf den Einzelfall bezogene anwaltliche oder steuerliche Beratung. Hierfür stehen unsere Ansprechpartner an den einzelnen Standorten zur Verfügung.

Luther.

Bangkok, Berlin, Brüssel, Delhi-Gurugram, Düsseldorf, Essen, Frankfurt a. M., Hamburg, Hannover, Ho-Chi-Minh-Stadt, Jakarta, Köln, Kuala Lumpur, Leipzig, London, Luxemburg, München, Shanghai, Singapur, Stuttgart, Yangon

Weitere Informationen finden Sie unter
www.luther-lawfirm.com
www.luther-services.com

unyer GLOBAL ADVISORS