Host Provider muss Deep-Fake-Video sperren

29.12.2025, 08:36 | Handel, Wirtschaft, Finanzen, Banken & Versicherungen

Pressemitteilung von: *MTR Legal Rechtsanwälte Pressearchiv*

Beschluss des OLG Frankfurt vom 4. März 2025 – Az. 16 W 10/25

Ist bereits ein Hinweis auf einen rechtsverletzenden Post erfolgt, muss der Hostprovider auch sinngleiche Beiträge sperren. Ein weiterer Hinweis ist dann nicht erforderlich. Das OLG Frankfurt betont dabei die Haftung des Hostproviders für rechtsverletzende Medien und Medieninhalte, insbesondere manipuliertes Videomaterial und die Fälschung von Personen. Das machte das OLG Frankfurt mit Beschluss vom 4. März 2025 in einem Eilverfahren deutlich (Az. 16 W 10/25).

Bei Rechtsverletzungen im Internet, z.B. durch ein Meme oder Deep-Fakes, müssen Hostprovider tätig werden und die entsprechenden Inhalte sperren, wenn sie Kenntnis von den rechtsverletzenden Posts haben. Das Angebot und die Leistungen von Hostprovidern umfassen dabei Webhosting, Server, Website, Domain, E-Mail-Adresse und Internetanschluss, wodurch sie den Zugang zum Internet ermöglichen. Es ist wichtig, die Unterscheidung zwischen Host Provider, Access Provider und Content Provider zu kennen, da alles, was hinter diesen Angeboten steckt, sehr komplex ist. Darüber hinaus gibt es verschiedene Angebote im Bereich Webhosting und Serverlösungen, die individuell auf die Bedürfnisse der Nutzer zugeschnitten sind. Das hat das OLG Frankfurt bereits mit Urteil vom 25. Januar 2024 entschieden (Az.: 16 U 65/22). In der konsequenten Fortsetzung dieser Rechtsprechung hat das OLG Frankfurt in einem Eilverfahren entschieden, dass Plattformbetreiber auch sinngleiche Inhalte sperren müssen, ohne dass ein erneuter Hinweis erforderlich ist, so die Wirtschaftskanzlei MTR Legal Rechtsanwälte , die u.a. im IT-Recht berät.

Deepfake Videos mit sinngleichem Inhalt

In dem zugrunde liegenden Verfahren war ein Deepfake Video auf einer Social-Media-Plattform veröffentlicht worden. Dieses Deepfake Video wurde mithilfe von Deepfake Technologie und Deepfake KI erstellt, wobei das Gesicht und die Stimme der betroffenen Person manipuliert wurden. In diesem Video wurde ein bekannter Arzt durch manipuliertes Bild- und Tonmaterial so dargestellt, als würde er für ein Produkt zur Gewichtsabnahme werben. Tatsächlich hatte er damit nichts zu tun. Nach einem entsprechenden Hinweis des Betroffenen entfernte der Plattformbetreiber dieses Video.

Kurze Zeit später tauchte jedoch ein weiteres Video mit nahezu identischem Inhalt auf. Es unterschied sich lediglich in

Details, etwa durch eine leicht abgewandelte Darstellung und eine andere Überschrift, vermittelte aber denselben täuschenden Gesamteindruck. Solche Fälschung von Medieninhalten und Videomaterial stellt ein wachsendes Problem für den Schutz der Wirklichkeit und die Privatsphäre von Personen dar. Für die Erstellung solcher Dinge werden fortschrittliche Technik und große Mengen an Daten genutzt, wobei das Lernen von AI-Modellen eine zentrale Rolle spielt, um die Anwendung immer realistischer zu machen. Auch dieses Video wurde zwar gelöscht, aber erst nach einer erneuten Meldung. Deepfake Videos können zur Verbreitung von Fake News beitragen, weshalb effektive Schutzmaßnahmen gegen solche Manipulationen immer wichtiger werden. Der Betroffene wollte die Plattform nun gerichtlich verpflichten lassen, derartige Inhalte zukünftig zu unterlassen, und beantragte eine einstweilige Verfügung.

Technologie und Erkennung von Deep-Fake-Videos

Die rasante Entwicklung von Deepfake-Technologien basiert auf dem Einsatz von künstlicher Intelligenz (KI) und fortschrittlichen Algorithmen des maschinellen Lernens. Mit diesen Verfahren lassen sich Videos und Audiodateien so manipulieren, dass sie täuschend echt wirken und selbst für geübte Augen und Ohren kaum von authentischen Inhalten zu unterscheiden sind. Besonders das sogenannte Face Swapping, bei dem das Gesicht einer Person durch das einer anderen ersetzt wird, ist eine der bekanntesten Techniken. Hierbei werden große Mengen an Bild- und Videomaterial benötigt, um die Mimik, Gestik und den Tonfall der Zielperson möglichst realistisch nachzubilden.

Technologische Grundlagen von Deepfakes

Die Erkennung solcher Fälschungen stellt Host Provider, Access Provider und andere Anbieter von Webhosting und Serverleistungen vor erhebliche Herausforderungen. Deepfake-Videos und manipulierte Audiodateien können gezielt zur Verbreitung von Fakes, Fake News oder zur Rufschädigung von Personen eingesetzt werden. Die eingesetzten KI-Systeme und Algorithmen werden dabei immer ausgefeilter, sodass klassische Prüfverfahren oft an ihre Grenzen stoßen.

Methoden zur Erkennung von Deepfakes

Um Deepfake-Videos und andere Fälschungen zu erkennen, kommen verschiedene Methoden zum Einsatz. Dazu zählen etwa die Analyse von Unregelmäßigkeiten in der Mimik, der Bewegungsabläufe oder der Lichtverhältnisse im Video. Auch die Überprüfung der Metadaten und der Einsatz spezialisierter KI-Tools zur Erkennung von Manipulationen sind gängige Verfahren. Dennoch bleibt die Erkennung eine ständige Herausforderung, da die Techniken zur Erstellung von Deepfakes sich kontinuierlich weiterentwickeln.

Risiken und Schutzmaßnahmen für Plattformbetreiber

Für Host Provider und Plattformbetreiber bedeutet dies, dass sie nicht nur auf Hinweise reagieren, sondern auch proaktiv Maßnahmen zum Schutz vor der Verbreitung von Deepfake-Inhalten ergreifen müssen. Dazu gehören der Einsatz von Content-Filtern, die regelmäßige Überprüfung der gehosteten Inhalte und die Zusammenarbeit mit Experten und Behörden. Ziel ist es, die Authentizität der auf ihren Servern und Webseiten bereitgestellten Medieninhalte zu gewährleisten und Manipulationen frühzeitig zu erkennen.

Die Nutzung von Deepfake-Technologien birgt erhebliche Risiken für die Privatsphäre und Sicherheit von Personen und Unternehmen. Manipulierte Videos, Audiodateien oder Bilder können gezielt zur Täuschung, Erpressung oder Verbreitung von Falschinformationen eingesetzt werden. Daher ist für Nutzerinnen und Nutzer im Internet wichtig, kritisch mit digitalen Inhalten umzugehen und bei Verdacht auf Fälschungen entsprechende Prüf-Tools oder einen Domain Check zu nutzen.

Notwendigkeit von Forschung und Zusammenarbeit

Angesichts der rasanten Weiterentwicklung von Deepfake-KI und der zunehmenden Verbreitung solcher Fälschungen ist es unerlässlich, dass Forschung, Technologieunternehmen, Hosting-Anbieter und Behörden eng zusammenarbeiten. Nur durch die Kombination aus innovativen Erkennungsmethoden, technischer Weiterentwicklung und klaren rechtlichen Rahmenbedingungen kann die Integrität digitaler Medieninhalte langfristig geschützt werden. So schaffen wir gemeinsam eine vertrauenswürdige und sichere Online-Umgebung, in der Manipulationen und Fakes keinen Platz haben.

Kein erneuter Hinweis erforderlich

Das Landgericht wies den Antrag zunächst ab, da es keine fortdauernde Verletzungspflicht der Plattform sah. Auf die sofortige Beschwerde des Antragstellers hin änderte das Oberlandesgericht Frankfurt diese Entscheidung jedoch teilweise ab. Nach Auffassung des Senats haftet die Plattform nicht für das erste Video, wohl aber für das zweite. Im rechtlichen Kontext ist zu beachten, dass der Betreiber einer Webseite als Content-Provider gilt, wenn er eigene oder fremde Inhalte kontrolliert, bearbeitet oder veröffentlicht, was eine besondere Haftung für die auf der Webseite bereitgestellten Inhalte mit sich bringt. Zur Begründung führte das OLG aus, dass der Plattform vor dem ersten Hinweis keine Kenntnis von der Rechtsverletzung vorlag und sie daher auch keine Pflicht zur Vorabkontrolle oder Löschung traf. Nach der Entfernung des ersten Videos habe sich die Situation jedoch geändert: Mit der konkreten Kenntnis der Rechtsverletzung entstehe für den Host-Provider die Pflicht, auch sinngleiche Inhalte zu prüfen und gegebenenfalls zu entfernen. Diese Pflicht sei verletzt worden, weil das zweite, nahezu inhaltsgleiche Video erst nach einem erneuten Hinweis gesperrt wurde. Die Sperrung hätte ohne eine weitere Abmahnung erfolgen müssen, machte das OLG Frankfurt deutlich.

Es stellte weiter klar, dass ein Host-Provider zwar grundsätzlich nicht verpflichtet sei, die von Nutzern eingestellten Inhalte vorab zu überwachen oder zu filtern. Ein solches generelles Monitoring wäre mit der Meinungs- und Kommunikationsfreiheit im Internet kaum vereinbar. In verschiedenen Situationen, etwa bei der Anwendung von KI-Systemen oder bei unterschiedlichen technischen und rechtlichen Rahmenbedingungen, können die Haftung und die Prüfpflichten unterschiedlich ausfallen. Sobald der Betreiber aber konkrete Kenntnis von einer klar erkennbaren Rechtsverletzung erhalten hat, müsse er den betreffenden Inhalt sperren und Vorkehrungen treffen, dass dieser nicht erneut in gleicher oder ähnlicher Form verbreitet wird. Das Problem der Abgrenzung zwischen zulässigen und unzulässigen Inhalten sowie die Wirksamkeit von Schutzmaßnahmen für Nutzer und Plattformen bleibt dabei eine Herausforderung. Diese Pflicht gehe über die bloße Entfernung des gemeldeten Inhalts hinaus.

Sinngleiche Inhalte: Erkennung und rechtliche Pflichten von Host-Providern

Sinngleiche Inhalte liegen dann vor, wenn sie trotz geringfügiger Änderungen z.B. anderer Schnitt, geänderte Farben, anderes Format oder leicht abgewandelter Text denselben rechtsverletzenden Gesamteindruck hervorrufen, so das OLG. Zur Erkennung solcher Inhalte kommen fortschrittliche Technik und die Auswertung großer Daten zum Einsatz, um Manipulationen zuverlässig zu identifizieren. Eine Plattform kann sich demnach nicht darauf berufen, dass ein neu hochgeladenes Video technisch nicht identisch ist, wenn es faktisch dieselbe täuschende Aussage enthält. Durch das Lernen von Algorithmen und die Anwendung von AI können Systeme zunehmend besser zwischen Wirklichkeit und manipulierten Inhalten unterscheiden. Ab dem Moment, in dem der Betreiber einmal über eine konkrete Rechtsverletzung informiert wurde, muss er angemessene technische und organisatorische Maßnahmen treffen, um Wiederholungen zu vermeiden. In der Praxis besteht jedoch das Problem, dass Erkennungsmethoden nicht in allen Situationen fehlerfrei funktionieren, weshalb effektive Schutzmaßnahmen besonders wichtig sind.

Für die Praxis bedeutet das, dass Host-Provider nicht nur auf Meldungen reagieren, sondern die Verbreitung irreführender oder manipulativer Inhalte auch aktiv bekämpfen müssen. Sie unterliegen zwar keiner allgemeinen Überwachungspflicht, aber einer situationsabhängigen Prüfpflicht. Diese entsteht, sobald der Betreiber über eine konkrete Rechtsverletzung informiert ist. Er muss dann nicht nur den konkreten Beitrag löschen, sondern auch prüfen, ob es auf der Plattform vergleichbare Inhalte gibt, die dieselbe Rechtsverletzung fortsetzen. Unterlässt er dies, kann er als sog. mittelbarer Störer auf Unterlassung in Anspruch genommen werden.

MTR Legal Rechtanwälte berät umfassend im IT-Recht.

Nehmen Sie gerne Kontakt zu uns auf!

MTR Legal Rechtsanwälte

Kurfürstendamm 11
10719 Berlin
Deutschland

MichaelRainer

+49 221 9999220

info@mtrlegal.com

www.mtrlegal.com

Portrait

MTR Legal Rechtsanwälte ist eine bundesweit und international tätige Full-Service-Wirtschaftskanzlei mit umfassender Expertise im Wirtschaftsrecht. Die Sozietät berät Unternehmen, institutionelle Investoren und vermögende Privatpersonen in den Bereichen Gesellschafts-, Steuer-, Handels-, Vertrags-, Vertriebs-, Kapitalmarkt- und Bankrecht. Proaktiv. Durchsetzungsstark. Erfolgreich. Diese Prinzipien prägen die Arbeitsweise der Kanzlei – vorausschauend, strategisch und wirtschaftlich fokussiert. MTR Legal arbeitet effizient, schnell, präsent und mit leading technology.

Mit Offices in Berlin, Düsseldorf, Frankfurt, Hamburg, Köln, Leipzig, München und Stuttgart sowie Representative Offices in London, Paris, Amsterdam und Singapore ist die Kanzlei international präsent. MTR Legal ist Mitglied im internationalen Netzwerk IR Global und wird regelmäßig von Handelsblatt und Best Lawyers empfohlen.

News-ID: 1296658 • Views: 379 (Stand: 11.05.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/1296658/Host-Provider-muss-Deep-Fake-Video-sperren.html