OLG München, Beschluss v. 17.03.2025 – 24 U 3020/24 e

Titel:

Kein Kontrollverlust nach Scraping-Vorfall bei Nutzung eines Fantasienamens

Normenkette:

DSGVO Art. 82

Leitsätze:

1. Ein Schadenersatzanspruch nach Art. 82 DSGVO setzt voraus, dass die den Schaden verursachende Handlung konkret durch den Betroffenen dargelegt werden, wobei er auch den Zeitpunkt der Handlung – etwa eines Scraping-Vorfalls – konkret darlegen muss. Dass dieser den genauen Zeitpunkt der schadensersatzbegründenden Handlung nur vermuteten kann, steht einem schlüssigen Vortrag nicht entgegen, soweit für die Vermutung hinreichende Anhaltspunkte vorgetragen werden. (Rn. 10) (redaktioneller Leitsatz)

2. Die Beklagte genügt ihrer sekundären Darlegungslast, wenn sie nachvollziehbar darlegt, dass der konkrete Zeitpunkt des Scraping-Vorfalls nicht mehr ermittelbar ist und keine Verpflichtung zur langfristigen Speicherung entsprechender Logdaten besteht. (Rn. 10) (redaktioneller Leitsatz)

3. Ein Kontrollverlust über personenbezogene Daten setzt voraus, dass der Betroffene konkrete Anhaltspunkte für eine missbräuchliche Verwendung darlegt. Eine abstrakte Möglichkeit des Missbrauchs genügt nicht, insbesondere wenn der Betroffene einer sozialen Plattform sein Profil unter einem Fantasienamen führt und kein Zusammenhang zwischen dem Scraping-Vorfall und späteren Belästigungen ersichtlich ist. (Rn. 14 – 15) (redaktioneller Leitsatz)

Schlagworte:

Berufung, Schadenersatzanspruch, Datenschutzgrundverordnung, Scraping, Kontrollverlust, Datenabgriff, Prozessuale Wahrheitspflicht

Vorinstanzen:

OLG München, Hinweisbeschluss vom 13.02.2025 – 24 U 3020/24 e
LG Memmingen, Endurteil vom 29.07.2024 – 26 O 1031/23

Fundstelle:

GRUR-RS 2025, 5371

Tenor

1. Die Berufung der Klagepartei gegen das Urteil des Landgerichts Memmingen vom 29.07.2024, Aktenzeichen 26 O 1031/23, wird zurückgewiesen.

2. Die Klagepartei hat die Kosten des Berufungsverfahrens zu tragen.

3. Das in Ziffer 1 genannte Urteil des Landgerichts Memmingen ist ohne Sicherheitsleistung vorläufig vollstreckbar.

4. Der Streitwert für das Berufungsverfahren wird auf 6.500,00 € festgesetzt.

Gründe

I.

1

Hinsichtlich der Darstellung des Sach- und Streitstandes wird auf den Tatbestand im angefochtenen Urteil des Landgerichts Memmingen vom 29.07.2024 Bezug genommen.

2

Im Berufungsverfahren wird beantragt:

Das angefochtene Urteil abzuändern und die Beklagte nach Maßgabe der Schlussanträge in erster Instanz zu verurteilen.

3
Die Beklagte beantragt

Klageabweisung.

4
Hinsichtlich des Vorbringens der Parteien im Berufungsverfahren wird auf die Berufungsbegründung vom 30.10.2024 (Bl. 7 – 31 d. Akte) und die Berufungserwiderung vom 09.12.2024 (Bl. 37 – 181 d. A.) Bezug genommen. Der Senat hat die Parteien mit Beschluss vom 13.02.2025 darauf hingewiesen, dass er beabsichtige, die Berufung durch Beschluss gem. § 522 ZPO zurückzuweisen. Der Kläger hat sich hierzu mit Schriftsatz vom 07.03.2025 geäußert.

II.

5
Die Berufung gegen das Urteil des Landgerichts Memmingen vom 29.07.2024, Aktenzeichen 26 O 1031/23, ist gemäß § 522 Abs. 2 ZPO zurückzuweisen, weil nach einstimmiger Auffassung des Senats das Rechtsmittel offensichtlich keine Aussicht auf Erfolg hat, der Rechtssache auch keine grundsätzliche Bedeutung zukommt, weder die Fortbildung des Rechts noch die Sicherung einer einheitlichen Rechtsprechung eine Entscheidung des Berufungsgerichts erfordert und die Durchführung einer mündlichen Verhandlung über die Berufung nicht geboten ist.

6
Zur Begründung wird auf den vorausgegangenen Hinweis des Senats Bezug genommen.

7
Auch die Ausführungen der Klagepartei vom 07.03.2025, die ohnehin nur einzelne Gesichtspunkte des Hinweises aufgreifen, geben zu keiner Änderung Anlass, zumal selbst bei ihrem Durchgreifen im Ergebnis keine Änderung veranlasst wäre.

Im einzelnen:

8
1. Die Klagepartei moniert hinsichtlich der Frage der zeitlichen Anwendbarkeit der DSGVO, es lägen keine konkreten Anhaltspunkte für einen Auslesen der Daten des Klägers bereits im Jahr 2018 vor.

9
Für ein Auslesen der Daten erst im Jahr 2019 bzw. nach Beginn der Geltung des DSGVO gibt es aber ebenfalls keine konkreten Anhaltspunkte. Soweit die Klagepartei vorträgt, es sei kein einziger anderer Fall bekannt, bei dem das Scraping 2018 stattgefunden haben soll, so hat der Senat hierzu keine Erkenntnisse. Aus der Akte ergibt sich nichts zu diesem Punkt. Es stellt sich vielmehr die Frage, ob überhaupt in irgendeinem Fall der konkrete Zeitpunkt bestimmt werden kann, zu dem das Scraping stattgefunden hat oder stets nur allgemein der Zeitraum angegeben werden kann, innerhalb dessen es stattgefunden haben kann.

10
Im vorliegenden erstinstanzlichen Urteil finden sich jedenfalls keine konkreten Feststellungen zum Zeitpunkt des Datenabgriffs im Fall des Klägers. Hier ist lediglich als unstreitig festgestellt, dass es jedenfalls ab 2019 zu Scraping von Benutzerdaten von der Plattform der Beklagten kam. Dies schließt einen Beginn der Scrapingvorfälle bereits im Jahr 2018 nicht aus. Darauf, ob die Beklagte konkret bestritten hat, dass das Scraping betreffend des Klägers im Jahr 2018 erfolgte, kommt es nicht an, weil zum maßgeblichen Zeitpunkt der letzten mündlichen Tatsachenverhandlung bereits kein schlüssiger Vortrag der Klagepartei dazu vorlag, dass der sie betreffende Vorfall zu einem Zeitpunkt stattgefunden habe, als die DSGVO bereits anwendbar war. Eine Klage ist schlüssig, wenn ihr Tatsachenvortrag, seine Richtigkeit unterstellt, geeignet ist, den Klageantrag sachlich zu rechtfertigen (Zöller, ZPO, 35. Aufl. 2024, vor § 253, Rn. 23). Dazu gehört bei Geltendmachung eines Schadenersatzanspruchs auch der Vortrag von Tatsachen, aus denen sich ergibt, dass die mögliche zum Schadenersatz verpflichtende Handlung, die den Schaden kausal verursacht hat, zu einem Zeitpunkt stattfand, als die entsprechende Norm bereits Geltung beanspruchte. Zwar ist, sofern man von einem Verstoß der Beklagten gegen den Grundsatz der Datenminimierung nach Art. 5 DSGVO ausgehen sollte, von einem durchlaufenden Pflichtverstoß der Beklagten bis zur Änderung der Voreinstellungen auszugehen. Kausal für den möglichen Schaden des Klägers kann dieser mögliche

Verstoß aber nur bis zum Zeitpunkt des konkreten ihn betreffenden Scraping-Vorfalls sein. Dies ist der maßgebliche Zeitpunkt. (vgl. BGH, 24.10.2024, VI ZR 10/24 – Rn. 90). Der Kläger gab ausdrücklich an, man kenne den genauen Zeitpunkt des Datenabgriffs nicht und äußerte mehrfach eine bloße und auch nicht näher begründete Vermutung dahingehend, dass es wohl im September 2019 gewesen sei. Dass die Klagepartei den genauen Zeitpunkt nicht weiß, hätte sie nicht an einem konkreten, schlüssigen Vortrag gehindert. Denn es dürfen auch lediglich vermutete Tatsachen als Behauptung eingeführt werden, ohne dass dies einen Verstoß gegen die prozessuale Wahrheitspflicht nach § 138 Abs. 1 ZPO darstellen würde, soweit die Klagepartei hierfür hinreichende Anhaltspunkte vortragen kann. (BGH, NJW 1995, 2111 (2112); NJW-RR 2002, 1419/1420; OLG Karlsruhe, 02.02.2023, 14 U 224/21 Rn. 61). Vorliegend hat der Kläger aber keine konkrete Tatsachenbehauptung eingeführt, sondern es bei dem Vortrag einer bloßen Vermutung belassen. Er hat auch keine konkreten Anhaltspunkte dafür vorgetragen, warum der Abgriff seiner Daten gerade erst im September 2019 erfolgt sein soll und nicht vor 25.05.2018 erfolgt sein kann. Auch dafür, dass es nur einen einzigen Abgriff von Daten von der Plattform der Beklagten im September 2019 gegeben hat, bei dem alle Daten abgegriffen wurden, ist weder etwas vorgetragen noch ist dies naheliegend – allein schon angesichts der schieren Anzahl der nach Angaben der Klagepartei betroffenen Profile (533 Millionen). Soweit die Klagepartei annimmt, dass sich hinsichtlich des nunmehr von der Beklagtenpartei dargelegten, relevanten Zeitraums, in dem es zu den Scraping-Vorfällen gekommen sein soll, eine Abweichung zur Pressemeldung der Beklagten vom 06.04.2021 ergebe, ist bereits nicht nachvollziehbar, worin diese Abweichung bestehen soll. In der genannten Pressemeldung ist lediglich angegeben, dass vor September 2019 durch böswillige Akteure Daten von der Plattform gescrapt worden seien. Die Beklagte habe die Funktion geändert, als ihr bewusst worden sei, dass böswillige Akteure im Jahr 2019 die Funktion zum Scrapen nutzten. Diese Pressemeldung sagt also lediglich etwas dazu, ab wann die Funktion, die das Scrapen ermöglichte, verändert wurde ("Wir haben dieses Problem im Jahr 2019 behoben) und wann der Beklagten die missbräuchliche Nutzung bewusst wurde. Dazu seit wann/ab welchem Anfangszeitpunkt konkret das Scraping möglich war und erfolgte, sagt diese Pressemitteilung nichts. Ob die Beklagte zum Zeitpunkt dieser Pressemeldung den Anfang des Zeitraums, in dem Abgriffe erfolgten, überhaupt eingrenzen konnte, ist ebenfalls nicht bekannt. Davon abgesehen ist, wollte man (wie nicht) von einer hinreichend schlüssigen Behauptung des Klägers hinsichtlich eines Abgriffs im September 2019 ausgehen, dieser Zeitpunkt durch den gegenteiligen Vortrag der Beklagtenpartei bestritten. Die Beklagte hat entgegen dem Vortrag der Klagepartei, jedenfalls im vorliegenden Verfahren, nicht gemutmaßt, dass einzelne Daten ja vielleicht vor Mai 2018 ausgelesen worden sein könnten. Die Beklagte hat vielmehr im vorliegenden Verfahren den Zeitraum angegeben, in dem der Scraping-Vorfall stattgefunden haben könne (Januar 2018 – September 2019). Dies sei der maßgebliche Zeitraum. Sie hat auch erklärt, warum sie den konkreten Zeitpunkt eines Scrapingvorfalls jeweils nicht mitteilen kann (Sie habe keine Kopie der Rohdaten, die gescrapt wurden oder von Logdaten für den fraglichen Zeitraum). Gerade letzteres ist ohne weiteres plausibel, denn es ist keine Rechtsgrundlage ersichtlich, aufgrund derer die Beklagte berechtigt sein könnte, über mehrere Jahre sämtliche Logdaten zu speichern (siehe hierzu: Art. 4 Nr. 2, 5, 6 DSGVO). An die Vorgaben der DSGVO musste die Beklagte nach dem 25.08.2018 auch bereits ggf. vorher stattgefundene Verarbeitungen/Speicherungen anpassen. Die Beklagte hat mit ihren Angaben ihre sekundäre Darlegungslast erfüllt (so auch: OLG Stuttgart, 04.12.2024 4 U 97/24 Rn. 20 in einem vergleichbaren Fall). Soweit die Klagepartei vorträgt, die Beklagte müsse die Zeitpunkte der Scrapingvorfälle nachvollziehen können, weil sie behaupte, nachvollziehen zu können, wessen Daten gescrapt wurden, so findet sich eine solche Behauptung der Beklagten in der vorliegenden Akte ebenfalls an keiner Stelle. Solches ergibt sich auch nicht aus der Anlage B 16 (= Anlage K2, Schreiben der Beklagten), in dem die Beklagte dargelegt, es sei … auf Grundlage der bislang vorgenommenen Analysen gelungen, der Nutzer-ID des Klägers folgende Datenkategorien zuzuordnen, die nach dem Verständnis von Meta in den durch Scraping abgerufenen Daten erscheinen und mit den auf dem … Profil des Klägers verfügbaren Informationen übereinstimmen (die Datenpunkte). Sofern man dies nicht ohnehin lediglich als Angabe derjenigen Datenkategorien versteht, die im jeweiligen Fall potentiell gescrapt worden sein könnten (weil diese eben öffentlich einsehbar waren), so könnte dies allenfalls noch so interpretiert werden, dass die Beklagte bei der von ihr beschriebenen Suche ihres External Data Misuse-Teams nach Daten im Internet, die von ihrer Plattform gescrapt sein könnten (siehe hierzu Anlage B 12), entsprechende Daten des Klägers gefunden hat. Dafür, dass sich aus solchen im Internet aufgefundenen, gescrapten Daten der Abgriffszeitpunkt ermitteln lassen würde, ist nichts ersichtlich und dies liegt auch völlig fern.

Soweit die Klagepartei ein Urteil des LG München I zitiert, wonach die Vorgängernorm der Datenschutzgrundverordnung, VO EU 2016/679, in ihrem Art. 6 entsprechende Regelungen für die Verarbeitung enthalte, so sind die Ausführungen in diesem Urteil bereits im Ansatz falsch. Bei der Verordnung EU 2016/679 vom 27.04.2016 handelt es nicht um eine Vorgängernorm der Datenschutzgrundverordnung, sondern es handelt sich um die Datenschutzgrundverordnung selbst. Dies ist unschwer zu ersehen aus Art. 99 Abs. 2 der Verordnung, der ihre Geltung zum 25.05.2018 regelt. Vorgängernorm der Datenschutzgrundverordnung war vielmehr die Richtlinie 95/46 EG, die mit Art. 94 DSGVO mit Wirkung vom 25.05.2018 aufgehoben wurde (siehe hierzu auch: BeckOK Datenschutzrecht, DSGVO Art. 94 Rn. 1). Diese Richtlinie wiederum wurde durch das damalige Bundesdatenschutzgesetz umgesetzt. Zum damaligen § 7 BDSG wurde bereits im Hinweisbeschluss ausgeführt (siehe hierzu auch BeckOK, 23. Edition, Stand 01.08.2017 Rn. 55). Der Irrtum des LG München I ist wohl dadurch zu erklären, dass die Datenschutzgrundverordnung aus dem Jahr 2016 stammt und zwischen ihrem Inkrafttreten und dem Beginn ihrer Geltung zwei Jahre liegen, um die nötigen Anpassungen bei den Verarbeitern bzw. im nationalen Recht zu ermöglichen.

12
Davon abgesehen scheitern die Ansprüche des Klägers nicht nur an der Problematik des zeitlichen Anwendungsbereichs. Wie ebenfalls bereits ausgeführt, sind auch die tatbestandlichen Voraussetzungen für einen Schadenersatzanspruch nach Art. 82 DSGVO nicht erfüllt.

13
2. Die Ausführungen der Klagepartei zum Punkt Betroffenheit sind vor dem Hintergrund, dass, wie bereits im Hinweisbeschluss dargelegt, die grundsätzliche Betroffenheit des Klägers aufgrund der nicht mit einem Tatbestandsberichtigungsantrag angegriffenen Feststellungen des erstinstanzlichen Urteils feststeht, nicht nachvollziehbar. Wie ebenfalls bereits ausgeführt, geht der Senat deshalb davon aus, dass jedenfalls die immer öffentlichen Nutzereinstellungen und die Telefonnummer von dem Scraping-Vorfall betroffen waren. Soweit der Kläger moniert, die Beklagte dürfe nicht mit „Nichtwissen“ bestreiten, welche Daten in dem jeweiligen Profil enthalten sind, so ist dies richtig. Aber das hat die Beklagte – jedenfalls im vorliegenden Verfahren – auch nicht getan. Die Beklagte hat vielmehr, unter Vorlage eines Screenshots des … (Anlage B 15) der Klagepartei und unter Bezugnahme auf ihre Mitteilung hinsichtlich der (möglicherweise) betroffenen, weil auf dem Profil der Klagepartei verfügbaren, Informationen (Anlage B 16), konkret bestritten, dass im konkreten Fall weitere Daten, wie etwa E-Mail-Adresse, Geburtsdatum u. a. betroffen gewesen sein sollen. Der Kläger hat demgegenüber nur ausgeführt, dass alle Daten betroffen gewesen seien, die auf dem Profil auf „öffentlich“ gestellt waren. Dies seien zumindest Vor- und Nachname sowie …ID und Handynummer.

14
3. Hinsichtlich der Frage des Kontrollverlusts vermischt die Klagepartei die Frage des schlüssigen Vortrags eines Kontrollverlusts mit der Frage des Nachweises eines solchen. Dass der Vortrag der Klagepartei hinsichtlich einer gezielten Weitergabe seiner Telefonnummer ausreichend für einen schlüssigen Vortrag dazu war, dass und warum der Kläger zum Zeitpunkt des Scraping-Vorfalls noch die Kontrolle über seine Daten gehabt haben will, hat der Senat in seinem Beschluss – unter ausdrücklicher Bezugnahme auf die Entscheidung des Bundesgerichtshofs, aus der Klägervertreter nunmehr zitiert – bejaht. Allerdings verbleibt das Risiko der Nichterweislichkeit eines Kontrollverlusts – wie der Bundesgerichtshof in derselben Entscheidung ausdrücklich klarstellt, beim Anspruchsteller. Soweit die Klagepartei behauptet, das Gericht habe für die Beklagte die normale Nutzung und Weitergabe der Handynummer bestritten, so ist es völlig unerfindlich, woraus der Klägervertreter derartiges ableiten will. Die Beklagtenpartei hat (unschwer erkennbar) das Eintreten eines Kontrollverlustes gerade aufgrund des Scrapingvorfalls mehrfach bestritten, wie sich aus den im Hinweisbeschluss bereits beispielhaft zitierten Fundstellen ergibt. So führt die Beklagte etwa in der Klageerwiderung (Bl. 67 d. A.) aus: „Selbst wenn die Klagepartei in begrenztem Umfang einen Verlust der Kontrolle über ihre personenbezogenen Daten erlitten hätte (was bestritten wird) …“ Die Lektüre auch der weiteren Fundstellen wird dem Klägervertreter anheimgestellt. Das Bestreiten der Beklagten ist auch ohne weiteres substantiiert genug, weil die Beklagte ausgeführt hat, dass und warum die E-Mail-Adresse sich nicht unter den von der Plattform der Beklagten gescrapten Daten befunden hat (siehe hierzu bereits oben), der Kläger aber auch einen Anstieg von Spam-Mails beklagt (siehe Anlage K4, Fragebogen). Dies stellt ein Indiz für ein mögliches Datenleck an anderer Stelle dar, durch das natürlich auch andere Daten als die E-Mail-Adresse, wie die Handynummer, bereits abgeflossen sein könnten. Dies gilt um so mehr, als der Kläger sein … Profil unter einem Fantasienamen führt, die in der Klageschrift angegebene E-

Mail-Adresse aber auf den richtigen Namen des Klägers lautet. Die E-Mail-Adresse kann also auch nicht durch Probieren von Kombinationen aus Namen und den Endungen verschiedener Mail-Anbieter herausgefunden worden sein. Der Kläger konnte ausweislich des vorgelegten Fragebogens außerdem überhaupt nicht zeitlich einordnen, wann er einen Anstieg von derartigen Belästigungen bemerkte, so dass auch durch eine zeitliche Korrelation kein Zusammenhang zu einem Scraping-Vorfall bei der Beklagten hergestellt werden kann. Ggf. hätte eine Anhörung des Klägers weitere Aufklärung bringen, bzw. zu einer entsprechenden Überzeugung des Gerichts führen können. Der Kläger ist jedoch, trotz ordnungsgemäßer Ladung und Anordnung des persönlichen Erscheinens des Klägers – ausdrücklich auch zur Sachaufklärung – nicht erschienen.

15
4. Dazu, warum der Kläger die Kontrolle über die von ihm bei … eingestellten, öffentlich sichtbaren Daten nicht in Zukunft durch eine Schließung des Accounts oder Änderung der öffentlich einsehbaren Daten zurück gewinnen kann, wurde ebenfalls bereits in Hinweisbeschluss ausgeführt. Ebenfalls wurde bereits dargelegt, dass aktive Telefonnummern auch auf andere Weise ermittelt werden können. Im übrigen ist die entscheidende Information, die durch das Scraping erlangt werden konnte und die das Risiko eines Missbrauchs birgt, wie ebenfalls bereits dargelegt wurde, die Veröffentlichung des Namens des Betroffenen in Verbindung mit seiner Telefonnummer (so auch BGH, 18.11.2024, VI ZR 10/24 Rn. 49). Die Besonderheit im vorliegenden Fall ist aber, dass der Kläger sein Profil unter einem Fantasienamen führt. Deswegen ist durch das Scraping gerade keine Verknüpfung seiner Telefonnummer mit seinem (richtigen) Namen erfolgt. Es ist weder ersichtlich, dass die Verknüpfung der Telefonnummer mit dem Fantasienamen Betrugsversuche ermöglichen würde, noch, dass ein Rückschluss auf den richtigen Namen des Klägers möglich wäre. Es ist daher bereits nicht ersichtlich, worin im vorliegenden Fall ein möglicher Kontrollverlust liegen soll.

16
4. Dass auf einem Kontrollverlust aufgrund eines Scraping-Vorfalls resultierende missbräuchliche Anrufe bzw. SMS und Spam-Emails, bzw. eine Steigerung solcher Vorfälle, geeignet wären, einen Schaden darzustellen ist, richtig. Vorliegend besteht aber die Problematik (siehe oben), dass sich aus den Schilderungen des Klägers gerade nicht herleiten lässt, dass diese Belästigungen bzw. deren Anstieg auf einem Kontrollverlust durch einen Scraping-Vorfall bei der Beklagten beruhen. Darin unterscheidet sich der Fall im übrigen auch von dem vom Bundesgerichtshof entschiedenen Fall. Außerdem ist erneut hervorzuheben, dass der Bundesgerichtshof lediglich zu entscheiden hatte, was für einen schlüssigen Vortrag hinsichtlich eines Schadens ausreicht, nicht aber, ob der Kläger im dortigen Fall einen solchen bewiesen hat.

17
5. Da der Kläger zu den Hinweisen des Senats zu etwaigen Schadenersatzansprüchen auf Grundlage des nationalen Rechts, zu dem Feststellungsantrag, dem Unterlassungs- und dem Auskunftsantrag und dazu, warum das Verfahren auch nicht auszusetzen war, nichts mehr vorgetragen hat, waren hierzu keine weiteren Ausführungen veranlasst.

18
Die Kostenentscheidung beruht auf § 97 Abs. 1 ZPO.

19
Die Feststellung zur vorläufigen Vollstreckbarkeit des angefochtenen Urteils erfolgte gemäß § 708 Nr. 10 ZPO.

20
Der Streitwert für das Berufungsverfahren wurde in Anwendung der §§ 47, 48 GKG bestimmt. Hierbei wurde für die beiden Anträge auf Schadenersatz (Ziff. 1 und 2), entsprechend der vom Kläger geltend gemachten Beträge, insgesamt 4.000,00 € angesetzt, für den Feststellungsantrag (Ziff. 3) 500,00 €, für die Unterlassungsanträge (Ziff. 4 a und b), jeweils 750,00 € und für den Auskunftsantrag (Ziff. 5) 500,00 €. Somit ergibt sich insgesamt ein Streitwert von 6.500,00 €.