

5 O 192/23



Verkündet am 02.07.2024

als Urkundsbeamtin
der Geschäftsstelle

LANDGERICHT DORTMUND

IM NAMEN DES VOLKES

URTEIL

In dem Rechtsstreit

Klägers,

Prozessbevollmächtigte:

Rechtsanwälte WBS.LEGAL, Eu-
pener Straße 67, 50933 Köln,

gegen

die Meta Platforms Ireland Limited, vertreten durch die Mitglieder des
Board Directors, Merrion Road, Dublin 4 X2K5, Irland,

Beklagte,

Prozessbevollmächtigte:

Rechtsanwälte Freshfields, Bruck-
haus, Deringer, Bockenheimer An-
lage 44, 60322 Frankfurt,

hat die 5. Zivilkammer des Landgerichts Dortmund auf die mündliche Verhandlung vom 11.06.2024 durch die Richterin am Landgericht als Einzelrichterin

für **R e c h t** erkannt:

1. Die Beklagte wird verurteilt, an den Kläger immateriellen Schadensersatz in Höhe von 100 € nebst Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 21.07.2023 zu zahlen.
2. Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger alle weiteren Schäden zu ersetzen, die ihm durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte, entstanden sind und noch entstehen werden.
3. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000 €, ersatzweise Ordnungshaft, zu vollstrecken an ihrem gesetzlichen Vertreter, oder Ordnungshaft bis zu 6 Monaten, zu vollstrecken an ihrem gesetzlichen Vertreter, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, die Telefonnummer des Klägers zu verarbeiten, wenn dieser seine Einwilligung hierzu nicht ausdrücklich erteilt hat.
4. Im Übrigen wird die Klage abgewiesen.
5. Die Kosten des Rechtsstreits tragen der Kläger zu 49 % und die Beklagte zu 51 %.

6. Das Urteil ist vorläufig vollstreckbar, für den Kläger jedoch nur gegen Sicherheitsleistung in Höhe von 5.000 €. Der Kläger darf die Vollstreckung durch Sicherheitsleistung in Höhe von 110 % des auf Grund des Urteils vollstreckbaren Betrages abwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 110 % des jeweils zu vollstreckenden Betrages leistet.

Tatbestand

Der Kläger verlangt von der Beklagten Schadensersatz, Unterlassung und Auskunft wegen mehrerer von ihm behaupteter Verstöße gegen die Datenschutzgrundverordnung (DSGVO).

Der Kläger nutzt die von der Beklagten betriebene Social-Media-Plattform facebook.com (im Folgenden: facebook). Die Plattform der Beklagten ermöglicht es ihren Nutzern, persönliche Profile für sich zu erstellen und diese mit Freunden zu teilen. Auf diesen persönlichen Profilen können die Nutzer Angaben zu verschiedenen Daten zu ihrer Person machen und im von der Beklagten vorgegebenen Rahmen darüber entscheiden, welche anderen Gruppen von Nutzern auf ihre Daten zugreifen können. Unterschieden dabei wird zwischen „privat“, „öffentlich“, „Freunde“ und „Freunde von Freunden“. Der Name, das Geschlecht und die Nutzer ID sind immer öffentliche Nutzerinformationen, d.h. sie sind allen Nutzern von facebook zugänglich, eine andere Einstellung kann auch nicht gewählt werden. Im Übrigen aber steht es den Nutzern frei, die Einstellungen jederzeit zu ändern und zu bestimmen, ob und wem welche Daten zur Einsicht bereitgestellt werden. Trifft der Nutzer keine Auswahl, bleibt es bei den Standardeinstellungen.

Unter der Rubrik „Bestimme, wer dich finden kann“ kann der Nutzer einstellen, auf welche Weise er von anderen gefunden werden kann. Dort war während des streitgegenständlichen Streitraums standardmäßig „alle“ eingestellt, d.h. dass über die Telefonnummer jeder den entsprechenden Nutzer finden kann. Dies galt auch dann, wenn in dem persönlichen Profil des Nutzers die Telefonnummer nicht öffentlich freigegeben war.

Ferner gab es eine Funktion zum Importieren von Kontakten. Importierte ein Nutzer seine Kontakte auf facebook, wurden ihm – sofern die Standardeinstellung in der Rubrik „Bestimme, wer dich finden kann“ auf „alle“ nicht ge-

ändert worden war – sämtliche Profile derjenigen Facebook-Nutzern angezeigt, deren Telefonnummern in seinen Kontakten vorhanden waren.

Anlass für die Klage ist ein Scraping-Vorfall aus 2019, bei dem Daten von ca. 533 Millionen Nutzern von facebook abgegriffen worden sind, so auch Daten des Klägers. Indem eine Vielzahl von Telefonnummern in ein virtuelles Adressbuch eingegeben wurde und die Funktion zum Importieren von Kontakten genutzt wurde, gelang es Unbekannten, die Telefonnummern konkreten Facebookprofilen zuzuordnen, soweit in diesen Profilen in der Rubrik „Bestimme, wer dich finden kann“ die Einstellung „alle“ gewählt war. Die Unbekannten kopierten sodann die öffentlich einsehbaren Informationen aus dem betreffenden Nutzerprofil und fügten die Telefonnummer den abgerufenen, öffentlich einsehbaren Daten sodann hinzu. Im April 2021 wurden diese Daten im Internet veröffentlicht.

Wegen dieses Vorfalls verhängte die irische Datenschutzbehörde DPC gegen die Beklagte am 28.11.2022 eine Geldbuße in Höhe von 265 Millionen €, die jedoch nicht rechtskräftig ist.

Der Kläger behauptet, im Darknet seien seine Telefonnummer, die Facebook-ID, sein Name, sein Geschlecht, sein Wohnort und sein Arbeitgeber zu finden. Er habe dadurch einen erheblichen Kontrollverlust über seine Daten erlitten und sei in einem Zustand großen Unwohlseins und großer Sorge über einen möglichen Missbrauch seiner Daten gewesen. Dies habe sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannt Nummern und Adressen manifestiert. Seit April 2021 erhalte er unregelmäßig unbekannte Kontaktversuche via sms und E-Mail, diese enthielten Nachrichten mit offensichtlichen Betrugsversuchen und potentiellen Virenlinks.

Der Kläger meint, die Einstellungen zur Sicherheit der Telefonnummer seien so undurchsichtig und kompliziert gestaltet, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne. Die Beklagte verletzte dadurch ihre Pflichten aus Art. 5 a bis c und g, Art. 15 Abs. 1 und 2, Art. 32, Art. 34 Abs. 1 und 2 DSGVO. Er behauptet, aufgrund der Vielzahl an Einstellungsmöglichkeiten sei mit hoher Wahrscheinlichkeit zu erwarten, dass ein Nutzer die voreingestellten Standardeinstellungen beibehalte.

Er meint, den Voreinstellungen komme besondere Bedeutung zu, ein „opt-out“ genüge nicht. Es müsse die datenschutzfreundlichste Variante als Standardeinstellung vorgesehen werden.

Er behauptet, die Beklagte habe keinerlei Sicherheitsmaßnahmen vorgehalten, um ein Ausnutzen des bereitgestellten Tools zum Import von Kontakten zu verhindern. Es seien keine Sicherheitscapchas verwendet worden, um sicherzustellen, dass es sich bei der Anfrage um die Anfrage eines Menschen und nicht um eine automatisch generierte Anfrage handelt. Ebenso wenig sei ein Mechanismus zur Überprüfung der Plausibilität der Anfragen bereitgehalten worden, etwa indem ungewöhnlich viele Anfragen derselben IP-Adresse auf einmal geblockt werden oder Adressbücher mit auffälligen Telefonnummernabfolgen automatisch abgelehnt werden.

Er meint, ein Verstoß liege auch darin, dass die Beklagte ihn zu keinem Zeitpunkt darüber informiert habe, dass seine Informationen durch Dritte entwendet und veröffentlicht wurden.

Der Kläger beantragt mit der am 20.07.2023 zugestellten Klage,

1. die Beklagte zu verurteilen, an ihn immateriellen Schadensersatz in angemessener Höhe zu zahlen, dessen Höhe in das pflichtgemäße Ermessen des Gerichts gestellt wird, mindestens jedoch 1.000,00 €

nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz,

2. festzustellen, dass die Beklagte verpflichtet ist, ihm alle künftigen Schäden zu ersetzen, die ihm durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte, entstanden sind und/oder noch entstehen werden,
3. die Beklagte zu verurteilen, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 €, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,
 - a. personenbezogene Daten des Klägers, namentlich Telefonnummer, FacebookID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern,
 - b. seine Telefonnummer auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch Ver-

wendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird,

4. die Beklagte zu verurteilen, ihm Auskunft über die ihn betreffenden personenbezogenen Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte meint, es handele sich schon nicht um eine unbefugte Offenlegung, weil die abgerufenen und veröffentlichten Informationen aufgrund der Einstellungen, die der Kläger vorgenommen habe, bereits öffentlich einsehbar gewesen seien. Auch wenn die Art des Abrufs der Daten gegen die Nutzungsbedingungen verstoßen habe, gelte dies nicht für den Zugang als solchen.

Die Beklagte meint, es habe dem Hauptzweck von facebook, nämlich den Nutzern zu helfen, einander zu finden und sich mit Freunden, der Familie und bedeutsamen Gemeinschaften zu verbinden, entsprochen, die Einstellung für die Suchbarkeit von Telefonnummern auf „Alle“ als Standard-Einstellung vorzusehen. Die Verarbeitung von Kontaktdaten wie E-Mail-Adresse oder Telefonnummer sei erforderlich, um diesen Verarbeitungszweck, nämlich die gegenseitige Auffindbarkeit und Vernetzung, zu erreichen.

Sie behauptet, sie habe sowohl über Übertragungsbegrenzungen als auch eine Bot-Erkennung verfügt. Es gebe jedoch keine formellen oder vorgeschriebenen Branchen- oder Industriestandards zur Bekämpfung von Scraping.

Sie meint, Unterlassung könne der Kläger schon deswegen nicht verlangen, weil die Regelungen der DSGVO im Hinblick auf die Rechte der von Datenschutzverstößen Betroffenen abschließend seien.

Entscheidungsgründe

I.

Die Klage ist überwiegend zulässig, jedoch nur in dem aus dem Tenor ersichtlichen Umfang begründet.

1.

Die internationale Zuständigkeit deutscher Gerichte folgt aus Art. 79 Abs. 2 Satz 1 und 2 DSGVO bzw. Art. 7 Nr. 2, Art. 63 Abs. 1 Buchst. a, c, Art. 63 Abs. 2 EuGVVO (vgl. OLG Hamm, Urteil vom 15. August 2023 - 7 U 19/23, juris Rn. 45 f.).

Die sachliche Zuständigkeit ergibt sich aus §§ 23, 71 GVG, nachdem der Gegenstandswert mehr als 5.000 € beträgt.

Den Antrag zu 2 hat die Kammer dabei mit 500 € bewertet.

Die Anträge zu 3a und 3b sind nach Ansicht der Kammer mit insgesamt 5.000 € zu bewerten. Diese gehen über das Interesse aus den Anträgen zu

1 und 2 hinaus. Während die Anträge zu 1 und 2 lediglich einen bereits eingetretenen bzw. noch eintretenden Schaden so gut wie möglich ausgleichen sollen, zielen die Anträge zu 3a und 3b darauf ab, weitere Schäden gar nicht erst eintreten zu lassen. Das Interesse daran ist deutlich höher als das Interesse an einer bloßen Kompensation von Schäden, weil gerade immaterielle Schäden durch Geldzahlung nur ausgeglichen, aber nicht ungeschehen gemacht werden können.

Der Antrag zu 4 war mit 300 € zu bewerten angesichts des Umstands, dass nur noch die Auskunft über die Identität der Scraper aussteht und nicht zu erwarten steht, dass der Kläger mit solchen Informationen mit Erfolg gegen die Scraper vorgehen können.

2.

Die Klage ist mit Ausnahme des Klageantrags zu 3a zulässig.

a)

Der Klageantrag zu 1 ist nicht auf unterschiedliche Lebenssachverhalte gestützt. Der Kläger macht Schadensersatz aufgrund des Umstands geltend, dass seine Daten im Internet veröffentlicht worden sind. Dass dies zeitlich auf zwei Umständen beruht, einerseits dem Scraping-Vorfall in 2019 und andererseits der Veröffentlichung der so gewonnenen Daten in 2021, führt nicht dazu, dass es sich um unterschiedliche Lebenssachverhalte handeln würde. Es handelt sich vielmehr immer noch um einen einheitlichen Lebenssachverhalt, der sich lediglich in zwei Schritten vollzogen hat.

b)

Der Klageantrag zu 2 ist zulässig. Insbesondere ist es unschädlich, dass im Klageantrag zu 2 die Feststellung der Ersatzpflicht für künftige Schäden begehrt wird, die „entstanden sind“. Künftige Schäden können zwar nicht bereits entstanden sein, so dass der Antrag dem Wortsinne nach widersprüchlich ist.

Aus der Klagebegründung wird aber deutlich, dass der Kläger nicht die Ersatzpflicht für künftige, sondern für weitere, d.h. über den Antrag zu 1 hinausgehende Schäden festgestellt wissen möchte. Insoweit besteht auch ein Feststellungsinteresse, weil die Möglichkeit besteht, dass die von Dritten veröffentlichten Daten weiterverwendet werden. Da der Kläger vorliegend die Verletzung eines absoluten Rechts, nämlich der informationellen Selbstbestimmung, geltend macht, genügt die bloße Möglichkeit eines weiteren Schadenseintritts, die hier zu bejahen ist. Allein der Umstand, dass bisher ein solcher Schaden nicht entstanden ist, steht dem aus Sicht der Kammer nicht entgegen (anders OLG Hamm aaO, juris Rn. 215).

Der Antrag ist auch hinreichend bestimmt. Eine hinreichende Bestimmtheit ist für gewöhnlich gegeben, wenn auf die konkrete Verletzungshandlung Bezug genommen wird und der Klageantrag zumindest unter Heranziehung des Klagevortrags unzweideutig erkennen lässt, in welchem Verhalten das zum Schadensersatz begründende Geschehen zu sehen sein soll (vgl. BGH, Urteil vom 8. November 2018 - I ZR 108/17, GRUR 2019, 627 [juris Rn. 15] – Deutschland-Kombi). Aus dem Klagevortrag wird hinreichend deutlich, dass der Kläger den „Scraping“-Vorfall aus 2019 zur Grundlage seines Schadensersatzanspruchs macht.

c)

Der Klageantrag zu 3a hingegen ist unbestimmt und damit unzulässig.

Nach § 253 Abs. 2 Nr. 2 ZPO darf ein Klageantrag - und nach § 313 Abs. 1 Nr. 4 ZPO eine darauf beruhende Verurteilung - nicht derart undeutlich gefasst sein, dass der Streitgegenstand und der Umfang der Prüfungs- und Entscheidungsbefugnis des Gerichts nicht klar umrissen sind, der Beklagte sich deshalb nicht erschöpfend verteidigen kann und im Ergebnis dem Vollstreckungsgericht die Entscheidung darüber überlassen bleibt, was dem Beklagten verboten ist (st. Rspr.; vgl. BGH, Urteil vom 11. Februar 2021 - I ZR 227/19, GRUR 2021, 758 [juris Rn. 13] - Rechtsberatung durch Architektin, mwN).

Diesen Vorgaben wird der Klageantrag zu 3a nicht gerecht, weil er den Begriff „unbefugte Dritte“ verwendet. Wer jedoch zu den unbefugten Personen gehören soll, wird aus dem Antrag nicht ersichtlich. Mangels Bezugnahme auf eine konkrete Verletzungshandlung wird dies auch im Rahmen der Klagebegründung nicht deutlich. Insbesondere greift der Kläger im Rahmen der Klagebegründung nicht nur den Umstand an, dass es Scrapern gelungen ist, seine Daten mithilfe der Software zum Importieren von Kontakten zu erlangen und zu veröffentlichen. Er macht vielmehr auch geltend, seine Einwilligung zur Weitergabe der Daten sei nicht wirksam, zum einen wegen unübersichtlicher Informationen, zum anderen wegen der Voreinstellungen. Bei dieser Sachlage bleibt unklar, ob der Kläger mit dem Klageantrag zu 3a eine Unterlassung nur hinsichtlich von Scrapern oder aber bezüglich aller Personen verlangen möchte. Auch die weitere Eingrenzung „ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern“ führt nicht zu einer hinreichenden Konkretisierung, sondern vielmehr zu einer weiteren Unbestimmtheit. Die Frage, zu welchem Zweck die Nutzung der Software zum Importieren von Kontakten erfolgt, lässt sich im Vorfeld überhaupt nicht bestimmen; die Beklagte hat daher keine Möglichkeit, zu ersehen, wem sie die Daten des Klägers zugänglich machen darf und wem nicht.

Dem Kläger wäre eine nähere Bezeichnung auch möglich gewesen, allein schon durch die Bezugnahme auf die konkrete Verletzungshandlung.

d)

Der Klageantrag zu 3b hingegen ist zulässig.

Dieser ist nach Auffassung der Kammer nicht auf ein aktives Tun gerichtet (so aber OLG Hamm aaO, juris Rn. 238 ff.). Mit diesem Antrag begehrt der Kläger vielmehr allein ein Unterlassen; die Beklagte soll es unterlassen, seine Daten zu verarbeiten. Die weiteren Ausführungen („eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird“) stellen Beschränkungen dieses Antrags dar, d.h. sie geben Umstände wieder, bei deren Vorliegen das Unterlassungsgebot nicht gelten soll. Dies bedeutet jedoch nicht, dass der Kläger damit auf Erfüllung dieser Bedingungen klagt oder klagen möchte. Der Kläger trägt damit lediglich dem Umstand Rechnung, dass ein Unterlassungsbegehren nicht so weit gefasst sein darf, dass es auch erlaubte Verhaltensweisen umfasst (vgl. BGH, Urteil vom 29. Juli 2021 - I ZR 162/19, juris Rn. 13 mwN).

Der Beklagten bleibt es auch nach dem Antrag des Klägers unbenommen, die Daten des Klägers nicht zu verarbeiten; dann unterliegt sie keinen weiteren Verpflichtungen.

3.

Die Klage ist hinsichtlich der begehrten Unterlassung und des Schadensersatzanspruchs teilweise begründet, im Übrigen unbegründet.

a)

Dem Kläger steht gegen die Beklagte ein Anspruch auf immateriellen Schadensersatz aus Art. 82 Abs. 1 DSGVO zu, jedoch nur in Höhe von 100 €.

aa)

Die Beklagte hat personenbezogene Daten des Klägers, nämlich seine Telefonnummer in Verbindung mit seinem Namen an Dritte weitergegeben. Dies stellt gemäß Art. 4 Nr. 2 DSGVO eine Verarbeitung dieser personenbezogenen Daten dar.

Auch ist mangels Angaben der Beklagten zum genauen Zeitpunkt des Scraping-Vorfalles zugunsten des Klägers davon auszugehen, dass dieser Vorfall nach dem 24.05.2018 und damit zum Zeitpunkt der Geltung der DSGVO stattgefunden hat (vgl. OLG Hamm aaO, juris Rn. 63 ff.).

bb)

Gem. Art. 6 Abs. 1 Buchst. a DSGVO bedarf es zur Rechtmäßigkeit dieser Verarbeitung grundsätzlich der Einwilligung des Klägers. An einer solchen fehlt es im vorliegenden Fall.

Zwar war im Profil des Klägers eingetragen, dass jeder ihn über seine Telefonnummer finden und dementsprechend über die Telefonnummer Zugriff auf sämtliche im Profil des Klägers als öffentlich eingestellte Daten erhalten darf. Diese Einwilligung des Klägers genügt jedoch nicht den Anforderun-

gen an eine Einwilligung nach Art. 6 Abs. 1 Buchst. a DSGVO und war damit unwirksam.

Die Beklagte hat gegen die sich aus Art. 25 Abs. 2 DSGVO ergebende Verpflichtung verstoßen, indem sie als Standardeinstellung für die Rubrik „Bestimme, wer dich finden kann“ die Einstellung „alle“ bestimmt hat. In dem Umstand, dass der Kläger diese Voreinstellungen nicht geändert hat, liegt keine wirksame Einwilligung des Klägers in die Weitergabe seiner Daten in Form der Telefonnummer, seines Wohnorts und seines Arbeitgebers.

Eine Einwilligung setzt ein aktives Verhalten des Einwilligenden voraus. Der Nutzer muss tätig werden, um seine Einwilligung zu erteilen (vgl. EuGH, Urteil vom 1. Oktober 2019 - C-673/17, NJW 2019, 3433 [juris Rn. 49] – Planet49). Nach dem 32. Erwägungsgrund der DSGVO soll die Einwilligung durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung. Dies könnte etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder durch eine andere Erklärung oder Verhaltensweise geschehen, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert. Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen.

Damit kann auch eine Voreinstellung dergestalt, dass jeder über die Telefonnummer auf das Profil des Nutzers und die darin enthaltenen personenbezogenen Daten zugreifen kann, keine wirksame Einwilligung in die Wei-

tergabe der auf diese Weise erlangten personenbezogenen Daten darstellen.

cc)

Diese durch die Voreinstellungen ermöglichte Datenerhebung ist auch nicht für die Durchführung eines rechtsgeschäftlichen Schuldverhältnisses erforderlich (Art. 6 Abs. 1 Satz 1 Buchst. b DSGVO), ebenso wenig zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO). Auch wenn facebook dazu dienen soll, Freunde zu finden und sich zu vernetzen, ist dafür nicht zwingend erforderlich, dass alle Nutzer Zugriff auf die Daten der anderen Nutzer erhalten. Schließlich ist es kaum denkbar, dass ein Nutzer von facebook Kontakt zu sämtlichen anderen Nutzern von facebook braucht oder auch nur wünscht.

dd)

Die Beklagte kann sich auch nicht nach Art. 82 Abs. 3 DSGVO entlasten. Sie hat ohne wirksame Einwilligung personenbezogenen Daten des Klägers – wenn auch unbeabsichtigt – weitergegeben. Dadurch, dass sie ein Tool zur Verfügung gestellt hat, mithilfe dessen man nur unter Angabe einer Telefonnummer diese einem Profil des Nutzers und allen darin enthaltenen Informationen zuordnen kann, hat sie das Risiko für eine Weitergabe der Daten an beliebig viele Dritte deutlich erhöht.

ee)

Hinsichtlich der übrigen Daten hat die Beklagte hingegen bestritten, dass die Voreinstellung „öffentlich“ war. Der Kläger hat für die gegenteilige Behauptung keinen Beweis angetreten. Damit hat insoweit der Kläger seine

Einwilligung zur Weitergabe seiner Daten an jeden beliebigen Besucher seines Profils erteilt.

ff)

Weitere Verstöße gegen die DSGVO liegen nicht vor.

Das Scraping selbst stellt keine über den bereits festgestellten Verstoß hinausgehenden Verstoß gegen die DSGVO dar. Scraper machen nichts, was nicht auch alle anderen tun können. Sie sind dabei lediglich effektiver, weil sie sich automatisierter Verfahren bedienen. Es kommt mithin nicht darauf an, ob die Beklagte ausreichende Sicherungsmaßnahmen zur Verhinderung von Scraping vorgesehen hat.

Auch die möglicherweise fehlende Unterrichtung über das erfolgte Scraping stellt keinen eigenständigen Verstoß gegen die DSGVO dar, der zusätzliche Ansprüche begründen würde. Es ist nicht ersichtlich, wie dadurch die Entstehung eines weiteren Schadens oder die Vertiefung des Schadens hätte verhindert werden können.

gg)

Dem Kläger ist auch ein kausaler Schaden entstanden.

Zwar begründet der bloße Verstoß gegen die DSGVO allein den Anspruch aus Art. 82 Abs. 1 DSGVO nicht (EuGH, Urteil vom 4. Mai 2023 - C-300/21, NJW 2023, 1930, 1932).

Nach Anhörung des Klägers ist das Gericht aber davon überzeugt, dass dem Kläger durch den streitgegenständlichen Vorfall ein immaterieller Schaden entstanden ist.

(1)

Soweit das OLG den vergleichbaren bzw. identischen Vortrag der dortigen Klägerin in einem Parallelverfahren für unsubstantiiert gehalten hat (OLG Hamm aaO, juris Rn. 162 ff.), folgt die Kammer dem nicht:

Ein Vortrag ist grundsätzlich ausreichend substantiiert, wenn er geeignet ist, in Verbindung mit einem Rechtssatz die geltend gemachten Ansprüche zumindest teilweise zu begründen. Sind diese Anforderungen erfüllt, ist es Sache des Tatgerichts, in die Beweisaufnahme einzutreten und dabei benannte Zeugen oder die zu vernehmende Partei nach weiteren Einzelheiten zu befragen (vgl. BGH, Beschluss vom 9. Mai 2023 – VIII ZR 160/21, juris Rn. 18).

Aus Sicht der Kammer war der schriftsätzliche Vortrag geeignet, einen Schaden zu begründen. Nähere Einzelheiten waren daher einer Beweisaufnahme bzw. persönlichen Anhörung des Klägers vorzubehalten.

Der Umstand, dass Hunderte Kläger angeblich die gleichen Beeinträchtigungen durch den Scraping-Vorfall erlitten haben, ist zwar im Rahmen der Beweiswürdigung zu berücksichtigen. Er führt jedoch nicht dazu, dass der Vortrag unsubstantiiert wäre: Die Frage, ob ein Vortrag substantiiert ist oder nicht, kann nur im Hinblick auf das konkrete Streitverfahren beurteilt werden, nicht aber im Hinblick auf andere, nicht von den Parteien geführte Rechtsstreitigkeiten. Gerade weil es um innere Vorgänge geht, können diese nur näherungsweise beschrieben werden. Bei der Vielzahl von Klägern ist eine individuelle, das heißt jeweils eine sich in keinem anderen Verfahren wiederholende Darstellung überhaupt nicht möglich. Auch kann nicht von vornherein ausgeschlossen werden, dass sich mehrere Kläger genau in der gleichen Weise durch den Vorfall geschädigt fühlen.

(2)

Der Kläger hat im Rahmen seiner persönlichen Anhörung angegeben, ihn habe der Scraping-Vorfall gestört, weil er zahlreiche Anrufe und sms erhalten habe, was ihn sehr belastet habe.

Insoweit ist seine Aussage auch glaubhaft. Sie wird auch gestützt durch den Umstand, dass der Kläger unstreitig nach Bekanntwerden des Scraping-Vorfalles die Voreinstellungen bezüglich der Suchbarkeit seiner Telefonnummer auf „nur ich“ umgestellt hat. Er hat damit nachgewiesen, dass ihn die Weitergabe seiner Telefonnummer an beliebige Dritte gestört hat.

(3)

Diese Beeinträchtigungen genügen nach Ansicht des Gerichts zur Begründung eines Schadens. Sie gehen über bloße negative Folgen, die in jedem Fall eintreten, hinaus. Der Schaden muss keinen bestimmten Grad an Erheblichkeit erreichen (vgl. EuGH, Urteil vom 4. Mai 2023 – C-300/21, NJW 2023, 1930, 1934).

Das Gericht sieht davon ab, den hiesigen Rechtsstreit im Hinblick auf die durch den BGH erfolgte Vorlage an den EuGH (BGH, Beschluss vom 26. September 2023 – VI ZR 97/22) auszusetzen. Zwar zielt die vierte Vorlagefrage gerade darauf ab, ob bloße negative Gefühle als immaterieller Schaden genügen. Diese Vorlagefrage ist daher nach Ansicht des Gerichts entscheidungserheblich. Es soll aber dem letztinstanzlichen Gericht vorbehalten bleiben, die Entscheidungserheblichkeit abschließend zu beurteilen und damit auch über eine Aussetzung des Verfahrens zu entscheiden.

(4)

Bei der Höhe war allerdings zu berücksichtigen, dass der Kläger hauptsächlich genervt von dem Scraping-Vorfall wirkte. Auch auf mehrfache Nachfrage hat er stets nur betont, wie belastend die zahlreichen Anrufe und sms gewesen seien. Dass er darüber hinaus aber sich Sorgen gemacht hätte, insbesondere dahingehend, Opfer von Betrugsversuchen zu werden, hat er zunächst nicht angegeben. Erst auf ausdrückliche Nachfrage seines Prozessbevollmächtigten hat er eine entsprechende Sorge bejaht. Anders als die Darstellung, wie sehr ihn die Anrufe und sms genervt haben, erschöpfte sich seine Aussage aber in einer pauschalen Bejahung, ohne weitere Details. Das Gericht ist daher davon überzeugt, dass der Kläger sich tatsächlich keine Sorgen darüber gemacht hat, Opfer von Betrugsversuchen zu werden.

Vor diesem Hintergrund ist ein Schmerzensgeld in Höhe von 100 € angemessen, aber auch ausreichend.

hh)

Der Zinsanspruch insoweit folgt aus §§ 288 Abs. 1, 291 BGB.

b)

Der Kläger hat aus Art. 82 Abs. 1 DSGVO auch einen Anspruch auf die Feststellung der Ersatzpflicht für weitere Schäden.

aa)

Die Weitergabe der Telefonnummer in Verbindung mit den Daten des Klägers durch die Beklagte war, wie ausgeführt, rechtswidrig.

bb)

Es ist nicht auszuschließen, dass es in Folge der Weitergabe dieser Daten bereits zu weiteren, dem Kläger noch unbekanntem Schäden gekommen ist oder noch kommen wird. Angesichts des verletzten Rechtsguts genügt vorliegend die Möglichkeit weiterer Schäden, auf eine besondere Wahrscheinlichkeit kommt es nicht an.

c)

Der Kläger kann von der Beklagten darüber hinaus aus §§ 1004, 823 Abs. 1 BGB verlangen, dass diese es unterlässt, seine Telefonnummer zu verarbeiten, wenn er einer solchen Verarbeitung nicht ausdrücklich zugestimmt hat.

aa)

Die Vorschriften sind neben der DSGVO anwendbar; diese enthält hinsichtlich der Frage, welche Rechtsbehelfe bei Verstößen gegen die DSGVO zur Verfügung stehen, kein abschließendes Sanktionssystem.

Zwar ist die Frage, inwieweit Mitbewerber befugt sind, Verstöße gegen die DSGVO geltend zu machen, bisher nicht geklärt und Gegenstand eines Vorlageersuchens an den EuGH (BGH, Beschluss vom 12. Januar 2023 – I ZR 223/19, MDR 2023, 377 – Arzneimittelbestelldaten).

Im Hinblick auf den Unterlassungsantrag der durch die rechtswidrige Datenverarbeitung betroffenen Person ergibt sich die Zulässigkeit weiterer nationaler Rechtsbehelfe jedoch bereits aus Art. 77 Abs. 1 DSGVO. Danach hat jede Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehen-

den Rechte infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden.

Einen solchen wirksamen Rechtsbehelf stellt insbesondere ein Unterlassungsanspruch dar, da er in der Lage ist, die bereits stattgefundene Verletzung zu beenden und weitere Verletzungen zu verhindern.

Das Gericht sieht auch diesbezüglich aus den bereits oben genannten Gründen davon ab, den Rechtsstreit im Hinblick auf das von dem BGH angestoßene Vorabentscheidungsersuchen (BGH, Beschluss vom 26. September 2023 - VI ZR 97/22) auszusetzen.

bb)

Der bereits erfolgte Verstoß indiziert die Wiederholungsgefahr. Diese ist auch nicht dadurch entfallen, dass die Beklagte mittlerweile die Software zum Importieren von Kontakten abgeschafft bzw. verändert hat.

Eine einmal begründete Wiederholungsgefahr entfällt nicht dadurch, dass das beanstandete Verhalten abgestellt wird. Erforderlich ist grundsätzlich vielmehr die Abgabe einer strafbewehrten Unterlassungserklärung (st. Rspr.; vgl. BGH, Urteil vom 26. Oktober 2000 - I ZR 180/98, GRUR 2001, 453 [juris Rn. 28] - TCM-Zentrum, mwN). Eine solche hat die Beklagte nicht abgegeben.

cc)

Wie bereits ausgeführt, ist eine wirksame Einwilligung nur dann gegeben, wenn der Kläger sich aktiv für die Einstellung „öffentlich“ entscheidet, nicht aber, wenn diese Einstellung bereits voreingestellt ist. Eine Verarbeitung

der Daten ist daher rechtswidrig, solange eine solche bewusste aktive Auswahl nicht erfolgt.

Im Übrigen ist dem Klageantrag zu 3b jedoch nicht stattzugeben. Es fehlt nicht deswegen an einer wirksamen Einwilligung, weil die Informationen der Beklagten hierzu unübersichtlich oder unvollständig sind. Die von der Beklagten erteilten Informationen machen vielmehr hinreichend deutlich, was die jeweilige Einstellung bedeutet. Dass dies an verschiedenen Stellen geschieht, liegt in der Natur der Sache; es macht einen Unterschied, ob man Profildaten generell mit denen teilen möchte, die das eigene Profil besuchen, oder ob man über seine Telefonnummer gefunden werden möchte. Es stellt also keinen Verstoß gegen das Transparenzgebot dar, dass ein Nutzer an verschiedenen Stellen Privatsphäreinstellungen treffen muss.

Dass im Falle der Nutzung der Facebook-Messenger App andere Einstellungen gelten würden als für die Nutzung von facebook, hat der Kläger nicht unter Beweis gestellt.

d)

Einen Anspruch auf Auskunft hat der Kläger nicht (mehr). Die Beklagte hat bereits Auskunft darüber erteilt, welche personenbezogenen Daten sie verarbeitet. Darüber hinaus konnte der Kläger dies unschwer selbst in Erfahrung bringen, indem er seinem Nutzerprofil entnimmt, welche Daten öffentlich eingestellt sind.

Informationen darüber, welche Daten durch welche Empfänger durch Scraping erlangt wurden, hat die Beklagte nicht, ihr ist insbesondere die Identität der Scraper nicht bekannt. Insoweit hat sie bereits alle Auskünfte erteilt, zu denen sie in der Lage ist; der Kläger hat jedenfalls nichts anderes zu beweisen vermocht.

II.

Die Kostenentscheidung beruht auf § 92 Abs. 1 Alt. 2 ZPO, die Entscheidung über die vorläufige Vollstreckbarkeit auf § 709 S. 1 und 2, § 708 Nr. 11, 711 ZPO.

Anlass zur Entscheidung über die Zulassung der Berufung besteht nicht, weil beide Parteien mit mehr als 600 € beschwert sind.