Oberlandesgericht Köln, 15 U 33/23

Datum:	07.12.2023
Gericht:	Oberlandesgericht Köln
Spruchkörper:	15. Zivilsenat
Entscheidungsart:	Urteil
Aktenzeichen:	15 U 33/23
ECLI:	ECLI:DE:OLGK:2023:1207.15U33.23.00

Tenor:

Die Berufung des Klägers gegen das Urteil des Landgerichts Aachen vom 10.2.2023 (8 O 200/22) wird zurückgewiesen.

Die Kosten des Berufungsverfahrens trägt der Kläger.

Das Urteil ist gegen Sicherheitsleistung in Höhe von 110% des jeweils zu vollstreckenden Betrages vorläufig vollstreckbar.

Die Revision wird zugelassen.

Gründe: 1

I. 2

Die Parteien streiten um Schadensersatz, Unterlassungs-, Feststellungs- und Auskunftsansprüche aus einem Scraping-Vorfall auf der Plattform der Beklagten, der im April 2021 bekannt wurde. 3

Bei diesem Vorfall wurden Mobiltelefonnummer, Name, Facebook-ID, Geschlecht und Wohnort des Klägers erlangt und – so sein Vortrag – in einem „Hacker-Forum“ veröffentlicht, wobei der „gescrapte“ Name des Klägers („*T. F.*“) nicht mit seinem tatsächlichen Namen („*F. A.*“) übereinstimmt und es zudem unstreitig ist, dass die Telefonnummer nicht im eigentlichen Sinne „gescrapt“, sondern von den Scrapern als randomisierte Nummernfolge in das sog. Contact Import Tool (CIT) eingepflegt und dann bei Auffinden des Profils des Klägers seinem Namen und den sonstigen dort vorhandenen Daten nur zugeordnet wurde. Wegen der weiteren Einzelheiten des Sach- und Streitstandes sowie der erstinstanzlichen Sachanträge wird auf den Tatbestand des angegriffenen Urteils Bezug genommen. 4

5

Das Landgericht hat die Klage abgewiesen, was der Kläger mit der Berufung angreift und seine erstinstanzlichen Anträge in vollem Umfang weiterverfolgt.

Er macht geltend, es liege ein Verstoß gegen Art. 5 Abs. 1 DSGVO vor, weil er nicht die Möglichkeit gehabt habe, in informierter Art und Weise über die Verarbeitung der ihn betreffenden Daten zu entscheiden. Angesichts der vielfach verschachtelten und mehrschichtigen Informationen auf der Plattform der Beklagten sei die erforderliche Transparenz nicht gewahrt worden. Weiter liege ein Verstoß gegen Art. 32 Abs. 1, 5 Abs. 1 lit. f) DSGVO vor, weil die Beklagte keine geeigneten technischen bzw. organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten vorgesehen hätte. Die Beweislast dafür trage nach Art. 5 Abs. 2 DSGVO die Beklagte, die selbst inzwischen anerkannt habe, dass das CIT mangelhaft ausgestaltet gewesen sei und daher weitere Sicherheitsvorkehrungen unternommen habe. Weiter habe die Beklagte gegen Art. 24, 25 DSGVO verstoßen, weil ein Nutzer davon ausgehe, dass er seine Telefonnummer lediglich im Rahmen der Zwei-Faktor-Authentifizierung hinterlege. Die durch die Beklagte gewählte Voreinstellung für die Telefonnummer in der Suchbarkeit auf „*alle*“/„*everyone*“ lasse sich nicht mit dem Unternehmenszweck bzw. dem Zweck des sozialen Netzwerks rechtfertigen. Der Kläger ist der Ansicht, die Einstellung zur Suchbarkeit hätte per default auf „*Freunde-Freunde* “ eingestellt sein müssen. Darüber hinaus stelle es einen Verstoß gegen Art. 13 Abs. 1 lit. c), 14 DSGVO dar, dass die Beklagte nicht hinreichend über den Zweck der Verwendung der Telefonnummer auch für das CIT informiert habe sowie einen Verstoß gegen Art. 33 DSGVO, weil der Scraping-Vorfall als eine „Verletzung“ im Sinne von Art. 4 Nr. 12 DSGVO nicht binnen 72 Stunden der Aufsichtsbehörde gemeldet worden sei. Es sei auch keine Datenschutz-Folgenabschätzung (Art. 35 DSGVO) vorgenommen worden. Ihrer Auskunftspflicht nach Art. 15 DSGVO habe die Beklagte nicht vollständig genügt, weil sie dem Kläger die konkreten Empfänger der Daten, nämlich die Scraper, nicht benannt und auch keine Auskunft darüber erteilt habe, wann und von wem die Telefonnummer des Klägers mit den anderen Daten zusammengeführt worden sei. 6

Zum immateriellen Schaden macht der Kläger geltend, er habe einen Kontrollverlust über seine Daten und außerdem Angst, Stress sowie eine Komfort- und Zeiteinbuße erlitten, weil er sich mit dem Datenleck und den Folgen habe auseinandersetzen müssen. Er gebe seine Telefonnummer stets bewusst und zielgerichtet weiter und mache sie nicht wahllos im Internet einer Öffentlichkeit zugänglich. Eine Änderung der Suchbarkeitseinstellungen auf seinem Profil würde zudem an der Gefahr eines weiteren Scrapings nichts ändern. Sein Schaden habe sich in Spam-E-Mails, Spam-SMS und Spam-Anrufen manifestiert. 7

Der Kläger ist weiter der Ansicht, es bestehe ein Feststellungsinteresse für seinen Feststellungsantrag, weil nicht abgesehen werden könne, welche Dritte Zugriff auf seine Daten hatten und wie sie die Daten noch missbrauchen könnten. Dazu macht er geltend, in H. sei durch Trickbetrügereien bis September 2022 ein Schaden von fast 3,3 Millionen Euro entstanden, wovon ein Betrag von 780.000 Euro auf sog. WhatsApp-Betrug entfalle. Daneben könnten „falsche“ Bankmitarbeiter Daten über Kontoverbindungen erfragen oder Täter als vermeintliche Zahlungsdienstleister anrufen. Er könne nicht sicher sein, dass die Beklagte das CIT ausreichend aktualisiert habe. 8

Der Kläger beantragt zuletzt, 9

unter Aufhebung des am 10.2.2023 verkündeten Urteils des Landgerichts Aachen (8 O 200/22) 10

11

1. die Beklagte zu verurteilen, an die Klägerseite immateriellen Schadensersatz in angemessener Höhe zu zahlen, dessen Höhe in das pflichtgemäße Ermessen des Gerichts gestellt wird, mindestens jedoch 1.000 Euro nebst Zinsen seit Rechtshängigkeit in Höhe von fünf Prozentpunkten über dem Basiszinssatz;

2. festzustellen, dass die Beklagte verpflichtet ist, der Klägerseite künftige materielle und künftige derzeit noch nicht vorhersehbare immaterielle Schäden zu ersetzen, die der Klägerseite durch den unbefugten Zugriff im Zeitraum ab dem 25.5.2018 bis September 2019 auf das Datenarchiv der Beklagten entstehen; 12

3. die Beklagte zu verurteilen, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000 Euro, 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, 13

a. personenbezogene Daten der Klägerseite, 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, 14

b. die Telefonnummer der Klägerseite 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 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; 15

4. die Beklagte zu verurteilen, der Klägerseite Auskunft über die Klägerseite betreffende personenbezogene 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. 16

Die Beklagte beantragt, 17

die Berufung zurückzuweisen. 18

Sie verteidigt die angegriffene Entscheidung unter Vertiefung ihres erstinstanzlichen Vorbringens. 19

Im Hinblick auf den geltend gemachten Auskunftsanspruch des Klägers ist die Beklagte der Ansicht, sie habe den Anspruch durch ihr außergerichtliches Schreiben (Anlage B16) vollständig erfüllt. Nähere Angaben über die Scraper müsse sie von Rechts wegen nicht machen, weil diese keine Empfänger der Daten seien. Sie selbst habe diesen die Daten nicht offengelegt und sei auch nicht verpflichtet, über etwaige Verarbeitungstätigkeiten von Scrapern – und damit Dritten – Auskunft zu erteilen. Im Übrigen habe das Landgericht zutreffend festgestellt, dass der Beklagten eine weitere Auskunftserteilung hinsichtlich der Scraper jedenfalls auch unmöglich sei, da sie deren Namen nicht kenne. 20

21

Der Kläger habe zu dem angeblich erlittenen Schaden – wie schon in erster Instanz – nur floskelhaft und unter Verwendung von Textbausteinen vorgetragen, die seine Prozessbevollmächtigten in hunderten anderer Verfahren ebenfalls benutzt hätten. Zu dem (bestrittenen) Empfang von Spam-SMS und Spam-Anrufen gebe es weder eine konkrete Darlegung noch einen Beweisantritt. Der vom Kläger geltend gemachte Kontrollverlust sei nicht schon per se ein immaterieller Schaden und daneben fehle es auch an Vortrag des Klägers zu den vermeintlichen Folgen dieses Kontrollverlustes.

Mit Schriftsatz vom 8.11.2023 hat der Kläger verschiedene Vorlagefragen formuliert und u.a. beantragt, das Verfahren analog § 148 ZPO bis zur Entscheidung des Europäischen Gerichtshofs über diese Vorlagefragen auszusetzen. Hilfsweise hat er beantragt, jedenfalls das Verfahren analog § 148 ZPO bis zu der Entscheidung des Europäischen Gerichtshofs in den dort anhängigen Verfahren C-189/22, C-741/21, C-687/21, C-667/21, C-340/21 und C-307/22 auszusetzen. 22

Hinsichtlich des weiteren Vortrags der Parteien wird auf die im Berufungsverfahren gewechselten Schriftsätze Bezug genommen. 23

II. 24

Die zulässige Berufung des Klägers bleibt in der Sache ohne Erfolg, da das Landgericht seine Klage, für die es als deutsches Gericht jedenfalls aufgrund der rügelosen Einlassung der Beklagten (Art. 26 Abs. 1 S. 1 EuGVVO) international zuständig war, zu Recht abgewiesen hat. 25

1. Der auf Ersatz immateriellen Schadens gerichtete Antrag zu 1) ist zulässig, aber unbegründet. 26

a. Soweit die Beklagte geltend macht, der Antrag zu 1) sei nicht hinreichend bestimmt, weil er auf mehrere angebliche Verstöße gegen die DSGVO gestützt werde und damit mehrere Streitgegenstände in Form einer unzulässigen alternativen Klagehäufung vorlägen, greift dies nicht durch. 27

Nach § 253 Abs. 2 Nr. 2 ZPO muss die Klageschrift neben einem bestimmten Antrag eine bestimmte Angabe des Gegenstandes und des Grundes des erhobenen Anspruchs enthalten. Damit werden der Streitgegenstand abgegrenzt und die Grenze der Rechtshängigkeit und der Rechtskraft festgelegt sowie Gegenstand und Umfang der Entscheidungsbefugnis des Gerichts bestimmt. Der Kläger muss die gebotene Bestimmung des Streitgegenstandes vornehmen und kann sie nicht zur Disposition des Gerichts stellen. Dies erfordert auch der Schutz des Beklagten, für den erkennbar sein muss, welche prozessualen Ansprüche gegen ihn erhoben werden, um seine Rechtsverteidigung danach ausrichten zu können. Für die damit erforderliche Individualisierung des Streitgegenstands ist es entsprechend dem Zweck der Klageerhebung, dem Beklagten den Willen des Klägers zur Durchsetzung seiner Forderungen zu verdeutlichen, im Allgemeinen ausreichend, wenn der Anspruch als solcher identifizierbar ist. Dazu gehört bei mehreren Streitgegenständen auch die Benennung der Reihenfolge, in der diese zur Überprüfung durch das Gericht gestellt werden. Der Kläger kann die Auswahl, über welche selbständigen Ansprüche bis zur Höhe der eingeklagten Forderung entschieden werden soll, nicht dem Gericht überlassen (BGH, Urt. v. 17.1.2023 – VI ZR 203/22, juris; BGH, Beschl. v. 24.3.2011 – I ZR 108/09, BGHZ 189, 56). 28

29

Nach diesen Grundsätzen liegt hier keine unzulässige alternative Klagehäufung vor, da der Kläger mit dem Antrag zu 1) nicht mehrere selbständige prozessuale Ansprüche geltend macht, sondern vielmehr einen einheitlichen Anspruch auf Ersatz eines immateriellen Schadens, der sich nur aus mehreren Datenschutzverstößen der Beklagten ergeben haben soll. Diese Verstöße haben sich zwar in einem längeren Zeitraum abgespielt, jedoch ist das betreffende Geschehen eindeutig abgrenzbar: Es bezieht sich auf den Scraping-Vorfall (angeblich unzureichende Sicherungsmaßnahmen bzw. Verarbeitung der Daten ohne vorherige ausreichende Informationen) sowie auf die im Anschluss daran fehlende Information von Nutzern und Behörden. Ungeachtet der Frage, ob man diese durch Auslegung ersichtliche Tatsache nicht schon für die Zulässigkeit ausreichen lassen kann (siehe etwa für einen Fall nach entsprechender Klarstellung OLG Hamm, Urt. v. 15.8.2023 - 7 U 19/23, juris Rn. 48 ff. und generell OLG Stuttgart, Urt. v. 22.11.2023 – 4 U 20/23, GRUR-RS 2023, 32883 Rn. 85 ff.), hat der Kläger zudem seinen Anspruch jedenfalls auch zulässig dahingehend konkretisiert, dass er einen Betrag von 500 Euro für das sog. Datenleck und von weiteren 500 Euro für die unzureichende Auskunft der Beklagten für angemessen hält (Bl. 319 d.A.).

b. Der Antrag ist jedoch unbegründet, da dem Kläger der geltend gemachte Schadensersatz weder aus Art. 82 Abs. 1 DSGVO noch aus einer anderen Anspruchsgrundlage zusteht. 30

aa. Der Anwendungsbereich von Art. 82 Abs. 1 DSGVO ist zwar in zeitlicher und sachlicher Hinsicht eröffnet. Denn auch wenn sich der Kläger bereits vor dem 24.5.2018 auf der Plattform der Beklagten angemeldet hat, war die Beklagte jedenfalls ab dem Zeitpunkt des Inkrafttretens der DSGVO verpflichtet, den dort statuierten Vorschriften gerecht zu werden; der Scraping-Vorfall selbst hat nach dem übereinstimmenden Vortrag der Parteien jedenfalls nicht vor dem 24.5.2018 stattgefunden. 31

bb. Die Beklagte hat auch als Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO gehandelt, da sie Inhaberin des sozialen Netzwerkes ist, von dem die Daten des Klägers „gescrapt“ wurden, und da sie innerhalb dieses Netzwerks selbst auch den entsprechenden Suchautomatismus durch das CIT zur Verfügung gestellt hat, der im Rahmen des streitgegenständlichen Datenschutzvorfalls benutzt wurde. 32

cc. Der Beklagten dürften darüber hinaus auch Verstöße gegen Art. 5 Abs. 1 lit. b), 25 Abs. 2, Art. 32 Abs. 1 DSGVO vorzuwerfen sein, weil sie keine geeigneten technischen und organisatorischen Maßnahmen getroffen hat, die sicherstellen konnten, dass durch die von ihr gewählten Voreinstellungen im Rahmen der Suchbarkeit des Profils mithilfe der Telefonnummer und das Zur-Verfügung-Stellen des CIT nur solche personenbezogenen Daten des Klägers verarbeitet wurden, die für den jeweiligen bestimmten Verarbeitungszweck erforderlich waren. Weiter dürfte durch die unterlassene bzw. verspätete Meldung des Vorfalls gegenüber dem Kläger und der irischen Datenschutzbehörde auch ein Verstoß gegen Art. 33 Abs. 1 bzw. Art. 34 Abs. 1 DSGVO vorliegen. 33

dd. Ob und welche Verstöße der Beklagten gegen die DSGVO vorzuwerfen sind, kann an dieser Stelle allerdings letztlich offen bleiben. Denn es ist aus prozessualen Gründen davon auszugehen, dass dem Kläger jedenfalls kein immaterieller Schaden durch diese – insofern zu seinen Gunsten als vorliegend unterstellten – Datenschutzverstöße der Beklagten entstanden ist. 34

In Bezug auf die sich aus Art. 82 DSGVO grundsätzlich ergebenden Vorgaben für die Zuerkennung von Schadensersatzansprüchen wegen immaterieller Schäden verweist der 35

Senat auf die Ausführungen in den Urteilen der Oberlandesgerichte Hamm vom 15.8.2023 – 7 U 19/23 – und Stuttgart vom 22.11.2023 – 4 U 20/23, jeweils juris. Diesen Anforderungen genügt das Klägervorbringen nicht.

Der Kläger macht geltend, dass er durch den Scraping-Vorfall einen Kontrollverlust erlitten habe, dass er Angst, Unwohlsein, Misstrauen und Sorge empfinde sowie durch Anrufe, SMS und E-Mails belästigt werde. Daneben habe er eine Komfort- und Zeiteinbuße erlitten, weil er sich mit den Folgen des Datenlecks habe auseinandersetzen müssen, und er habe Zeit und Mühe aufgewendet, um sich vor drohendem (weiteren) Missbrauch zu schützen. Mit diesen Angaben rügt der Kläger zwar mehr als einen bloßen Verstoß der Beklagten gegen die Vorschriften der DSGVO (vgl. dazu EuGH, Urt. v. 4.5.2023 – C-300/21, NJW 2023, 1930). Sein Vortrag reicht jedoch nicht aus, um einen bei ihm entstandenen immateriellen Schaden im Sinne von Art. 82 Abs. 1 DSGVO anzunehmen, der nach der Rechtsprechung des Europäischen Gerichtshofs nicht nach dem Recht der Mitgliedstaaten, sondern als autonomer Begriff des Unionsrechts einheitlich unionsrechtlichen auszulegen ist (EuGH, Urt. v. 4.5.2023 – C-300/21, NJW 2023, 1930). 36

(1) Soweit der Kläger seinen immateriellen Schaden auf die Veröffentlichung derjenigen Daten stützt, die auf seinem Profil bei der Beklagten als „*immer öffentlich*“ eingestellt waren (Vorname, Wohnort, Geschlecht und Facebook-ID), scheidet die Annahme eines immateriellen Schadens schon deswegen aus, weil sich der Kläger durch seine im Zuge der Registrierung auf der Plattform der Beklagten erklärte Zustimmung mit den dort geltenden Nutzungsbedingungen damit einverstanden erklärt hat, dass diese Daten in die Öffentlichkeit gelangen. Im Hinblick darauf bestand schon keine Verpflichtung der Beklagten, diese Daten des Klägers durch datenschutzkonforme Voreinstellungen oder technische Sicherheitsmaßnahmen vor einer Kenntnisnahme durch Dritte weitergehend zu schützen. Jedenfalls – und das ist maßgeblich - können sich die vom Kläger angeblich verspürten Gefühle wie Angst, Unwohlsein oder Misstrauen nicht darauf beziehen, dass gerade solche personenbezogenen Daten von den Scrapern im sog. Darknet veröffentlicht worden sind, die er selbst auf der Plattform der Beklagten der Öffentlichkeit zugänglich gemacht hat. 37

(2) Soweit der Kläger seinen immateriellen Schaden darauf stützt, dass seine Telefonnummer in Verbindung mit seinem Vor- und Spitznamen („*T. F.*“) veröffentlicht wurde, handelt es sich bei der Telefonnummer zwar um ein personenbezogenes Datum, das er nicht der Öffentlichkeit zugänglich machen wollte. Jedoch reicht sein diesbezüglicher Vortrag zu einem angeblichen Kontrollverlust nicht aus, um einen immateriellen Schaden im Sinne von Art. 82 Abs. 1 DSGVO anzunehmen. 38

(a) Der Senat vermag auf Basis des Vortrags des Klägers schon nicht festzustellen, dass dieser durch den streitgegenständlichen Scraping-Vorfall tatsächlich einen Kontrollverlust im Hinblick auf seine Telefonnummer erlitten hat. 39

Wie bereits dem Wortlaut dieses Begriffes zu entnehmen ist, setzt ein Kontrollverlust voraus, dass der Betroffene zunächst die Kontrolle über das konkrete personenbezogene Datum hatte und diese Kontrolle später gegen seinen Willen verloren hat. Der Kläger hat jedoch nicht dargelegt, dass er vor dem streitgegenständlichen Scraping-Vorfall die Kontrolle über seine Mobilfunknummer hatte und diese erst durch die streitgegenständliche Veröffentlichung der Telefonnummer im sog. Darknet verloren gegangen ist. Er hat vielmehr zu dem angeblich erlittenen Kontrollverlust nur pauschal unter Verwendung von Textblöcken vorgetragen, die seine Prozessbevollmächtigten in einer Vielzahl von beim Senat anhängigen Verfahren in identischer Form verwendet haben. Außer der pauschalen, durch die Verwendung einer geschlechtsneutralen Parteibezeichnung in jeglichem Rechtsstreit einsetzbaren 40

Formulierung, „*die Klägerseite*“ habe „*einen erheblichen Kontrollverlust*“ erlitten (vgl. Bl. 24, 42, 317, 370 d.A.) und „*die Klägerseite gibt die Telefonnummer stets bewusst und zielgerichtet weiter, und macht diese nicht wahl- und grundlos der Öffentlichkeit zugänglich, wie etwa im Internet*“ (vgl. Bl. 894 d.A.), hat der Kläger insbesondere keine Angaben zur konkreten Verwendung seiner Telefonnummer vor dem streitgegenständlichen Scraping-Vorfall gemacht. Eine solche Darlegung einer zunächst ausgeübten Kontrolle über die eigene Telefonnummer ist auch nicht entbehrlich. Denn bei einer Telefonnummer handelt es sich nicht um ein per se sensibles oder der Geheimhaltung unterliegendes personenbezogenes Datum, sondern vielmehr um ein solches, das nach seiner Zweckbestimmung dem Betroffenen ermöglichen soll, in Kontakt mit anderen Personen zu treten und das daher im täglichen Leben auch solchen anderen Personen oft in großem Umfang zugänglich gemacht wird. Im Hinblick darauf hätte der Kläger, wie mit den Parteien im Termin erörtert, konkret dazu vortragen müssen, wie er im privaten, geschäftlichen und/oder beruflichen Umfeld mit seiner Telefonnummer vor dem streitgegenständlichen Scraping-Vorfall umgegangen ist, ob und unter welchen Bedingungen er sie an wen weitergegeben hat und dass insofern durch die Veröffentlichung nach dem Scraping-Vorfall tatsächlich ein Verlust der zuvor über diese Telefonnummer durch ihn noch ausgeübten Kontrolle eingetreten ist. Solcher Vortrag findet sich aber weder in seinen Schriftsätzen noch ist er im Rahmen der Erörterung vor dem Senat erfolgt.

Soweit der Prozessbevollmächtigte des Klägers in der mündlichen Verhandlung ausgeführt hat, er selbst gebe seine Telefonnummer nur sehr selten weiter und wenn, dann nur an wenige privat bekannte Personen bzw. an Unternehmen, denen er vollständig vertraue, bezieht sich dieses geschilderte Verhalten zum einen schon nicht auf die Person des Klägers. Für diesen bzw. für dessen Umgang mit der Telefonnummer wurde Entsprechendes nicht vorgetragen, sondern es wurden lediglich die oben auszugsweise zitierten Textbausteine verwendet. Zum anderen wäre auch zu berücksichtigen, dass auch die Weitergabe der Telefonnummer an persönlich nicht bekannte Dritte im Rahmen geschäftlicher Beziehungen – selbst wenn der Betroffene diesen zunächst Vertrauen entgegenbringt – mit einem Risiko verbunden ist, da auch in diesen Fällen ein Dritter über das personenbezogene Datum verfügt und es damit eben nicht mehr der alleinigen Kontrolle des Betroffenen unterliegt, ob dieser Dritte bzw. bei diesem beschäftigte Personen unbefugt, unabsichtlich oder im Rahmen technischer Vorfälle die Nummer anderen Personen zugänglich macht. 41

(b) Selbst wenn man vorliegend zugunsten des Klägers unterstellt, dass er durch den Scraping-Vorfall tatsächlich einen Kontrollverlust über seine Telefonnummer erlitten hat, weil diese Nummer in Verbindung mit seinem Vornamen nunmehr durch die Veröffentlichung im sog. Darknet jedenfalls auch einem Personenkreis bekannt geworden ist, dem er sie selbst gerade so nicht mitteilen wollte, liegt damit noch kein immaterieller Schaden im Sinne von Art. 82 Abs. 1 DSGVO vor. 42

Zwar ist der Ersatz eines immateriellen Schadens nach der Rechtsprechung des Europäischen Gerichtshofs (Urt. v. 4.5.2023 – C-300/21, NJW 2023, 1930) nicht davon abhängig, dass dieser Schaden eine bestimmte Erheblichkeitsschwelle überschreitet. Diese Verneinung einer solchen Erheblichkeitsschwelle bedeutet jedoch nach den Ausführungen des Europäischen Gerichtshofs in der vorzitierten Entscheidung nicht, dass eine Person, die von einem Verstoß gegen die DSGVO betroffen ist, der für sie negative Folgen gehabt hat, vom Nachweis befreit wäre, dass diese Folgen einen immateriellen Schaden im Sinne von Art. 82 DSGVO darstellen. 43

44

Im Rahmen dieses ihm obliegenden Nachweises ist der Kläger allerdings substantiierten Vortrag schuldig geblieben. Denn dass er durch den – hier zu seinen Gunsten unterstellten – Kontrollverlust durch die Veröffentlichung seiner Telefonnummer im sog. Darknet einen immateriellen Schaden erlitten hat, hat er nicht dargelegt. Vielmehr hat er sich im Verfahren – auch nach entsprechender Rüge der Beklagten in den erst- und zweitinstanzlichen Schriftsätzen sowie nach einem entsprechenden Hinweis des Senats in der mündlichen Verhandlung – allein auf den Umstand berufen, dass er hinsichtlich der Telefonnummer einen Kontrollverlust erlitten habe und die Ansicht vertreten, dass damit ein von ihm erlittener immaterieller Schaden bereits feststehe. Dieser Kontrollverlust ist jedoch – im Sinne der vorzitierten Entscheidung des Europäischen Gerichtshofs – lediglich die „*negative Folge*“ des Datenschutzverstoßes der Beklagten, nicht aber für sich genommen bereits der immaterielle Schaden. In diesem Zusammenhang kommt es auch nicht auf die zwischen den Parteien diskutierte Frage an, ob ein Verlust der Kontrolle über personenbezogene Daten schon generell keinen immateriellen Schaden des Betroffenen darstellen kann, sondern es müssen stets – wie es die Beklagte auch geltend macht – darüber hinausgehende Auswirkungen auf die Person oder die Lebensumstände des Betroffenen vorliegen. Nach Ansicht des Senats kann diese Frage nur im Einzelfall und nur unter Berücksichtigung der Art des konkreten personenbezogenen Datums beantwortet werden, über das der Betroffene die Kontrolle verloren zu haben behauptet. In Fällen wie dem vorliegenden, in denen sich der geltend gemachte Kontrollverlust auf eine Telefonnummer bezieht, die ihrem Wesen nach nicht ohne weiteres auf strikte Geheimhaltung angelegt ist und hinsichtlich derer der Betroffene – wie hier der Kläger – auch keine in der Vergangenheit praktizierte Geheimhaltung vorgetragen hat, fehlt es an tatsächlichen Anhaltspunkten, die den Rückschluss darauf erlauben, dass der entsprechende Kontrollverlust über dieses personenbezogene Datum schon einen immateriellen Schaden darstellt (im Ergebnis ebenso OLG Stuttgart, Urt. v. 22.11.2023 – 4 U 20/23, GRUR-RS 2023, 32883, Rn. 123, wonach ein „*bloß abstrakter Kontrollverlust*“ nicht ausreicht).

Dieser Bewertung stehen, anders als dies der Kläger geltend macht, auch nicht die Erwägungsgründe 75 und 85 entgegen. Erwägungsgrund 75 führt den Kontrollverlust nicht etwa generell als einen immateriellen Schaden auf, sondern zählt nur Fallgestaltungen auf, die im Rahmen einer Verarbeitung personenbezogener Daten mögliche Risiken für die Rechte und Freiheiten natürlicher Personen darstellen. Schon dem Wortlaut und dem dort verwendeten Konjunktiv nach („ … , *die zu einem physischen, materiellen oder immateriellen Schaden führen könnte* …“) werden in diesem Zusammenhang keine abstrakt feststehenden (immateriellen) Schäden aufgeführt, sondern risikobehaftete Situationen dargestellt, in denen solche Schäden beim Betroffenen im Einzelfall eintreten können. Erwägungsgrund 85 führt zwar den „*Verlust der Kontrolle über ihre personenbezogenen Daten*“ mit der Einleitung „*wie etwa*“ als eine der möglichen Fallgestaltungen eines physischen, materiellen oder immateriellen Schadens auf, den eine Verletzung des Schutzes personenbezogener Daten für eine natürliche Person nach sich ziehen kann. Auch dies ist im dortigen Kontext der Informationspflichten des Datenverarbeiters gegenüber der Aufsichtsbehörde jedoch nicht als Definition eines jeweils per se feststehenden immateriellen Schadens in der Art eines abstrakten Gefährdungsdelikts zu verstehen, sondern als Begründung des hohen Stellenwertes der Informationspflicht nach einer Verletzung des Schutzes personenbezogener Daten. In diesem Sinne hat auch der Europäische Gerichtshof in seinem Urteil vom 4.5.2023 (C-300/21, NJW 2023, 1930 Rn. 37) ausgeführt, dass sich aus den Formulierungen in den Erwägungsgründen 75 und 85 („…*die Risiken ... aus einer Verarbeitung personenbezogener Daten hervorgehen (könne), die zu einem … Schaden führen könnte“* bzw. *„… Verletzung des Schutzes personenbezogener Daten … ein … Schaden… nach sich ziehen (kann)*“) ergebe, dass der Eintritt eines Schadens im Rahmen 45

einer solchen Verarbeitung nur potentiell sei.

(c) Soweit der Kläger weiter geltend macht, er leide aufgrund der Veröffentlichung seiner Telefonnummer in Verbindung mit seinem Vor- und Spitznamen unter Angst, Sorge und Unwohlsein, ist auch damit kein immaterieller Schaden hinreichend substantiiert vorgetragen worden. 46

Bei den vom Kläger geschilderten Beeinträchtigungen handelt es sich um psychische Folgen des Datenschutzverstoßes der Beklagten, die als solche nur von ihm selbst wahrgenommen werden können. Um daraus einen Schaden ableiten zu können, also einen Nachteil des Betroffenen, der im Sinne von Erwägungsgrund 146 konkret „*erlitten*“ wurde (vgl. EuGH, Urt. v. 4.5.2023 – C-300/21, NJW 2023, 1930 Rn. 58) und damit über die reine Behauptung des entsprechenden Gefühls hinausgeht, muss der Kläger konkrete Indizien vortragen und unter Beweis stellen, die eine solche psychische Beeinträchtigung seiner Person stützen können (vgl. dazu auch die Schlussanträge im Verfahren C-340/21, GRUR-RS 2023, 8707, wonach die Objektivierung einer nachweisbaren Beeinträchtigung der physischen und psychischen Sphäre oder des Beziehungslebens einer Person entscheidend ist). Der Senat folgt insoweit den überzeugenden Ausführungen des Oberlandesgerichts Hamm im Urteil vom 15.8.2023 (7 U 19/23, juris Rn. 163 ff.; ebenso OLG Stuttgart, Urt. v. 22.11.2023 – 4 U 20/23, GRUR-RS 2023, 32883, Rn. 124), wonach für die vom Kläger behaupteten immateriellen Schäden in Form von Angst, Sorge und Unwohlsein jedenfalls auch objektive Beweisanzeichen vorhanden sein müssen, da andernfalls die bloße Bekundung des Betroffenen, einen immateriellen Schaden in Form belastender Gefühle erlitten zu haben, für einen Ersatzanspruch ausreichen würde. Dies bedeutet auch gerade nicht, dass damit doch wieder eine wie auch immer gelagerte Erheblichkeitsschwelle im Rahmen des Art. 82 Abs. 1 DSGVO implementiert würde, sondern allein, dass wegen der Natur des auf Schadenskompensation gerichteten Ersatzanspruchs eine objektivierbare immaterielle Beeinträchtigung feststellbar sein muss. 47

Wie mit den Parteien im Termin zur mündlichen Verhandlung erörtert, handelt es sich bei der hier betroffenen Telefonnummer des Klägers um ein personenbezogenes Datum, welches jedenfalls nicht per se als „sensibel“ einzustufen oder seiner Natur nach auf Geheimhaltung angelegt ist, wie dies beispielsweise bei Gesundheits- oder Bankdaten der Fall sein kann, aber nicht auf die Fälle des Art. 9 DSGVO beschränkt sein muss. Mag bei einer Veröffentlichung solcher Daten bereits deren sensibler Charakter im Einzelfall im Rahmen des § 286 Abs. 1 ZPO indiziell dafür sprechen können, dass der Kontrollverlust darüber dem Betroffenen tatsächlich Angst, Sorge oder Unwohlsein bereitet, so ist dies bei einer Telefonnummer – einem personenbezogenen Datum, welches üblicherweise im Alltag der Kommunikation mit anderen Personen im privaten und beruflichen Bereich zu dienen bestimmt ist – gerade so nicht der Fall. Insofern wäre es Aufgabe des Klägers gewesen, konkret in seiner Person liegende Umstände vorzutragen, die einen Rückschluss darauf zulassen, dass er durch die Veröffentlichung seiner Telefonnummer im sog. Darknet tatsächlich Angst, Ärger oder Unwohlsein erlitten hat. 48

Dies hat er jedoch nicht getan, sondern vielmehr lediglich mit Textbausteinen, die seine Prozessbevollmächtigten in einer Vielzahl von beim Senat anhängigen Verfahren in identischer Form verwendet haben, pauschal behauptet, „*die Klägerseite*“ sei nach Kenntnis der Veröffentlichung ihrer Telefonnummer „*in einem Zustand großen Unwohlseins und großer Sorge über möglichen Missbrauch ihrer sie betreffender Daten*“ verblieben. Wenn auch ein Sachvortrag bereits dann schlüssig und ausreichend substantiiert ist, wenn die vorgetragenen Tatsachen in Verbindung mit einem Rechtssatz geeignet sind, das geltend gemachte Recht 49

zu begründen (vgl. BGH, Urt. v. 28.4.2023 – V ZR 270/21, juris), so wird allerdings dieser textbausteinmäßige Vortrag diesen Anforderungen nicht gerecht. Auch auf entsprechenden Hinweis des Senats in der mündlichen Verhandlung (vgl. dazu BGH, Urt. v. 27.9.2006 – VIII ZR 19/04, NJW 2007, 2414) haben die Prozessbevollmächtigten des Klägers keine näheren Ausführungen dazu gemacht, welche konkreten Gefühle der Kläger in Reaktion auf den Datenschutzvorfall bei der Beklagten gehabt hat, wie sich diese Gefühle bei ihm gezeigt haben bzw. welches konkrete Verhalten des Klägers nach Kenntniserlangung von dem Scraping-Vorfall eindeutige Schlussfolgerungen auf vom Kläger empfundene negative Gefühle oder psychische Beeinträchtigungen erlaubt. Aus dem sonstigen Akteninhalt sind solche objektiven Beweisanzeichen ebenfalls nicht ersichtlich, denn unstreitig hat der Kläger seinen Account auf der Plattform der Beklagten bis zuletzt weder gekündigt noch die Suchbarkeitseinstellungen seines Profils geändert. Auch seine Telefonnummer hat er unverändert beibehalten. Mangels hinreichend konkreten Klägervorbringens bestand keine Veranlassung zur persönlichen Anhörung des Klägers, da dies auf eine Ausforschung hinausgelaufen wäre.

(d) Daneben hat der Kläger auch zu vermeintlichen immateriellen Schäden, die er in Form einer Belästigung mit Spam-SMS bzw. Spam-Anrufen erlitten haben will, nicht substantiiert vorgetragen. Denn auch in diesem Zusammenhang finden sich in den Schriftsätzen außer dem erneut nur pauschalen Vorbringen in Form der universell einsetzbaren Textbausteine („*Darüber hinaus erhält die Klägerseite seit dem Vorfall unregelmäßig unbekannte Kontaktversuche via SMS und E-Mail*“, vgl. Bl. 24 d.A. bzw. „*Seit April 2021 erhält die Klägerseite vermehrt dubiose Nachrichten und E-Mails der oben beschriebenen Art*“, vgl. Bl. 42 d.A.) keine konkreten Angaben des Klägers dazu, in welchem Umfang er vor dem streitgegenständlichen Scraping-Vorfall bereits Spam-SMS oder Spam-Anrufe erhalten hat und in welchem Maße sich dies im nachfolgenden Zeitraum dann geändert hat. Der einzige konkrete Vortrag des Klägers in diesem Zusammenhang beschränkt sich auf die mit Schriftsatz vom 8.11.2023 als Anlage K 6 vorgelegten zwei Screenshots, aus denen sich zwei Anrufe unbekannter Nummern mit mutmaßlich verdächtigen Links am 6.10.2021 ergeben. Das von ihm pauschal behauptete „*vermehrte*“ Auftreten „*dubioser Nachrichten*“ ab April 2021 ist damit nicht dargelegt; ebensowenig trägt der verwendete Textbaustein den Umständen des konkreten Einzelfalles Rechnung, da die E-Mail-Adresse des Klägers unstreitig nicht im gescrapten Datensatz enthalten war und daher das streitgegenständliche Scraping schon aus diesem Grunde nicht – wie aber textbausteinmäßig vorgetragen – zu „*Kontaktversuchen via …E-Mail*“ bzw. „*dubiosen … E-Mails*“ hat führen können. 50

(e) Einen immateriellen Schaden hat der Kläger auch nicht insoweit substantiiert dargelegt, als er Zeit und Mühe für eine Auseinandersetzung mit dem Scraping-Vorfall bzw. für Maßnahmen zum Schutz vor künftigem Missbrauch seiner Daten aufgewendet haben will. 51

Der Kläger hat in diesem Zusammenhang weder vorgetragen, wie und wann er sich – in welcher Form – überhaupt näher mit dem Scraping-Vorfall auseinandergesetzt hat noch hat er dargetan, welche konkreten Maßnahmen er ergriffen hat, um sich vor künftigem Missbrauch seiner Daten zu schützen. Vielmehr beschränkt sich sein Vortrag auch in diesem Fall auf Textbausteine, die seine Prozessbevollmächtigten in einer Vielzahl von beim Senat anhängigen Verfahren in identischer Form verwendet haben (vgl. Bl. 44, 317, 370 d.A., Bl. 222 SH). Dies reicht nicht aus, um einen konkret dem Kläger entstandenen Schaden darzulegen. Die prozessuale Unzulänglichkeit dieser pauschalen Verwendung der immer gleichen Textbausteine ohne Bezug zum konkreten Einzelfall zeigt sich vorliegend unter anderem auch daran, dass im Schriftsatz vom 13.1.2023 (Bl. 895 d.A.) vorgetragen wird: „*Die* 52

Klägerseite hat auch zusätzlich Zeit und Mühe aufgewendet, um sich vor drohendem (weiteren) Missbrauch zu schützen. Auch dies hat die Klägerseite in der Verhandlung bestätigt“, obwohl der Kläger in der mündlichen Verhandlung beim Landgericht weder Angaben zur Sache gemacht hat noch überhaupt anwesend war.

(f) Soweit der Beklagten möglicherweise ein Verstoß gegen Art. 33 Abs. 1, Art. 34 Abs. 1 DSGVO wegen einer unterlassenen Meldung des Datenschutzvorfalls vorzuwerfen ist, hat der Kläger jedenfalls keine immateriellen Schäden geltend gemacht, die auf diesen Verstoß zurückzuführen sind. 53

Dabei kann dahinstehen, ob – wie dies die Beklagte geltend macht – ein Verstoß gegen diese Vorschriften nicht in den Schutzbereich von Art. 82 DSGVO fällt, weil der Datenschutzverstoß nicht im Zuge einer Verarbeitung entstanden sein soll. Denn die behaupteten immateriellen Schäden in Form von Angst, Sorge, Unwohlsein sowie Belästigung durch Spam-Anrufe bzw. Spam-SMS könnten, selbst wenn sie beim Kläger tatsächlich vorliegen würden und man sie im Rahmen des Art. 82 Abs. 1 DSGVO ausreichen lassen wollte (vgl. dazu Vorlagefrage 4 im Verfahren BGH, Beschl. v. 26.9.2023 – VI ZR 97/22, GRUR-RS 2023, 30210), jedenfalls nicht kausal auf einen Verstoß der Beklagten gegen Art. 33 Abs. 1, 34 Abs. 1 DSGVO zurückgeführt werden. Dabei kommt es auch nicht auf die Frage der genauen Verteilung der Darlegungs- und Beweislast für die Kausalitätsfragen im Rahmen des Art. 82 Abs. 1 DSGVO (dazu OLG Stuttgart, Urt. v. 31.3.2021 – 9 U 34/21, BeckRS 2021, 6282 – z.Zt. BGH – VI ZR 111/21) an. Denn die für diese Schäden nach eigenen Angaben des Klägers maßgebliche Veröffentlichung der Telefonnummer in Verbindung mit seinem Namen im sog. Darknet hätte – anderes macht auch der Kläger selbst gar nicht geltend – durch eine Meldung der Beklagten bei ihm oder der Aufsichtsbehörde offensichtlich nicht mehr verhindert werden können. Der Kläger hat auch nichts dazu vorgetragen – und es ist auch sonst nicht ersichtlich – ob und in welcher Weise er sich bei früherer Information der Beklagten vor den angeblich erlittenen Schäden (Angst, Unsicherheit, Misstrauen, Belästigung durch Anrufe etc.) geschützt hätte bzw. wie ihn die irische Datenschutzbehörde bei einer frühzeitigen Information vor diesen angeblichen Auswirkungen hätte schützen können. 54

Soweit der Kläger sich im Rahmen der Verstöße gegen Art. 33 Abs. 1, 34 Abs. 1 DSGVO darauf beruft, er hätte bei früherer Information zeitnah Schritte zur Risikominimierung und Absicherung einleiten können (vgl. Bl. 45 d.A.), ist auch dies kein hinreichender Vortrag, um einen bei ihm entstandenen immateriellen Schaden feststellen zu können. Auch hier fehlen jegliche Angaben des Klägers dazu, um welche Schritte es sich gehandelt hätte und welche Auswirkungen sie gehabt hätten – zumal er wie gezeigt – die Sicherheitseinstellungen im Profil bis heute nicht geändert und auch seine Telefonnummer beibehalten hat. Soweit der Kläger behauptet, dass die von Seiten der Beklagten unterlassene Meldung des Vorfalls bei der Aufsichtsbehörde seinen Schaden vertieft bzw. intensiviert habe, ist auch dieser Vortrag – trotz entsprechender Rüge der Beklagten – pauschal und unsubstantiiert geblieben. 55

(g) Soweit der Kläger seinen Schadensersatzanspruch schließlich auf eine Verletzung von Art. 15 DSGVO im Hinblick auf eine vermeintlich unzureichende Auskunft der Beklagten über den Scraping-Vorfall stützt, greift auch dies nicht durch. Dabei kann auch hier dahinstehen, ob ein Verstoß gegen diese Vorschrift in den Schutzbereich von Art. 82 DSGVO fällt. Denn die Beklagte hat im Hinblick auf die vom Kläger geforderte Auskunft ihre Verpflichtung aus Art. 15 DSGVO nicht verletzt, da sie weder eine verspätete noch eine unvollständige Auskunft erteilt hat. 56

Die Prozessbevollmächtigten des Klägers haben mit Schreiben vom 4.10.2021 (Anlage K1, Bl. 61 d.A.) Auskunft darüber gefordert, „*ob Sie unsere Mandantschaft betreffende* 57

personenbezogene Daten … im Zusammenhang mit dem im April 2021 bekannt gewordenen Datenschutzvorfall verarbeiten“. Insofern bezog sich das außergerichtliche klägerische Auskunftsersuchen ausdrücklich nur auf den streitgegenständlichen Scraping-Vorfall. Zu diesem Auskunftsersuchen hat die Beklagte in der Folgezeit auch Stellung genommen. Das vom Kläger vorgelegte Schreiben vom 23.8.2021 (Anlage K2) kann zwar nicht den Kläger betreffen, weil dieser selbst erst am 4.10.2021 Auskunft verlangt hat, sondern dürfte einem von den Prozessbevollmächtigten des Klägers geführten Parallelverfahren zuzuordnen sein. Der Kläger trägt jedoch in der Klageschrift – von der Beklagten unbestritten – vor, dass auch er auf sein Begehren hin seinerzeit ein inhaltlich entsprechendes Schreiben erhalten habe (vgl. Bl. 25 d.A.). In diesem Schreiben hat die Beklagte hinsichtlich der allgemein von ihr verarbeiteten Daten des Klägers auf ihr Information-Tool verwiesen (Bl. 80 d.A.) und hinsichtlich der konkret verlangten Auskünfte über den Scraping-Vorfall mitgeteilt, es handele sich dabei nicht um eine Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO, so dass der Anwendungsbereich des Art. 15 DSGVO nicht eröffnet sei (Bl. 78 d.A.). Auf entsprechende Nachfrage des Senats im Verhandlungstermin vom 16.11.2023 hat der Prozessbevollmächtigte der Beklagten zudem bestätigt, dass sein schriftsätzlicher Vortrag, die Beklagte besitze keine Kopie der Rohdaten bzw. keine Log-Files, dahingehend zu verstehen sei, dass der Beklagten selbst keine Informationen über die Personen der Scraper bzw. die Einzelheiten des Scraping-Vorgangs vorliegen und sie nur – wie im Falle des Klägers nicht – in den Fällen gegen die Scraper vorgegangen sei, in denen sie ausnahmsweise Kenntnis von den Personen erlangt habe. Dem ist die Klägerseite nicht konkret entgegengetreten. Insofern liegt dann aber eine Auskunft vor, die erkennbar den Gegenstand des berechtigten Auskunftsbegehrens des Klägers vollständig abdeckt. Eine Verletzung von Art. 15 Abs. 1 DSGVO durch die Beklagte scheitert daran, dass sie die Auskunft hinsichtlich der allgemeinen Daten des Klägers – soweit eine solche überhaupt verlangt worden sein sollte – (unstreitig) erfüllt hat und sich hinsichtlich der vom Kläger primär begehrten Daten bezüglich des Scraping-Vorfalls – Namen der Scraper, Datum des Zugriffs etc. – jedenfalls von Anfang an auf Unmöglichkeit berufen konnte.

Soweit der Kläger in diesem Zusammenhang die Entscheidung des Europäischen Gerichtshofs vom 12.1.2023 (C-154/21, NJW 2023, 973) zur Reichweite des Auskunftsanspruchs anführt, kann auch dies der Berufung nicht zum Erfolg verhelfen. Der Europäische Gerichtshof hat zwar die Regelung in Art. 15 Abs. 1 lit. c) DSGVO dahingehend ausgelegt, dass sich das Auskunftsrecht des Betroffenen gegen den Verantwortlichen auch auf die Identität des Empfängers der Daten bezieht. Er hat jedoch gleichzeitig klargestellt, dass diese Verpflichtung zur Auskunft über die Identität des Empfängers nicht eingreift, wenn es dem Verantwortlichen – wie vorliegend der Fall – nicht möglich ist, die Empfänger zu identifizieren und sich in diesen Fällen das Auskunftsrecht auf Informationen über die Kategorie von Empfängern bezieht. 58

Auch auf die weitere Rechtsfrage, ob ein Auskunftsbegehren nach Art. 15 Abs. 1 DSGVO dann schon als erfüllt anzusehen ist, wenn der Auskunftspflichtige nur deutlich machen kann, sich vollständig erklärt zu haben (u.a. BGH, Urt. v. 15.6.2021 – VI ZR 576/19, NJW 2021, 2726) und die Frage der inhaltlichen Richtigkeit und Vollständigkeit dann möglicherweise im Verfahren auf Abgabe einer eidesstattlichen Versicherung (§§ 259, 260 BGB analog) zu klären wäre, kommt es wegen der Unmöglichkeit – die ganz zweifelsfrei den Anspruch zu Fall bringt – nicht mehr an. 59

c. Eine andere Anspruchsgrundlage kommt für den mit dem Antrag zu 1) geltend gemachten Anspruch auf Ersatz eines immateriellen Schadens nicht in Betracht. Da weder eine deliktische Haftung der Beklagten aus § 823 Abs. 1 BGB i.V.m. dem Recht des Klägers 60

auf informationelle Selbstbestimmung noch eine vertragliche Haftung wegen Pflichtverletzung im Rahmen des zwischen den Parteien bestehenden Nutzungsvertrages, auf den nach den Nutzungsbedingungen der Beklagten deutsches Recht anzuwenden ist (vgl. dazu BGH Urt. v. 12.7.2018 – III ZR 183/17, NJW 2018, 3178), einen Ersatz für immaterielle Schäden in der vom Kläger behaupteten Form vorsieht, kommt es auf die Frage eines Vorrangs der europarechtlichen Schadensersatzregelungen der DSGVO vor nationalen Schadensersatzbestimmungen nicht an. Selbst wenn man hier mit Blick auf Erwägungsgrund Nr. 146 S. 4 der DSGVO etwa das nationale Institut der Geldentschädigung für anwendbar halten wollte, fehlt es ersichtlich an einer schweren Persönlichkeitsrechtsverletzung, zu deren Ausgleich eine Geldzahlung in Betracht gezogen werden könnte.

2. Der – im Termin konkretisierte – Antrag zu 2) auf Feststellung einer Ersatzpflicht für künftige materielle sowie künftige derzeit noch nicht vorhersehbare immaterielle Schäden ist schon unzulässig. Denn es fehlt insoweit an einem Feststellungsinteresse des Klägers. 61

a. Bei reinen Vermögensschäden hängt die Zulässigkeit einer Feststellungsklage von der Wahrscheinlichkeit eines auf die Verletzungshandlung zurückzuführenden Schadenseintritts ab (vgl. BGH, Urt. v. 24.1.2006 – XI ZR 384/03, BGHZ 166, 84; BGH, Urt. v. 29.6.2021 – VI ZR 52/18, NJW 2021, 1330). Grund dafür ist der Schutz des möglichen Schädigers, dem nicht ein Rechtsstreit über gedachte Fragen aufgezwungen werden soll, von denen ungewiss ist, ob sie jemals praktische Bedeutung erlangen könnten. Dagegen genügt bei Verletzung eines absoluten Rechts oder aber in solchen Fällen, in denen bereits ein (Teil-)Schaden eingetreten ist, die bloße Möglichkeit des Eintritts eines Schadens (vgl. BGH, Urt. v. 24.1.2006 – XI ZR 384/03, BGHZ 166, 84; BGH, Urt. v. 29.6.2021 – VI ZR 52/18, NJW 2021, 1330). An der Möglichkeit weiterer Schäden fehlt es in solchen Fällen nur dann, wenn aus Sicht des Klägers bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines weiteren Schadens wenigstens zu rechnen (vgl. BGH, Urt. v. 30.7.2020 – VI ZR 397/19, NJW 2020, 1642; BGH, Urt. v. 5.10.2021 – VI ZR 136/20, juris). 62

b. Soweit das Oberlandesgericht Hamm in seiner Entscheidung vom 15.8.2023 (7 U 19/23, juris, Rn. 208; ebenso OLG Stuttgart, Urt. v. 22.11.2023 – 4 U 20/23, GRUR-RS 2023, 32883 Rn. 91) im Hinblick auf die vom Europäischen Gerichtshof im Zusammenhang mit der Geltendmachung eines sich aus Art. 82 DSGVO ergebenden Schadensersatzanspruchs betonten Gesichtspunkte der Äquivalenz und der Effektivität davon ausgegangen ist, dass diese Rechtsprechung zu den Anforderungen an das Feststellungsinteresse bei Verletzung eines absoluten Rechts auch auf Fälle der Verletzung des „*nach Art. 82 DSGVO absolut geschützten Rechtsguts Datenschutz als (abschließende) europarechtliche Ausformung des deutschen allgemeinen Persönlichkeitsrechts*“ zu übertragen ist, kann diese Frage im Ergebnis hier offen bleiben. Denn auch nach dem für den Kläger günstigeren Maßstab fehlt es vorliegend an einem Feststellungsinteresse, da er nicht hinreichend zur Möglichkeit eines künftigen materiellen oder immateriellen Schadens vorgetragen hat und damit davon auszugehen ist, dass aus seiner Sicht bei verständiger Würdigung kein Grund besteht, mit dem Eintritt weiterer Schäden zu rechnen. 63

aa. Der Kläger hat zunächst behauptet, es sei noch nicht abzusehen, welche Dritten Zugriff auf die Daten erhalten hätten und für welche konkreten kriminellen Zwecke diese Daten missbraucht werden würden (Bl. 48 d.A., Bl. 235 SH). Daneben hat er vorgetragen, es sei möglich, dass er „*erhebliche Belästigung durch eine Vielzahl von betrügerischen Anrufen erleiden*“ könne, bei denen sich die Anrufer beispielsweise als Bankmitarbeiter ausgeben würden, um an sensible Kontodaten zu gelangen (Bl. 321 d.A.). Diese Gefahr sei deshalb groß, weil die Anrufer „*private Details*“ des Klägers kennen würden und damit überzeugend 64

auftreten könnten. Er müsse sich möglicherweise wegen drohender Spam-Anrufe, -SMS oder -Emails eine neue Handynummer zulegen, was mit finanziellen Kosten verbunden sei. Schließlich sei es vorstellbar, dass er sich bei Anrufen mit seinem Namen melde und dann „*in irgendwelchen dubiösen Verträgen drinhänge*“ bzw. auf betrügerische Links klicke, die per SMS oder Email versendet würden (Bl. 897 d.A.). Mit der Berufungsbegründung macht der Kläger darüber hinaus noch geltend, in H. seien in der Zeit bis September 2022 Schäden durch sog. WhatsApp-Betrug in Höhe von 780.000 Euro entstanden und weitere Schäden durch andere Trickbetrügereien im Zusammenhang mit Handy und Computern.

bb. Auf Basis dieses Vortrags besteht aus Sicht des Klägers bei verständiger Würdigung kein Grund, mit dem künftigen Eintritt eines materiellen und/oder derzeit noch nicht vorhersehbaren immateriellen Schadens zu rechnen, da sämtliche seiner Befürchtungen zur künftigen Schadensentwicklung rein theoretischer Natur sind. Dem Kläger ist bis zum Tag der mündlichen Verhandlung vor dem Senat – vier Jahre nach dem streitgegenständlichen Scraping-Vorfall und 2 ½ Jahre nach dessen Bekanntwerden in der Öffentlichkeit – kein materieller oder immaterieller Schaden entstanden und er hat auch keine Anhaltspunkte dafür vorgetragen, die solche (zudem auf den Vorfall zurückzuführenden) Schäden in Zukunft als möglich erscheinen lassen. 65

Dies gilt zunächst für die Ausführungen des Klägers zu möglichen kriminellen Aktivitäten per E-Mail, da seine E-Mail-Adresse unstreitig weder im Rahmen des streitgegenständlichen Vorfalls „gescraped“ noch anschließend veröffentlicht wurde. 66

Dies gilt ebenso für die von ihm behauptete Gefahr, dass Kriminelle am Telefon ihm gegenüber deshalb überzeugend auftreten könnten, weil sie Kenntnis von „*privaten Details*“ hätten. Denn im konkreten Fall ist der Nachname des Klägers – als mögliches „*privates Detail* “ – gerade nicht „gescraped“ und in Verbindung mit seiner Handynummer veröffentlicht worden. Der Senat hat durchgreifende Zweifel, dass der Kläger einen Anrufer, der ihn mit „*T. F.*“ anspricht, tatsächlich für einen Bankmitarbeiter hält. 67

Soweit der Kläger bereits aktuell vorträgt, durch ungebetene Anrufe belästigt worden zu sein und dass mit solchen Anrufen möglicherweise auch in Zukunft noch zu rechnen sein könnte, ist dies allenfalls ein immaterieller Schaden, der vom Antrag zu 2) nicht erfasst wird, weil sich dieser nur auf derzeit noch nicht vorhersehbare immaterielle Schäden beziehen soll, die Belästigung nach dem Vortrag des Klägers jedoch bereits bekannt und damit vorhersehbar ist und insofern auch zum Gegenstand des mit dem Antrag zu 1) geltend gemachten Ersatzanspruchs gemacht wurde. Dass der Kläger im Rahmen eines solchen Anrufs einen ungewollten Vertrag abschließt und damit möglicherweise künftig ein materieller Schaden entsteht, hält der Senat vor dem Hintergrund, dass der Kläger gleichzeitig geltend gemacht hat, aufgrund des Scraping-Vorfalls bei der Beklagten sehr misstrauisch gegenüber Anrufen und SMS-Nachrichten geworden zu sein, ebenfalls für fernliegend. Gleiches gilt schließlich für einen möglichen künftigen Schaden durch die angeblich drohende Notwendigkeit eines Wechsels seiner Handynummer, da ein solcher bisher – vier Jahre nach dem Vorfall und 2 ½ Jahre nach dessen Bekanntwerden – noch nicht erfolgt ist. Auf die Frage, ob für einen solchen Wechsel tatsächlich Kosten anfallen kommt es daher nicht an. 68

Soweit das OLG Stuttgart (Urt. v. 22.11.2023 – 4 U 20/23, GRUR-RS 2023, 32883, Rn. 92 ff.) eine Möglichkeit künftiger immaterieller bzw. gegebenenfalls auch materieller Beeinträchtigungen mit dem Argument bejaht hat, „*die (endgültig) verlorene Kontrolle über die Telefonnummer*“ ermögliche einen weiteren Missbrauch und es bestehe daher „*evident die Möglichkeit, dass … weitere materielle oder immaterielle Beeinträchtigungen beim Kläger eintreten könnten*“, vermag sich der Senat dem nicht anzuschließen. Soweit der Kläger – was 69

möglich sein dürfte – auch in Zukunft Anrufe von Dritten erhält, die seine Telefonnummer aus dem „gescrapten“ Datensatz erlangt haben, ist die damit verbundene immaterielle Beeinträchtigung bereits bekannt und vom Kläger zum Gegenstand seines Schadensersatzanspruchs nach dem Antrag zu 1) gemacht worden. Hinsichtlich künftiger materieller Schäden fehlt es – wie bereits ausgeführt – an jeglichen Anhaltspunkten dafür, dass der Kläger nach dem zwischenzeitlichen Zeitablauf und seiner von ihm selbst vorgetragenen misstrauischen Einstellung gegenüber Anrufen und SMS noch einen materiellen Schaden aus entsprechenden Anrufen erleiden könnte, unabhängig von der Frage, ob sich in Zukunft stattfindende Anrufe, SMS-Nachrichten überhaupt dem hier in Rede stehenden Scraping-Vorfall zuordnen lassen können. Würde man die Anforderungen an den Möglichkeitsnachweis im Rahmen des § 256 Abs. 1 ZPO mit dem OLG Stuttgart (a.a.O.) so weit absenken, würde die besondere Sachentscheidungsvoraussetzung aus § 256 Abs. 1 ZPO in Fällen wie hier letztlich obsolet (so im Ergebnis auch OLG Hamm, Urt. v. 15.8.2023 – 7 U 19/23, juris Rn. 214 ff.).

3. Der auf Unterlassung gerichtete Antrag zu 3) ist ebenfalls unzulässig. 70

a. Mit dem Antrag zu 3a) verlangt der Kläger Unterlassung insoweit, als seine personenbezogenen Daten „*unbefugten Dritten*“ über das CIT zugänglich gemacht werden, ohne dass die „*nach dem Stand der Technik möglichen Sicherheitsmaßnahmen*“ vorgesehen würden, um die „*Ausnutzung des Systems*“ zu verhindern. 71

aa. Ob der Kläger damit – wie das Oberlandesgericht Hamm (Urt. v. 15.8.2023 – 7 U 19/23, juris Rn. 219 ff.) angenommen hat – in der Sache tatsächlich einen Leistungsantrag geltend macht, dessen Zulässigkeit dann an § 259 ZPO scheitert, kann dahinstehen. Ebenso kann offen bleiben, ob es dem Antrag schon deshalb an der hinreichenden Bestimmtheit fehlt (OLG Hamm, a.a.O., Rn. 238 ff.), weil er bezüglich der beantragten Unterlassungspflicht der Beklagten auf die „*nach dem Stand der Technik möglichen Sicherheitsmaßnahmen*“ abstellt und dem Antrag damit nicht zu entnehmen ist, welche konkreten Maßnahmen die Beklagte im Verurteilungsfall zu treffen hat, womit der Streit über die „*möglichen Sicherheitsmaßnahmen*“ unzulässigerweise ins Vollstreckungsverfahren verlagert wird, oder aber ob ein solcher Antrag im Hinblick auf den Anspruch des Klägers auf effektiven Rechtsschutz und seine fehlende Kenntnis über die Details der Sicherheitsmaßnahmen bei der Beklagten hinzunehmen ist. 72

bb. Denn letztlich ist der Antrag zu 3a) jedenfalls aus einem anderen Grund zu unbestimmt und damit unzulässig: Sowohl der Begriff „*unbefugte Dritte*“ als auch die Formulierung „*Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme*“ lassen das Rechtsschutzziel des Klägers nicht hinreichend deutlich erkennen. Es wäre bei einer entsprechenden Verurteilung der Beklagten nicht nur ungeklärt, welche konkreten (technischen) Sicherheitsmaßnahmen diese im Rahmen der vom Kläger begehrten Unterlassungsverpflichtung zu ergreifen hätte, sondern es ergäbe sich aus einem solchen Titel auch nicht, welches konkrete Ziel sie mit den betreffenden Sicherungsmaßnahmen überhaupt erreichen müsste. Nach § 253 Abs. 2 Nr. 2 ZPO darf ein Verbotsantrag nicht derart undeutlich gefasst sein, dass Gegenstand und Umfang der Entscheidungsbefugnis des Gerichts (§ 308 S. 1 ZPO) nicht erkennbar abgegrenzt sind, sich der Beklagte deshalb nicht erschöpfend verteidigen kann und letztlich die Entscheidung darüber, was dem Beklagten verboten ist, dem Vollstreckungsgericht überlassen bliebe (vgl. BGH, Urt. v. 4.10.2007 – I ZR 143/04, NJW 2008, 1384). Zwar sind auslegungsbedürftige Begriffe im Rahmen von § 253 Abs. 2 Nr. 2 ZPO bei Unterlassungsanträgen nicht schlechthin unzulässig. Sie können hingenommen werden, wenn über den Sinngehalt der verwendeten Begriffe oder 73

Bezeichnungen kein Zweifel besteht, so dass die Reichweite von Antrag und Urteil feststeht (vgl. BGH, Urt. v. 1.12.1999 – I ZR 49/97, BGHZ 143, 214). Gerade dies ist vorliegend aber nicht der Fall, da weder durch die Klageanträge noch durch eine zur Auslegung heranzuziehende Klagebegründung (vgl. dazu BGH, Urt. v. 8.5.2014 – I ZR 217/122, BGHZ 201, 129; BGH, Urt. v. 13.9.2012 – I ZR 230/11, BGHZ 194, 314; BGH, Urt. v. 18.12.2015 – V ZR 160/14, NJW 2016, 863) festgestellt werden kann, welches konkrete Verhalten die Beklagte nach dem Willen des Klägers künftig zu unterlassen haben soll.

Der Kläger bezieht sich mit seinem Antrag – wie mit den Parteien in der mündlichen Verhandlung erörtert – auch nicht etwa auf einen konkreten rechtswidrigen Datenschutzvorfall in der Vergangenheit, dessen Wiederholung auf der Plattform der Beklagten er für die Zukunft verhindern will, was etwa – wie auch sonst bei Unterlassungsbegehren - durch Aufnahme der konkreten Verletzungsform in den Antrag hätte deutlich gemacht werden können. Vielmehr erstrebt er ganz allgemein und pauschal, dass die Beklagte ihre im sozialen Netzwerk erfolgende Datenverarbeitung künftig an den Regelungen der DSGVO, insbesondere den Anforderungen an die Sicherheit der Verarbeitung nach Art. 32 DSGVO ausrichtet und damit den Zugriff durch „*unbefugte Dritte*“ zu „*anderen Zwecken als der Kontaktaufnahme*“ verhindert. Aus einem entsprechenden Titel wäre aber keine hinreichend deutliche Unterlassungsverpflichtung der Beklagten abzuleiten: Den vom Kläger beanstandeten Zwischenfall in Form des massenhaften Zugriffs auf das CIT sowie die dabei erfolgte Verbindung zwischen Telefonnummer und Nutzerprofil kann es – unabhängig davon, dass dieser konkrete Zwischenfall schon nicht zum Gegenstand des hier gestellten Unterlassungsantrags gemacht wurde – ohnehin nicht mehr geben, da der Kläger die Suchbarkeit seiner Telefonnummer durch entsprechende Einstellungen (z.B. Umstellung auf „*only me*“) einfach selbst verhindern kann, es das CIT in seiner damaligen (technischen) Form nicht mehr gibt und die Beklagte auch deutlich gemacht hat, es nicht mehr implementieren zu wollen. Einen über diesen konkreten Vorfall hinausgehenden allgemeinen Anspruch gegen die Beklagte, bei Betrieb ihres sozialen Netzwerkes die Vorschriften der DSGVO – insbesondere jene zur Sicherheit der Verarbeitung nach Art. 32 DSGVO – zu beachten und einzuhalten, kann der Kläger aber dann nicht mit einem Unterlassungsantrag geltend machen (nur im Ergebnis ebenso OLG Stuttgart, Urt. v. 22.11.2023 – 4 U 20/23, GRUR-RS 2023, 32883 Rn. 268, wonach der Unterlassungsanspruch zwar zulässig aber unbegründet sei, weil Art. 17 DSGVO allein ein Löschungsrecht bezüglich personenbezogener Daten einräumt, jedoch keine weitergehenden Rechte bezüglich der Datenverarbeitungsvorgänge an sich normiere). 74

Dabei verkennt der Senat nicht, dass die Nutzer der sozialen Plattform der Beklagten durchaus ein berechtigtes Interesse daran haben mögen, dass die Beklagte die nach den Umständen gebotene größtmögliche Sicherheit für die von ihr verarbeiteten Daten garantiert. Ein pauschaler Unterlassungsanspruch lässt sich aus einem derartigen Interesse jedoch nicht ableiten. Vielmehr bezieht sich der Unterlassungsantrag in seiner konkret gestellten Form auf eine unübersehbare Zahl unterschiedlicher Verletzungsformen wegen künftiger möglicher Verstöße der Beklagten gegen die DSGVO oder sonstige für sie geltende gesetzliche Bestimmungen. Durch die unbestimmten Formulierungen „*unbefugte Dritte*“ und „*anderen Zwecke als der Kontaktaufnahme*“ wird der Streit zwischen den Parteien, auf welche Art und Weise die Datenverarbeitung auf der Plattform der Beklagten abzusichern ist, wer als unbefugter Dritter gilt und in welchen Fällen – diese müssen für die Beklagte erkennbar sein, um technische Vorkehrungen für die Abwehr treffen zu können – eine Nutzung der Suchfunktionen der Plattform zu „*anderen Zwecken als der Kontaktaufnahme*“ erfolgt, in das Vollstreckungsverfahren verlagert. 75

76

Entgegen der Auffassung des Oberlandesgerichts Stuttgart (Urt. v. 22.11.2023 – 4 U 20/23, GRUR-RS 2023, 32883 Rn. 101) muss die Unbestimmtheit des Antrags auch nicht etwa deshalb hingenommen werden, weil dem Kläger eine exakte Beschreibung der Sicherheitsmaßnahmen auf der Plattform der Beklagten nicht möglich ist und ihm andernfalls kein wirksamer Rechtsschutz gewährt würde. Wie mit den Parteien in der mündlichen Verhandlung erörtert, hätte der Kläger – was nach der beibehaltenen Antragsfassung aber gerade nicht gewollt ist – ggf. eine Unterlassung der konkret durch die Beklagte begangenen Verletzung verlangen können, wenn man etwa aus Art. 17 DSGVO einen Unterlassungsanspruch ableiten (vgl. Vorlagefragen 1 ff. im Verfahren BGH, Beschl. v. 26.9.2023 – VI ZR 97/22, GRUR-RS 2023, 30210) bzw. einen solchen über §§ 280, 241 Abs. 2 BGB konstruieren wollte (BGH, Urt. v. 29.7.2021 – III ZR 179/20, NJW 2021, 3179) und man dann etwa aus dem (unterstellten) Verstoß gegen die DSGVO bzw. die damit korrespondierenden Pflichten aus § 241 Abs. 2 BGB eine tatsächliche Vermutung der Wiederholungsgefahr hätte ableiten können. In diesem Fall wäre durch eine Bezugnahme auf die konkrete Verletzungsform und deren Beschreibung in der Klagebegründung deutlich geworden, worauf konkret das Rechtsschutzziel des Klägers gerichtet ist und welches Verhalten von der Beklagten in Zukunft verlangt wird. Auf diese erfolgte Verletzung, den unkontrollierten Zugriff auf das nicht hinreichend abgesicherte CIT unter Verwendung einer Masse automatisch generierter Ziffernfolgen in Verbindung mit den Voreinstellungen zur Suchbarkeit, wird der Antrag jedoch nicht gestützt (§ 308 Abs. 1 ZPO); vielmehr ist es nach dem eigenen Vortrag des Klägers so, dass er befürchtet, Dritte könnten trotz der technischen Maßnahmen der Beklagten (Veränderung der Suchmöglichkeiten im oben beschriebenen Umfang) auch künftig neue, letztlich aber andersartige Wege finden, um auf Daten der Nutzer zuzugreifen. Das ist aber zu unbestimmt, zumal man damit eine allgemeine „Gesetzes- und Vertragstreue-Pflicht“ bei jeder einmaligen konkreten Rechtsverletzung für die Zukunft titulieren würde, womit nichts gewonnen wäre. Selbst wenn man dies anders sehen wollte, würde zudem für derart unbestimmte, künftige, anderweitige DSGVO-Verstöße der Beklagten jedenfalls auch eine Erstbegehungsgefahr fehlen.

b. Daneben ist auch der Antrag zu 3b) unzulässig, ohne dass es darauf ankommt, ob die vom Kläger begehrte Unterlassungsverpflichtung im Hinblick auf die Formulierungen „*unübersichtlich*“ und „*unvollständig*“ zu unbestimmt ist (verneinend OLG Stuttgart, Urt. v. 22.11.2023 – 4 U 20/23, GRUR-RS 2023, 32883 Rn. 102). Denn jedenfalls fehlt dem Antrag in der konkret gestellten Form das notwendige Rechtsschutzbedürfnis (vgl. auch OLG Hamm, Urt. v. 15.8.2023 – 7 U 19/23, juris Rn. 236 ff.). 77

aa. Die im Antrag genannten personenbezogenen Daten des Klägers „*Facebook-ID, Familienname, Vorname, Geschlecht*“ sind nach den Nutzungsbedingungen der Beklagten, mit denen sich der Kläger im Rahmen seiner Anmeldung auf der Plattform einverstanden erklärt hat, sog. „*immer öffentliche*“ Nutzerinformationen. Soweit der Kläger dagegen einwendet, die Facebook-ID sei nicht aus seinem Profil ersichtlich, sondern müsse abgerufen werden, ändert dies nichts daran, dass er sich im Rahmen seiner Registrierung auf der Plattform der Beklagten damit einverstanden erklärt, dass es sich um „*immer öffentliche*“ Daten handelt. Sind diese Daten damit mit dem Einverständnis des Klägers der Öffentlichkeit zugänglich, kann er nicht verlangen, dass die Beklagte es künftig unterlässt, diese Daten Dritten zugänglich zu machen. Hinsichtlich der Daten „*Stadt, Beziehungsstatus*“ – letzteres Datum ist vom streitgegenständlichen Scraping ausweislich des vom Kläger vorgelegten Datensatzes gar nicht betroffen – kann der Antrag ebenfalls keinen Erfolg haben, weil der Kläger diese Daten nach dem nicht bestrittenen Vortrag der Beklagten (Bl. 152, 181, 184, 716 d.A.) als „*öffentlich*“ auf seinem Profil eingestellt hat. Weiter werden die Daten „*Land*“ und „*Bundesland*“ nach dem nicht bestrittenen Vortrag der Beklagten (Bl. 130 d.A.) auf der 78

Plattform nicht als Rubrik veröffentlicht.

bb. Daneben fehlt es dem Unterlassungsantrag zu 3b) auch im Hinblick auf die Verarbeitung der Telefonnummer des Klägers, dem einzigen personenbezogenen Datum, welches ohne sein Einverständnis an die Öffentlichkeit gelangt ist, am Rechtsschutzbedürfnis. Denn der Kläger ist – soweit dies nicht ohnehin bereits durch die Systemumstellung der Beklagten bzw. durch die Umgestaltung des CIT im September 2019 obsolet geworden sein sollte, weil die Suche nach einem Nutzerprofil auf Basis der Telefonnummer jetzt ausgeschlossen ist und über das CIT nur noch mit der PYMK-Funktion gesucht werden kann (vgl. Bl. 146, 226, 700 d.A.) – ohne gerichtliche Hilfe selbst in der Lage, seine Telefonnummer einer Verarbeitung durch die Beklagte im Rahmen der Suchbarkeit zu entziehen, indem er die entsprechenden Einstellungen ändert. Er hat zwar schon in erster Instanz (Bl. 323 d.A.) und auch wieder mit der Berufungsbegründung (Bl. 225 SH) geltend gemacht, eine Änderung der konkreten Einstellung würde „*nichts ändern*“ bzw. er könne sich dessen nicht sicher sein. Dieser Vortrag ist allerdings pauschal geblieben und nicht näher erläutert worden. Sollte damit gemeint sein, dass der Kläger befürchtet, es werde auch bei einer Suchbarkeitseinstellung als „*privat*“ bzw. „*only me*“ künftig (technische) Möglichkeiten für Scraper geben, seine Telefonnummer auf der Plattform der Beklagten in Erfahrung zu bringen, würde es sich dabei um einen anderen Streitgegenstand handeln als den vorliegenden, in welchem die betreffenden Daten konkret über eine Nutzung des CIT der eingegebenen Ziffernfolge als Telefonnummer zugeordnet wurden. Sollte damit gemeint sein, dass der Kläger auch einer Einstellung seiner Telefonnummer als „*privat*“ bzw. „*only me*“ in den Suchbarkeitseinstellungen misstraut, was nicht damit in Übereinstimmung zu bringen ist, dass er selbst diese Einstellung der Suchbarkeit an anderer Stelle in seinen Schriftsätzen als erstrebenswerte datenschutzfreundliche Voreinstellung von der Beklagten fordert, erstreckt sich die Antragsfassung (§ 308 Abs. 1 ZPO) darauf nicht. Zudem bleibt es dem Kläger auch unbenommen, seine Telefonnummer komplett aus dem bei der Beklagten gespeicherten Datensatz zu löschen. Die Nutzung eines Profils auf der Plattform der Beklagten ist – von der erstmaligen Registrierung oder der Sicherung über eine Zwei-Faktor-Authentifizierung abgesehen – unstreitig nicht von der (dauerhaften) Speicherung einer solchen Nummer im Datenbestand der Beklagten abhängig. Auch der Kläger stellt nicht in Abrede, dass die Beklagte dem Nutzer die einfache Möglichkeit anbietet, seine Telefonnummer dauerhaft zu löschen. Insofern erschließt sich dem Senat nicht, woher dann noch ein Bedürfnis gerade des Klägers für einen entsprechenden Unterlassungstitel herrühren soll. Ein Rechtsschutzbedürfnis für die Geltendmachung eines Unterlassungsanspruchs zugunsten anderer Nutzer besteht ebenfalls nicht. 79

cc. Soweit der Kläger in der Berufungsbegründung erstmals geltend macht, ein Scraping über das CIT wäre damals auch möglich gewesen, wenn die Suchbarkeitseinstellungen für die Telefonnummer auf „*Freunde von Freunden*“ eingestellt gewesen wären, kann offen bleiben, ob dieser neue Vortrag trotz § 531 Abs. 2 ZPO noch zuzulassen ist, wozu entgegen § 520 Abs. 3 S. 2 Nr. 4 ZPO auch jedwedes Vorbringen fehlt. Denn auch wenn man im Sinne des Klägers unterstellt, dass eine solche technische Missbrauchsgefahr bestanden hätte, würde auch dies nicht dazu führen, heute noch ein Rechtsschutzbedürfnis für den hier gestellten Unterlassungsantrag zu bejahen. Da es in den Suchbarkeitseinstellungen unstreitig mittlerweile noch die weitere Einstellung „*privat*“ bzw. „*only me*“ gibt bzw. der Kläger seine Telefonnummer vollständig aus dem bei der Beklagten gespeicherten Datensatz löschen könnte, ist es unerheblich, ob und in welchem Umfang das streitgegenständliche Scraping in der Vergangenheit auch bei der Einstellung „*Freunde von Freunden*“ technisch möglich gewesen wäre. 80

81

c. Im Hinblick auf die Unzulässigkeit der vom Kläger gestellten Unterlassungsanträge kommt es auf die Frage, ob ein solcher Unterlassungsanspruch hinsichtlich einer Verarbeitung von Daten aus Art. 17 DSGVO hergeleitet werden kann und auf die weitere Frage, ob alternativ oder daneben möglicherweise auch Unterlassungsansprüche nach nationalem Recht aus §§ 823, 1004 analog BGB geltend gemacht werden können (vgl. zum Streitstand die Ausführungen bei OLG Stuttgart, Urt. v. 22.11.2023 – 4 U 20/23 Rn. 261 ff. sowie Vorlagenfragen 1 ff. bei BGH, Beschl. v. 26.9.2023 – VI ZR 97/22, GRUR-RS 2023, 30210), ebensowenig an wie auf die Frage, ob sich mit dem oben Ausgeführten nicht auch Ansprüche aus §§ 280 Abs. 1, 241 Abs. 2 BGB herleiten lassen würden.

4. Der mit dem Antrag zu 4) geltend gemachte Auskunftsanspruch ist zulässig, aber unbegründet. 82

a. Anders als dies zunächst der Wortlaut des Antrags („*Auskunft über Daten, welche die Beklagte verarbeitet*“) nahelegt, verlangt der Kläger ausweislich seiner Ausführungen in der Klageschrift mit diesem Antrag auch weiterhin keine allgemeine/umfassende Auskunft über seine bei der Beklagten gespeicherten personenbezogenen Daten, sondern vielmehr (lediglich) – wie schon im außergerichtlichen Schreiben vom 4.10.2021 (Anlage K 1, Bl. 61 f. d.A.) – Auskunft darüber, welchen konkreten Empfängern welche seiner Daten im Rahmen des „*Datenschutzvorfalls*“ durch Ausnutzung des CIT zugänglich gemacht wurden (Bl. 39, 314 d.A.). Damit korrespondiert auch sein Hinweis in der Berufungsbegründung, dass die Beklagte sein Auskunftsverlangen noch nicht vollständig erfüllt habe, weil sie ihm – entsprechend der neueren Rechtsprechung des Europäischen Gerichtshofs (Urt. v. 12.1.2023 – C-154/21) – die konkreten Empfänger der „gescrapten“ Daten noch nicht benannt habe, obwohl sie mit Hilfe von sog. Logfiles nachvollziehen könne, wann und von wem seine Telefonnummer mit den anderen Daten seines Profils zusammengeführt worden sei. In dieser Form ist der Auskunftsantrag zulässig, da unter Hinzuziehung der Klagebegründung deutlich wird, auf welchen konkreten Vorfall sich die im Antrag gewählte Formulierung „Scraping“ beziehen soll. Ob dem Kläger eine entsprechende Auskunft (teilweise) bereits erteilt ist bzw. ob diese der Beklagten im Übrigen (teilweise) unmöglich ist, ist allein eine Frage der Begründetheit des Antrags. 83

b. Der Antrag ist jedoch unbegründet, da der Beklagten die vom Kläger verlangte Auskunft über die konkreten Dritten, welche seine Daten von der Plattform abgerufen haben, unmöglich ist. Insofern kann auf die obigen Ausführungen Bezug genommen werden. 84

5. Die prozessualen Nebenentscheidungen beruhen hinsichtlich der Kosten auf § 97 Abs. 1 ZPO und hinsichtlich der vorläufigen Vollstreckbarkeit auf § 709 ZPO. 85

6. Die Revision war zuzulassen, da die Sicherung einer einheitlichen Rechtsprechung eine Entscheidung des Revisionsgerichts erfordert (§ 543 Abs. 2 Nr. 2 ZPO). Der Senat weicht von der Entscheidung des Oberlandesgericht Stuttgart (aaO) ab, was angesichts der Vielzahl an anhängigen Rechtsstreiten zu demselben Sachverhalt und mit identischem Vortrag der Kläger künftig weiterhin auftreten wird. 86

7. Der Senat sieht dagegen keinen Anlass für die Einleitung eines Vorabentscheidungsverfahren nach Art. 267 AEUV oder für die Aussetzung des vorliegenden Verfahrens bis zur Entscheidung des Europäischen Gerichtshofs in den Verfahren C-189/22, C-741/21, C-687/21, C-667/21, C-340/21 und C-307/22. 87

Zur Durchführung eines Vorabentscheidungsverfahrens besteht nach Art. 267 AEUV keine Pflicht, da das vorliegende Urteil in vollem Umfang mit Rechtsmitteln angefochten werden 88

kann. Daneben besteht auch kein Anlass für eine Aussetzung des Verfahrens analog § 148 ZPO. Eine solche Aussetzung kann zwar erfolgen, wenn die Entscheidung des vorliegenden Rechtsstreits von der Beantwortung einer Frage abhängt, die dem Europäischen Gerichtshof bereits in einem anderen Rechtsstreit zur Vorabentscheidung nach Art. 267 AEUV vorgelegt wurde (vgl. BGH, Beschl. v. 28.3.2023 – VI ZR 225/21, juris; BGH, Beschl. v. 24.1.2021 – III ZR 236/10, juris). Dies ist hier aber nicht der Fall:

Die Vorlagefragen im Verfahren C-189/22 und C-667/21 sind für den hier zu entscheidenden Rechtsstreit nicht erheblich, da sie sich mit Problemen bei der Bemessung der Höhe des immateriellen Schadensersatzes befassen, dem Kläger jedoch nach den obigen Ausführungen schon dem Grunde nach gar kein immaterieller Schaden entstanden ist. Gleiches gilt für die Vorlagefragen im Verfahren C-741/21, die sich darum drehen, ob Art. 82 DSGVO jede Beeinträchtigung der geschützten Rechtsposition umfasst bzw. wiederum Fragen der Bemessung und des Ausschlusses eines Ersatzanspruchs für immaterielle Schäden thematisieren. Auch die Vorlagefragen im Verfahren C-687/21 sind für die Entscheidung des hiesigen Rechtsstreits nicht erheblich, da der Senat weder von einer mangelnden Bestimmtheit des Art. 82 DSGVO ausgeht noch über den Fall einer irrtümlichen Weitergabe von Daten in ausgedruckter Form zu entscheiden hat. Im Hinblick auf die in diesem Verfahren formulierte Vorlagefrage Nr. 2 hat der Europäische Gerichtshof bereits in der Entscheidung vom 4.5.2023 (C-300/21, NJW 2023, 1930) entschieden, dass der Betroffene darzulegen und nachzuweisen hat, dass er durch die aus einem Datenschutzverstoß resultierenden negativen Folgen einen immateriellen Schaden erlitten hat. Gleichermaßen unerheblich sind die Vorlagefragen im Verfahren C-340/21, da der Anspruch des Klägers vorliegend zum einen nicht daran scheitert, dass ihm die Beweislast für das Vorliegen geeigneter technischer und organisatorischer Maßnahmen im Sinne von Art. 32 DSGVO auferlegt wird und es zum anderen auch nicht um die Haftung der Beklagten für einen sog. „Hackerangriff“ geht. Soweit im Verfahren C-307/22 schließlich Fragen zur Auskunftspflicht eines Arztes gegenüber seinem Patienten, insbesondere der Überlassung unentgeltlicher Kopien in Rede stehen, ist dem Senat nicht ersichtlich, warum dies für den vorliegenden Rechtsstreit eine Rolle spielen sollte; im Übrigen ist dieses Verfahren durch Urteil des Europäischen Gerichtshofs vom 26.10.2023 bereits entschieden. 89

Auch die vom Bundesgerichtshof im Verfahren VI ZR 97/22 formulierten Vorlagefragen führen hier nicht zu einer Pflicht des Senats, das Verfahren auszusetzen. Denn auch die in diesem Verfahren vorgelegten Fragen sind für den hiesigen Rechtsstreit nicht entscheidungserheblich. Durch die Vorlagefrage Nr. 4 („*Ist Art. 82 Abs. 1 DSGVO dahingehend auszulegen, dass für die Annahme eines immateriellen Schadens im Sinne dieser Bestimmung bloße negative Gefühle wie z.B. Ärger, Unmut, Unzufriedenheit, Sorge und Angst, die an sich Teil des allgemeinen Lebensrisikos und oft des täglichen Erlebens sind, genügen? Oder ist für die Annahme eines Schadens ein über diese Gefühle hinausgehender Nachteil für die betroffene natürliche Person erforderlich?*“) will der Bundesgerichtshof eine Klärung darüber herbeiführen, ob allein alltägliche negative Gefühle des Betroffenen einen Schaden begründen können. Vorliegend scheitert der Schadensersatzanspruch des Klägers allerdings nicht daran, dass der Senat seine behaupteten Gefühle (Angst, Sorge, Ungewissheit etc.) nicht als immateriellen Schaden eingestuft hat, sondern vielmehr daran, dass es an hinreichendem Vortrag des Klägers dazu fehlt, dass er solche Gefühle überhaupt erlebt hat. 90

Berufungsstreitwert: **3.500 Euro** 91

92

(Antrag zu 1): 1.000 Euro, Antrag zu 2): 500 Euro, Antrag zu 3): 1.500 Euro, Antrag zu 4): 500 Euro)
