
Datum: 07.12.2023
Gericht: Oberlandesgericht Köln
Spruchkörper: 15. Zivilsenat
Entscheidungsart: Urteil
Aktenzeichen: 15 U 99/23
ECLI: ECLI:DE:OLGK:2023:1207.15U99.23.00

Tenor:

Die Berufung der Klägerin gegen das Urteil des Landgerichts Aachen vom 23.5.2023 (8 O 241/22) wird zurückgewiesen.

Die Kosten des Berufungsverfahrens trägt die Klägerin.

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

Die Revision wird zugelassen.

Gründe:

I.

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

Die Klägerin hat in erster Instanz behauptet, bei diesem Vorfall seien von ihr Mobiltelefonnummer, Facebook-ID, Vorname, Nachname, Land und Geschlecht erlangt und im sog. Darknet veröffentlicht worden (Bl. 402 d.A.). Einen Auszug aus dem Datensatz hat sie in erster Instanz nicht vorgelegt und ihren Antrag auf Erstattung immaterieller Schäden (Antrag zu 1)) auf die Veröffentlichung „*der Telefonnummer (+49163xxxxxxx) sowie weiterer personenbezogener Daten der Klägerseite*“ gestützt. Weiter hat sie in erster Instanz vorgetragen, dass sie aufgrund der Belästigungen durch Telefonanrufe unbekannter Nummern sowie Spam-SMS die Telefonnummer gewechselt habe. Wegen der weiteren Einzelheiten des Sach- und Streitstandes sowie der erstinstanzlichen Sachanträge wird auf den Tatbestand des angegriffenen Urteils Bezug genommen.

1

2

3

4

5

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

Sie macht geltend, das Landgericht habe verkannt, dass die Beklagte verschiedene Datenschutzverstöße – insbesondere gegen Art. 5, 25 Abs. 1 und 32 Abs. 1 DSGVO sowie gegen Art. 13, 14, 33 und 34 DSGVO – begangen habe. Soweit die Kammer ihren Vortrag zum Schaden als „*pauschal und nichtssagend*“ bezeichnet habe, habe sie übersehen, dass die Klägerin in der Klageschrift vom 12.7.2022 (dort S. 30 ff.) und im Schriftsatz vom 6.2.2023 (dort S. 22 ff.) zu den tatsächlichen Beeinträchtigungen vorgetragen und entsprechend Beweis angetreten habe. Insofern liege eine Verletzung rechtlichen Gehörs der gerichtlichen Hinweispflicht vor, da die Kammer weder Hinweise erteilt noch die Klägerin angehört habe. Nach dem Urteil des Europäischen Gerichtshofs vom 4.5.2023 (C-300/21) sei ein Verstoß gegen die DSGVO zusammen mit einem möglichen Kontrollverlust personenbezogener Daten ausreichend, um einen immateriellen Schaden anzunehmen. Ebenso ergebe eine Auslegung von Erwägungsgrund 85, dass der Verlust der Kontrolle über personenbezogene Daten als Beispiel für einen immateriellen Schaden aufgeführt werde. Vom Betroffenen könne nicht erwartet werden, dass er konkrete Angaben dazu mache, wie sich der Kontrollverlust auf seine persönliche Lebensgestaltung ausgewirkt habe. Im Übrigen habe die Klägerin konkrete Schäden über den Kontrollverlust hinaus erlitten, wie beispielsweise eine Vielzahl von Belästigungen durch Spam- und Betrugsnachrichten über E-Mail und SMS, wenngleich es bisher bei Betrugsversuchen geblieben sei. Die erkennbaren Auswirkungen der bestehenden Ängste, des Stresses, der Komfort- und Zeiteinbußen etc. würden darin liegen, dass sich die Klägerin mit dem Datenleak und der Herkunft der Daten habe auseinandersetzen müssen. Sie sei zeitlich vor dem Scraping-Vorfall kaum bis gar nicht – schon gar nicht in gleicher Quantität – mit Spam-SMS und Spam-Anrufen belästigt worden, wie nach dem Datenleck.

6

Hinsichtlich des Feststellungsanspruchs sei zu berücksichtigen, dass drohende Spam-Anrufe, -SMS oder -E-Mails es erforderlich machen könnten, dass sich die Klägerin eine neue Handynummer zulegen oder den Anbieter wechseln müsse, was mit finanziellen Kosten verbunden sei. Außerdem sei es möglich, dass sie bei betrügerischen Anrufen mit „*ja*“ antworte und dann in „*irgendwelchen dubiosen Verträgen festhänge*“. Dass bereits finanzielle Schäden durch Datenlecks entstanden seien, zeige ein Blick nach H., wo „*immense Schäden durch WhatsApp-Betrug*“ entstanden seien.

7

Bezüglich des vom Landgericht verneinten Unterlassungsanspruchs nimmt die Klägerin zur Begründung der Berufung Bezug auf ihre erstinstanzlichen Ausführungen. Schließlich sei der Auskunftsanspruch entgegen den Ausführungen des Landgerichts nicht erfüllt, weil die Beklagte die Scraper als Empfänger der Daten nicht konkret benannt habe. Wenn sie im Hinblick auf Schutzmaßnahmen für die Nutzer behaupte, dass sie gegen Scraper mit Abmahnungen und Unterlassungsverfügungen vorgehe, müsse sie auch im vorliegenden Verfahren „*Roß und Reiter*“ nennen.

8

Mit Schriftsatz vom 10.11.2023 hat die Klägerin erstmals vorgetragen, dass der Datensatz „*Tel01, Tel02, X., G., female ,,,,, 7/10/2018 12,00,00 AM*“, (vgl. Bl. 417 SH) von dem Scraping-Vorfall betroffen gewesen sei. Im Hinblick auf die in diesem Datensatz enthaltene, vom bisherigen Vortrag abweichende Telefonnummer (+Tel03) hat die Klägerin den Antrag zu 1), der sich bisher auf eine Telefonnummer mit der Bezeichnung (+49163xxxxxx) bezog, geändert. Dies hat sie damit erklärt, dass aufgrund eines Redaktionsversehens/Schreibfehlers die aktuelle Telefonnummer im Antrag wiedergegeben worden sei. Dazu hat die Prozessbevollmächtigte der Klägerin in der mündlichen

9

Verhandlung vor dem Senat ergänzend erklärt, die Klägerin habe, nachdem ihre damalige Telefonnummer (+Tel03) vom streitgegenständlichen Scraping-Vorfall betroffen gewesen sei, Ende des Jahres 2021 die Telefonnummer gewechselt. Ihre neue Telefonnummer (+49163xxxxxxx) sei jedoch ebenfalls vom streitgegenständlichen Scraping-Vorfall betroffen, da sie zum maßgeblichen Zeitpunkt dem Profil eines ihr unbekanntem anderen Nutzers der Beklagten zugeordnet gewesen sei.

- Die Klägerin beantragt nunmehr, 10
- unter Abänderung des am 23.5.2023 verkündeten Urteils des Landgerichts Aachen (8 O 241/22), 11
1. die Beklagte zu verurteilen, an die Klägerseite als Ausgleich für 12
Datenschutzverstöße und die Ermöglichung der unbefugten Ermittlung der Telefonnummer (+49177xxxxxxx) sowie weiterer personenbezogener Daten der Klägerseite wie Vorname, Nachname, E-Mail-Adresse, Geschlecht, Geburtsdatum einen immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, den Betrag von 2.000 Euro aber nicht unterschreiten sollte, nebst Zinsen in Höhe von fünf Prozentpunkten über dem Basiszinssatz seit Rechtshängigkeit zu zahlen;
 2. festzustellen, dass die Beklagte verpflichtet ist, der Klägerseite alle materiellen 13
künftigen Schäden zu ersetzen, die der Klägerseite 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, an die Klägerin für die Nichterteilung einer den 14
gesetzlichen Anforderungen entsprechenden außergerichtlichen Datenauskunft i.S.d. Art. 15 DSGVO einen weiteren immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, den Betrag von 1.000,00 Euro aber nicht unterschreiten sollte, nebst Zinsen in Höhe von fünf Prozentpunkten über dem Basiszinssatz seit Rechtshängigkeit zu zahlen;
 4. die Beklagte zu verurteilen, der Klägerseite Auskunft über die die Klägerseite 15
betreffenden weiteren personenbezogenen Daten zu erteilen, die durch Unbefugte erlangt werden konnten, namentlich welche Daten außer der Telefonnummer der Klägerseite durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch „Web Scraping“, die Anwendung des Kontaktimporttools oder auf andere Weise unbefugt erlangt werden konnten;
 5. die Beklagte verurteilen, es bei Meidung eines für jeden Fall der Zuwiderhandlung 16
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, personenbezogene Daten der Klägerseite, insbesondere die Telefonnummer, unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, wie geschehen anlässlich des sogenannten Facebook-Datenleaks, das nach Aussage der Beklagten im Jahr 2019 stattfand;
 6. die Beklagte zu verurteilen, es bei Meidung eines für jeden Fall der 17
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, personenbezogene Daten

der Klägerseite, insbesondere die Telefonnummer, ohne Einholung einer Einwilligung oder Erfüllung sonstiger gesetzlicher Erlaubnistatbestände zu verarbeiten;

7. die Beklagte zu verurteilen, die Klägerseite von vorgerichtlichen Rechtsanwaltskosten in Höhe von 973,66 Euro zuzüglich Zinsen seit Rechtshängigkeit in Höhe von fünf Prozentpunkten über dem Basiszinssatz gegenüber den Prozessbevollmächtigten der Klägerseite freizustellen. 18

Die Beklagte beantragt, 19

die Berufung zurückzuweisen. 20

Die Beklagte rügt die teilweise Unzulässigkeit der Berufung, da die Klägerin hinsichtlich des vom Landgericht verneinten Unterlassungs- bzw. Auskunftsanspruchs lediglich auf ihren erstinstanzlichen Vortrag verwiesen habe, was nicht ausreichend sei. 21

Im Hinblick auf den angeblich von der Klägerin erlittenen Kontrollverlust könne der Rechtsprechung des Europäischen Gerichtshofs nicht entnommen werden, dass allein ein solcher bereits ausreichend sei, um einen immateriellen Schaden zu begründen. Der Kontrollverlust werde in Erwägungsgrund 75 nicht als Beispiel für einen immateriellen Schaden aufgeführt, sondern könne allenfalls zu einem solchen Schaden führen. Die Klägerin habe keine konkreten Angaben zu den von ihr persönlich erlittenen Beeinträchtigungen gemacht. Vielmehr handele es sich bei ihren Ausführungen um einen formelhaften Vortrag, den die Prozessbevollmächtigten der Klägerin in hunderten von anderen Verfahren wortgleich vorgetragen hätten. Die Beklagte macht geltend, dass das öffentliche Bekanntwerden einer Mobilfunknummer nach der Lebenserfahrung nicht zu psychologischen Beeinträchtigungen führe. 22

Die Beklagte bestreitet weiter – wie schon in erster Instanz – dass die Klägerin durch Spam-SMS oder Spam-E-Mails belästigt worden sei. Auch insofern sei nur floskelhaft und ohne Beweisansatz vorgetragen worden. Den Vortrag der Klägerin zur Betroffenheit ihrer Telefonnummer bzw. zum Wechsel derselben in der mündlichen Verhandlung vom 16.11.2023 bestreitet die Beklagte mit Nichtwissen und rügt insoweit Verspätung. 23

Hinsichtlich des weiteren Vortrags der Parteien wird auf die im Berufungsverfahren gewechselten Schriftsätze Bezug genommen. 24

II. 25

Die zulässige Berufung der Klägerin bleibt in der Sache ohne Erfolg, da das Landgericht ihre 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. 26

A. Entgegen der Ausführungen der Beklagten ist die Berufung der Klägerin nicht deshalb teilweise unzulässig, weil sie im Hinblick auf die Angriffe gegen den Unterlassungsanspruch (Anträge zu 5) und zu 6)) sowie gegen den Auskunftsanspruch (Antrag zu 4)) durch den erfolgten Verweis auf die erstinstanzlichen Ausführungen den Anforderungen des § 520 Abs. 3 Nr. 2 – 4 ZPO nicht genügt. 27

Nach § 520 Abs. 3 Nr. 2 – 4 ZPO muss die Rechtsmittelbegründung die bestimmte Bezeichnung der im Einzelnen anzuführenden Gründe der Anfechtung enthalten. Die gesetzliche Regelung bezweckt, formale und nicht auf den konkreten Streitfall bezogene 28

Rechtsmittelbegründungen auszuschließen, um dadurch auf die Zusammenfassung und Beschleunigung des Verfahrens im zweiten Rechtszug hinzuwirken. Die Rechtsmittelbegründung muss zudem geeignet sein, die erstinstanzliche Entscheidung im Umfang der Anfechtung infrage zu stellen. Bei mehreren Streitgegenständen oder einem teilbaren Streitgegenstand muss sie sich grundsätzlich auf alle Teile der angefochtenen Entscheidung erstrecken, hinsichtlich derer eine Abänderung beantragt ist; andernfalls ist das Rechtsmittel für den nicht begründeten Teil unzulässig (BGH, Beschl. v. 29.11.2017 – XII ZB 414/17, NJW-RR 2018, 386 m.w.N.). Die Bezugnahme auf das erstinstanzliche Vorbringen ist als Begründung unzureichend. Erforderlich ist eine aus sich heraus verständliche Angabe, welche bestimmten Punkte des angefochtenen Urteils der Berufungskläger weshalb bekämpft. Etwas anderes gilt nur dann, wenn in der Berufungsbegründung an einer in erster Instanz zurückgewiesenen Rechtsansicht festgehalten wird (BGH, Beschl. v. 7.6.2018 – I ZB 57/17, NJW 2018, 2894).

Das Landgericht hat den mit dem Antrag zu 4) geltend gemachten Auskunftsanspruch als unbegründet zurückgewiesen, da die Beklagte den Anspruch der Klägerin aus Art. 15 DSGVO bereits erfüllt habe; soweit durch das Scraping öffentlich einsehbare Daten von Dritten verarbeitet wurden, sei jedenfalls nicht die Beklagte auskunftspflichtig. Die Klägerin verweist in diesem Zusammenhang in ihrer Berufungsbegründung allerdings nicht allein auf die erstinstanzlichen Ausführungen, sondern macht daneben auch geltend, das Landgericht habe übersehen, dass die Scraper als Empfänger konkret zu benennen seien. Dies ist ein hinreichender Angriff gegen die erstinstanzliche Entscheidung, da insofern das Ziel der Klägerin deutlich wird, die Frage der erfolgten Erfüllung des Auskunftsanspruchs unter Hinweis auf den aus ihrer Sicht „offenen“ Teil der Auskunft anzugreifen. Insofern hat die Klägerin zudem – an anderer Stelle des Schriftsatzes – fehlenden Vortrag der Beklagten dazu gerügt, ob und warum diese nicht nachvollziehen könne, wann und von wem die Telefonnummer der Klägerin mit anderen Daten zusammengeführt worden sei. 29

Die Unterlassungsanträge der Klägerin hat das Landgericht daran scheitern lassen, dass ein Verstoß der Beklagten gegen die DSGVO weder in der Vergangenheit zu erkennen noch für die Zukunft zu befürchten sei (Antrag zu 5)) bzw. dass es an einem Verstoß der Beklagten gegen die Vorgaben aus Art. 6, 13 DSGVO (Verarbeitung personenbezogener Daten ohne Einwilligung bzw. ohne sonstigen Erlaubnistatbestand) fehle (Antrag zu 6)). Im Hinblick auf diese Zurückweisung hat die Klägerin in ihrer Berufungsbegründung zwar unter Ziff. V keine konkreten Angriffe formuliert, sondern lediglich auf ihren erstinstanzlichen Vortrag verwiesen. Jedoch hat sie an anderer Stelle der Berufungsbegründung (Ziff. II, Bl. 192 ff. SH) umfangreiche Ausführungen dazu gemacht, welche Datenschutzverstöße die Beklagte vermeintlich begangen hat. Insofern ist auch bei den Unterlassungsanträgen von einer zulässigen Berufung auszugehen. 30

B. Die Berufung der Klägerin ist jedoch unbegründet, da ihr die geltend gemachten Ansprüche gegen die Beklagte nicht zustehen. 31

1. Der auf Ersatz immateriellen Schadens gerichtete Antrag zu 1) ist zulässig, aber unbegründet. 32

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. 33

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).

Nach diesen Grundsätzen liegt hier keine unzulässige alternative Klagehäufung vor, da die Klägerin 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 im April 2021 bekannt gewordenen Scraping-Vorfall, der auf angeblich unzureichenden Sicherungsmaßnahmen bzw. einer Verarbeitung der Daten ohne vorherige ausreichende Informationen zurückzuführen ist 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 die Klägerin zudem seinen Anspruch jedenfalls auch zulässig dahingehend konkretisiert, dass sie den geltend gemachten Betrag von 2.000 Euro für die unzulässige Offenlegung ihrer Telefonnummer sowie sonstige Daten ihres Profils und die damit verbundenen Folgen verlangt.

35

b. Soweit die Klägerin ihren Schadensersatzanspruch mit Schriftsatz vom 10.11.2023 auf das Scraping einer gegenüber der Klagebegründung abweichenden Mobilfunknummer gestützt hat, stellt dies – wenn man darin nicht lediglich eine Korrektur der dem unstreitig bestehenden Profil der Klägerin zugeordneten Mobilfunknummer sehen will – jedenfalls eine zulässige Klageänderung (§ 533 ZPO) dar. Es ist sachdienlich, den zwischen den Parteien bestehenden Streit über Ansprüche der Klägerin aus dem Scraping-Vorfall abschließend zu entscheiden und die vorliegende Entscheidung kann auch auf Tatsachen gestützt werden, die der Senat seiner Entscheidung ohnehin zugrunde zu legen hat. Die Beklagte hat zwar in der mündlichen Verhandlung vor dem Senat den Vortrag der Klägerin zur irrtümlichen Fehlbezeichnung der Telefonnummer im ursprünglichen Klageantrag mit Nichtwissen bestritten. Sie hat aber weder in Reaktion auf das außergerichtliche Schreiben der Klägerin vom 23.5.2022 noch im Verlauf des Verfahrens bestritten, dass die Klägerin über ein Profil auf der Plattform der Beklagten verfügt, dem der von der Klägerin im Schriftsatz vom 10.11.2023, S. 20 vorgetragene Datensatz „Tel01, Tel02, X., G., female, 7/10/2018 12,00,00 AM,“ zugeordnet werden kann.

36

- b.** Der Antrag ist jedoch unbegründet, da der Klägerin der geltend gemachte Schadensersatz weder aus Art. 82 Abs. 1 DSGVO noch aus einer anderen Anspruchsgrundlage zusteht. 37
- aa.** Der Anwendungsbereich von Art. 82 Abs. 1 DSGVO ist zwar in zeitlicher und sachlicher Hinsicht eröffnet. Denn auch wenn sich die Klägerin 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. 38
- 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 der Klägerin „gescrap“ wurden und da sie innerhalb dieses Netzwerkes selbst auch den entsprechenden Suchautomatismus durch das CIT zur Verfügung gestellt hat, der im Rahmen des streitgegenständlichen Datenschutzvorfalls benutzt wurde. 39
- cc.** Der Beklagten dürften darüber hinaus auch Verstöße gegen Art. 5 Abs. 1 lit. b), 25 Abs. 2, 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 der Klägerin verarbeitet wurden, die für den jeweiligen bestimmten Verarbeitungszweck erforderlich waren. Weiter dürfte durch die unterlassene bzw. verspätete Meldung des Vorfalls gegenüber der Klägerin und der irischen Datenschutzbehörde auch ein Verstoß gegen Art. 33 Abs. 1 bzw. Art. 34 Abs. 1 DSGVO vorliegen. 40
- 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 der Klägerin jedenfalls kein immaterieller Schaden durch diese – insofern zu ihren Gunsten als vorliegend unterstellten – Datenschutzverstöße der Beklagten entstanden ist. 41
- In Bezug auf die sich aus Art. 82 DSGVO grundsätzlich ergebenden Vorgaben für die Zuerkennung von Schadensersatzansprüchen wegen immaterieller Schäden verweist der 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 Vorbringen der Klägerin nicht. 42
- Die Klägerin macht geltend, dass sie durch den Scraping-Vorfall einen Kontrollverlust erlitten habe, dass sie Angst, Unwohlsein, Misstrauen und Sorge empfinde sowie durch Anrufe, SMS und E-Mails belästigt werde. Daneben habe sie eine Komfort- und Zeiteinbuße erlitten, weil sie sich mit den Folgen des Datenlecks habe auseinandersetzen müssen und sie habe Zeit und Mühe aufgewendet, um sich vor drohendem (weiteren) Missbrauch zu schützen. Mit diesen Angaben rügt die Klägerin 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). Ihr Vortrag reicht jedoch nicht aus, um einen bei ihr 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). 43

(1) Soweit die Klägerin ihren immateriellen Schaden auf die Veröffentlichung derjenigen Daten stützt, die auf ihrem Profil bei der Beklagten als „*immer öffentlich*“ eingestellt waren (Name, Wohnort, Geschlecht und Facebook-ID), scheidet die Annahme eines immateriellen Schadens schon deswegen aus, weil sich die Klägerin durch ihre 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 der Klägerin durch datenschutzkonforme Voreinstellungen oder technische Sicherheitsmaßnahmen vor einer Kenntnisnahme durch Dritte weitergehend zu schützen. Jedenfalls – und das ist maßgeblich – können sich die von der Klägerin 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 sie selbst auf der Plattform der Beklagten der Öffentlichkeit zugänglich gemacht hat.

(2) Soweit die Klägerin ihren immateriellen Schaden darauf stützt, dass ihre Telefonnummer in Verbindung mit ihrem Vor- und Nachnamen veröffentlicht wurde, handelt es sich bei der Telefonnummer zwar um ein personenbezogenes Datum, das sie nicht der Öffentlichkeit zugänglich machen wollte. Jedoch reicht ihr diesbezüglicher Vortrag zu einem angeblichen Kontrollverlust nicht aus, um einen immateriellen Schaden im Sinne von Art. 82 Abs. 1 DSGVO anzunehmen. 45

(a) Der Senat vermag auf Basis des Vortrags der Klägerin schon nicht festzustellen, dass diese durch den streitgegenständlichen Scraping-Vorfall tatsächlich einen Kontrollverlust im Hinblick auf ihre Telefonnummer erlitten hat. 46

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. Die Klägerin hat jedoch nicht dargelegt, dass sie vor dem streitgegenständlichen Scraping-Vorfall die Kontrolle über ihre Mobilfunknummer hatte und diese erst durch die streitgegenständliche Veröffentlichung der Telefonnummer im sog. Darknet verloren gegangen ist. Sie hat vielmehr zu dem angeblich erlittenen Kontrollverlust nur pauschal unter Verwendung von Textblöcken vorgetragen, die ihre Prozessbevollmächtigten in einer Vielzahl von beim Senat anhängigen Parallelverfahren in identischer Form verwendet haben. Außer der pauschalen, durch die Verwendung einer geschlechtsneutralen Parteibezeichnung in jeglichem Rechtsstreit einsetzbaren Formulierung, „*die Klägerseite*“ habe „*einen Kontrollverlust über ihre Daten*“ erlitten (vgl. Bl. 10, 26 d.A.) bzw. „*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. 226 SH), hat die Klägerin insbesondere keine Angaben zur konkreten Verwendung ihrer 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 die Klägerin, wie mit den Parteien im Termin erörtert, konkret dazu vortragen müssen, wie sie im privaten, geschäftlichen und/oder beruflichen Umfeld mit seiner Telefonnummer vor dem streitgegenständlichen Scraping-Vorfall umgegangen ist, ob und unter welchen Bedingungen sie sie an wen weitergegeben hat und dass insofern durch die Veröffentlichung nach dem Scraping-Vorfall tatsächlich ein Verlust der zuvor über diese 47

Telefonnummer durch sie noch ausgeübten Kontrolle eingetreten ist. Solcher Vortrag findet sich aber weder in ihren Schriftsätzen noch ist er im Rahmen der Erörterung vor dem Senat erfolgt.

(b) Selbst wenn man vorliegend zugunsten der Klägerin unterstellt, dass sie durch den Scraping-Vorfall tatsächlich einen Kontrollverlust über ihre Telefonnummer erlitten hat, weil diese Nummer in Verbindung mit ihrem Vor- und Nachnamen nunmehr durch die Veröffentlichung im sog. Darknet jedenfalls auch einem Personenkreis bekannt geworden ist, dem sie sie selbst gerade so nicht mitteilen wollte, liegt damit noch kein immaterieller Schaden im Sinne von Art. 82 Abs. 1 DSGVO vor. 48

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. 49

Im Rahmen dieses ihr obliegenden Nachweises ist die Klägerin allerdings substantiierten Vortrag schuldig geblieben. Denn dass sie durch den – hier zu ihren Gunsten unterstellten – Kontrollverlust durch die Veröffentlichung ihrer Telefonnummer im sog. Darknet einen immateriellen Schaden erlitten hat, hat sie nicht dargelegt. Vielmehr hat sie 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 sie hinsichtlich der Telefonnummer einen Kontrollverlust erlitten habe. Sie hat in diesem Zusammenhang die Ansicht vertreten, dass damit ein von ihr erlittener immaterieller Schaden bereits feststehe und von ihr als Betroffener nicht erwartet werden könne, konkrete Angaben dazu zu mache, wie sich der Kontrollverlust auf ihre persönliche Lebensgestaltung ausgewirkt habe. 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 die Klägerin – 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). 50

Dieser Bewertung stehen, anders als dies die Klägerin 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 einer solchen Verarbeitung nur potentiell sei.

(c) Soweit die Klägerin weiter geltend macht, sie leide aufgrund der Veröffentlichung ihrer Telefonnummer in Verbindung mit ihrem Vor- und Nachnamen unter Angst, Sorge und Unwohlsein und die Beklagte habe bei ihr einen langanhaltenden Zustand belastender Ungewissheit verursacht, ist auch damit ein immaterieller Schaden nicht hinreichend substantiiert vorgetragen worden. 52

Bei den von der Klägerin geschilderten Beeinträchtigungen handelt es sich um psychische Folgen des Datenschutzverstößes der Beklagten, die als solche nur von ihr 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, Urte. v. 4.5.2023 – C-300/21, NJW 2023, 1930 Rn. 58) und damit über die reine Behauptung des entsprechenden Gefühls hinausgeht, muss die Klägerin konkrete Indizien vortragen und unter Beweis stellen, die eine solche psychische Beeinträchtigung ihrer 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, Urte. v. 22.11.2023 – 4 U 20/23, GRUR-RS 2023, 32883, Rn. 124), wonach für die von der Klägerin behaupteten immateriellen Schäden in Form von Angst, Sorge, Unwohlsein und belastender Ungewissheit 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 53

immaterielle Beeinträchtigung feststellbar sein muss.

Wie mit den Parteien im Termin zur mündlichen Verhandlung erörtert, handelt es sich bei der hier betroffenen Telefonnummer der Klägerin 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 der Klägerin gewesen, konkret in ihrer Person liegende Umstände vorzutragen, die einen Rückschluss darauf zulassen, dass sie durch die Veröffentlichung seiner Telefonnummer im sog. Darknet tatsächlich Angst, Ärger oder Unwohlsein erlitten hat. 54

Dies hat sie jedoch nicht getan, sondern vielmehr lediglich mit Textbausteinen, die ihre 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 von Unwohlsein und Sorge über möglichen Missbrauch ihrer Daten*“ verblieben, was sich „*unter anderem in einem verstärkten Misstrauen gegenüber unerwünschten Kontaktversuchen*“ manifestiert habe. 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 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) hat die Prozessbevollmächtigte der Klägerin keine näheren Ausführungen dazu gemacht, welche konkreten Gefühle die Klägerin in Reaktion auf den Datenschutzvorfall bei der Beklagten gehabt hat, wie sich diese Gefühle bei ihr gezeigt haben bzw. welches konkrete Verhalten der Klägerin nach Kenntniserlangung von dem Scraping-Vorfall eindeutige Schlussfolgerungen auf von ihr empfundene negative Gefühle oder psychische Beeinträchtigungen erlaubt. Aus dem sonstigen Akteninhalt sind solche objektiven Beweisanzeichen ebenfalls nicht ersichtlich, denn unstreitig hat die Klägerin ihren Account auf der Plattform der Beklagten bis zuletzt nicht gekündigt und ihre Telefonnummer auch erst mehrere Monate nach Bekanntwerden des Scraping-Vorfalles geändert. Daneben hat sie auch nicht vorgetragen, auf welchen Umständen ihre Änderungen der Suchbarkeitseinstellungen von „*everyone*“ auf „*only me*“ am 18.9.2020 (vgl. Bl. 355) – also noch vor Kenntniserlangung vom Scraping-Vorfall im April 2021 und fast zwei Jahre vor der Abmahnung vom 23.5.2022 – im Einzelnen beruhten. Mangels hinreichend konkreten Klägervorbringens bestand keine Veranlassung zu einer Anhörung der Klägerin, da dies auf eine Ausforschung hinausgelaufen wäre. 55

(d) Daneben hat die Klägerin auch zu vermeintlichen immateriellen Schäden, die sie 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 („*Die Klägerseite erhielt (und erhält immer noch) insbesondere eine Vielzahl von unerwünschten Telefonanrufen unbekannter Nummer sowie Spam SMS. Darüber hinaus erhält die Klägerseite über WhatsApp Werbung*“, vgl. Bl. 418 d.A. bzw. „*Dazu*“ 56

zählen insbesondere eine Vielzahl von Belästigungen durch Spam- und Betrugsnachrichten via E-Mail und SMS“, vgl. Bl. 223 SH) keine konkreten Angaben der Klägerin dazu, in welchem Umfang sie 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. Auch hier tragen die verwendeten Textbausteine der Prozessbevollmächtigten dem Umstand nicht Rechnung, dass die E-Mail-Adresse der Klägerin unstreitig vom Scraping-Vorfall nicht betroffen ist und daher das streitgegenständliche Scraping schon aus diesem Grunde nicht – wie aber textbausteinmäßig vorgetragen – zu „*Belästigungen durch Spam- und Betrugsnachrichten via E-Mail*“ hat führen können.

(e) Einen immateriellen Schaden hat die Klägerin auch nicht insoweit substantiiert dargelegt, als sie Zeit und Mühe für eine Auseinandersetzung mit dem Scraping-Vorfall, die Ermittlung des Sachverhaltes bzw. für Maßnahmen zum Schutz vor künftigem Missbrauch ihrer Daten aufgewendet haben will. 57

Die Klägerin hat in diesem Zusammenhang weder vorgetragen, wie und wann sie sich – in welcher Form – überhaupt näher mit dem Scraping-Vorfall auseinandergesetzt hat noch hat sie dargetan, welche konkreten Maßnahmen sie ergriffen hat, um sich vor künftigem Missbrauch ihrer Daten zu schützen. Vielmehr beschränkt sich ihr Vortrag auch in diesem Fall auf Textbausteine, die ihre Prozessbevollmächtigten in einer Vielzahl von beim Senat anhängigen Verfahren in identischer Form verwendet haben (vgl. Bl. 33, 418, 419 d.A.). Dies reicht nicht aus, um einen konkret der Klägerin entstandenen Schaden darzulegen. Soweit die Klägerin dem Landgericht im Rahmen der Prüfung eines immateriellen Schadens eine Verletzung der gerichtlichen Hinweispflicht vorwirft, erfolgt dann aber auch mit der Berufungsbegründung (Bl. 220 ff. SH) kein hinreichend substantiiertes Vortrag dazu, welche konkreten Schäden die Klägerin erlitten bzw. welche Maßnahmen sie im Hinblick auf den Scraping-Vorfall ergriffen haben will. Hier hätte insbesondere im Hinblick auf die von der Klägerin tatsächlich gewechselte Telefonnummer ohne weiteres Vortrag erfolgen können und müssen, wie sich dieser Wechsel – als solches letztlich nur ein alltäglicher Vorgang ohne allzu große Mühewaltung – bzw. vorgelagert das Bedürfnis für einen solchen Wechsel konkret ausgewirkt und dabei angeblich einen immateriellen Schaden der Klägerin verursacht haben soll. Dies ist jedoch nicht geschehen; vielmehr vertieft die Klägerin insoweit lediglich ihre Rechtsansicht, bereits ein Verstoß gegen die DSGVO und ein damit verbundener Kontrollverlust sei für einen immateriellen Schaden ausreichend und es könne von ihr als Betroffener nicht erwartet werden, konkrete Angaben dazu zu machen, wie sich der Datenschutzverstoß auf die persönliche Lebensgestaltung ausgewirkt habe. 58

Mangels näheren Sachvortrages hält der Senat es – auch in Ansehung der Bedenken bei der Anwendung der Rechtsfigur des Anscheinsbeweises auf rein individuelle Vorgänge, subjektive Merkmale und innere Tatsachen (dazu allgemein Musielak/Voit/*Foerste*, ZPO, 20. Aufl. 2023, § 286 Rn. 30; Zöller/*Greger*, ZPO, 35. Aufl. 2024, Vor § 284 Rn. 31 jeweils m.w.N.) – nicht für geboten, allein aus dem äußeren Anzeichen des erfolgten Wechsels einer Telefonnummer, zumal dieser erst acht Monate nach Bekanntwerden des Scraping-Vorfalles erfolgt ist, eine entsprechende tatsächliche Vermutung für einen immateriellen Schaden abzuleiten und/oder den Wechsel schon als ausreichendes Beweisanzeichen i.S.d. § 286 Abs. 1 ZPO dafür anzuerkennen. 59

(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 die Klägerin jedenfalls keine immateriellen Schäden geltend gemacht, die auf diesen 60

Verstoß zurückzuführen sind.

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 bei der Klägerin 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 der Klägerin maßgebliche Veröffentlichung der Telefonnummer in Verbindung mit ihrem Namen im sog. Darknet hätte – anderes macht auch die Klägerin selbst gar nicht geltend – durch eine Meldung der Beklagten bei ihr oder der Aufsichtsbehörde offensichtlich nicht mehr verhindert werden können. Die Klägerin hat auch nichts dazu vorgetragen – und es ist auch sonst nicht ersichtlich – ob und in welcher Weise sie sich bei früherer Information der Beklagten vor den angeblich erlittenen Schäden (Angst, Unsicherheit, Misstrauen, Belästigung durch Anrufe etc.) geschützt hätte bzw. wie die irische Datenschutzbehörde sie bei einer frühzeitigen Information vor diesen angeblichen Auswirkungen hätte schützen können.

Soweit die Klägerin sich im Rahmen der Verstöße gegen Art. 33 Abs. 1, 34 Abs. 1 DSGVO darauf beruft, sie hätte bei früherer Information für Aufklärung der konkreten Geschehnisse sorgen (vgl. Bl. 10 d.A.) bzw. sie bei sofortiger Information zeitnahe Schritte zur Risikominimierung und Absicherung hätte einleiten können (Bl. 34 d.A.), ist auch dies kein hinreichender Vortrag, um einen bei ihr entstandenen immateriellen Schaden feststellen zu können. Auch hier fehlen jegliche Angaben der Klägerin dazu, um welche Schritte es sich gehandelt hätte und welche Auswirkungen sie gehabt hätten. Soweit die Klägerin behauptet, dass die von Seiten der Beklagten unterlassene Meldung des Vorfalls bei der Aufsichtsbehörde das Missbrauchsrisiko gesteigert hätten, ist auch dieser Vortrag – trotz entsprechender Rüge der Beklagten – pauschal und unsubstantiiert geblieben.

(g) Soweit die Klägerin ihren 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 von der Klägerin geforderte Auskunft ihre Verpflichtung aus Art. 15 DSGVO nicht verletzt, da sie weder eine verspätete noch eine unvollständige Auskunft erteilt hat.

Die Prozessbevollmächtigten der Klägerin haben mit Schreiben vom 23.5.2022 (Anlage KGR 4, Bl. 138, 147 d.A.) Auskunft darüber gefordert, „*ob Sie unsere Mandantschaft betreffende personenbezogene Daten ... im Zusammenhang mit dem im April 2021 bekannt gewordenen Datenschutzvorfall verarbeiten*“. Insofern bezog sich das außergerichtliche klägerische Auskunftersuchen ausdrücklich nur auf den streitgegenständlichen Scraping-Vorfall. Zu diesem Auskunftersuchen hat die Beklagte in der Folgezeit auch Stellung genommen und mit Schreiben vom 21.6.2022 (Anlage KGR 5, Bl. 151 d.A.) mitgeteilt, nicht über eine Kopie der Rohdaten zu verfügen, die die durch Scraping abgerufenen Daten enthalten. 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 der Klägerin 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 der Klägerin vollständig abdeckt. Eine Verletzung von Art. 15 Abs. 1 DSGVO durch die Beklagte scheidet daran, dass sie die Auskunft hinsichtlich der allgemeinen Daten der Klägerin – soweit eine solche überhaupt verlangt worden sein sollte – (unstreitig) erfüllt hat und sich hinsichtlich der von der Klägerin primär begehrten Daten bezüglich des Scraping-Vorfalles – Namen der Scraper, Datum des Zugriffs etc. – jedenfalls von Anfang an auf Unmöglichkeit berufen konnte.

Soweit die Klägerin 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. 65

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. 66

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 der Klägerin 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 von der Klägerin 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. 67

2. Der Antrag zu 2) auf Feststellung einer Ersatzpflicht der Beklagten für künftige materielle Schäden ist schon unzulässig. Denn es fehlt insoweit an einem Feststellungsinteresse der Klägerin. 68

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).

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 die Klägerin günstigeren Maßstab fehlt es vorliegend an einem Feststellungsinteresse, da sie nicht hinreichend zur Möglichkeit eines künftigen materiellen Schadens vorgetragen hat und damit davon auszugehen ist, dass aus ihrer Sicht bei verständiger Würdigung kein Grund besteht, mit dem Eintritt weiterer Schäden zu rechnen. 70

aa. Die Klägerin hat zu den künftigen materiellen Schäden vorgetragen, es sei noch nicht abzusehen, welche Dritten Zugriff auf die Daten erhalten hätten und für welche konkreten kriminellen Zwecke die Daten missbraucht werden würden (Bl. 36 d.A.). Daneben hat sie geltend gemacht, es könne nicht sicher gesagt werden, ob die Beklagte das Datenleck beseitigt bzw. die unzureichenden technischen Maßnahmen hinsichtlich des CIT ausreichend korrigiert habe (Bl. 37 d.A.). Weiter könnten es in Zukunft drohende Spam-Anrufe, -SMS oder -E-Mails erfordern, dass sie sich eine neue Handynummer zulegen müsse (Bl. 236 SH) und es sei vorstellbar, dass sie bei Betrugsanrufen mit „ja“ antworte und dann in dubiosen Verträgen „festhänge“ (Bl. 236 SH). 71

bb. Auf Basis dieses Vortrags besteht aus Sicht der Klägerin bei verständiger Würdigung kein Grund, mit dem künftigen Eintritt eines materiellen Schadens zu rechnen, da sämtliche ihrer Befürchtungen zur künftigen Schadensentwicklung rein theoretischer Natur sind. Der Klägerin 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 Schaden entstanden und sie hat auch keine Anhaltspunkte dafür vorgetragen, die einen solchen (zudem auf den Vorfall zurückzuführenden) Schaden in Zukunft als möglich erscheinen lassen. 72

Dies gilt zunächst für die textbausteinartigen Ausführungen der Klägerin zu möglichen kriminellen Aktivitäten per E-Mail, da ihre E-Mail-Adresse unstreitig weder im Rahmen des streitgegenständlichen Vorfalls „gescraped“ noch anschließend veröffentlicht wurde. Dies gilt 73

daneben ebenso für die von ihr behauptete Gefahr, dass sie bei Betrugsanrufen mit „ja“ antworte und dann in „*dubiosen Verträgen festhänge*“. Denn selbst man in diesem Zusammenhang zugunsten der Klägerin, die ihre Telefonnummer bereits gewechselt hat, als zutreffend unterstellt, dass die von ihr aktuell verwendete Mobilfunknummer ebenfalls von dem streitgegenständlichen Scraping-Vorfall betroffen und damit der behaupteten Gefahr von Betrugsanrufen ausgesetzt ist, kommt der geltend gemachte künftige Schaden nicht in Betracht: Zum einen handelt es sich bei der Nummer, die die Klägerin aktuell benutzt, nicht um eine Telefonnummer, die ihrem Nutzungsverhältnis mit der Beklagten im Zeitpunkt des streitgegenständlichen Scrapings zugrunde lag. Vielmehr hat die Klägerin diese Nummer erst zu einem späteren Zeitpunkt von einem Provider – dies „belastet“ mit einer Scraping-Betroffenheit eines anderen Nutzers – erhalten. Insofern würde ein krimineller Dritter, der die Klägerin künftig unter dieser (neuen) Nummer anruft, nicht ihren Vor- und Nachnamen aus dem gescrapten Datensatz kennen, sondern vielmehr nur den Datensatz des früheren Nutzers. Darüber hinaus macht die Klägerin selbst geltend, aufgrund des streitgegenständlichen Vorfalls besonders vorsichtig und misstrauisch im Hinblick auf Anrufe und SMS geworden zu sein, so dass der Senat nicht erkennen kann, wie sich in Zukunft – lange Zeit nach dem streitgegenständlichen Vorfall – ein Telefonat mit einem Dritten zu einem ungewollten Vertragsschluss auswachsen könnte, der dann einen materiellen Schaden der Klägerin mit sich bringen könnte.

Soweit die Klägerin geltend macht, sie könne in Zukunft gezwungen sein, ihre Handynummer zu wechseln, was dann wieder einen materiellen Schaden in Form anfallender Kosten mit sich bringen würde, zeigt auch dieser Vortrag die fehlende Eignung von Textbausteinen im Rahmen eines gerichtlichen Verfahrens. Denn unstreitig hat die Klägerin ihre Mobilfunknummer bereits gewechselt, so dass eventuell dafür anfallende Kosten als Schaden bereits entstanden wären und insofern auch beziffert im Rahmen eines Leistungsantrages geltend gemacht werden könnten, was hier jedoch gerade nicht erfolgt ist. 74

Schließlich sind auch die Bedenken der Klägerin gegen die Qualität der technischen Umrüstung des CIT bzw. der künftig herrschenden Sicherheitsmaßnahmen der Beklagten zur Annahme der Möglichkeit eines künftigen materiellen Schadens nicht geeignet. Denn der von ihr gestellte Feststellungsantrag („... *Schäden zu ersetzen, die der Klägerseite durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte ...*“) erstreckt sich auf den früheren Datenschutzvorfall und daraus vermeintlich zu erwartende Schäden, nicht dagegen auf mögliche Schäden aus eventuellen künftigen Vorfällen auf der Plattform der Beklagten, wie sie angeblich trotz technischer Umgestaltungen und erhöhter Sicherheitsanforderungen drohen sollen. 75

Soweit das OLG Stuttgart (Urt. v. 22.11.2023 – 4 U 20/23, GRUR-RS 2023, 32883, Rn. 92 ff.) eine Möglichkeit künftiger 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 ... Beeinträchtigungen beim Kläger eintreten könnten*“, vermag sich der Senat dem nicht anzuschließen. Denn hinsichtlich künftiger materieller Schäden fehlt es – wie bereits ausgeführt – an jeglichen Anhaltspunkten dafür, dass die Klägerin nach dem zwischenzeitlichen Zeitablauf und ihrer von ihr 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 (aaO) so 76

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 Schadensersatz wegen Nichterteilung einer Auskunft gerichtete Antrag zu 3) ist zwar zulässig, aber ebenfalls unbegründet. Denn im Hinblick auf die von der Klägerin geforderte Auskunft über den Scraping-Vorfall hat die Beklagte ihre Pflichten aus Art. 15 DSGVO nicht verletzt, da sie weder eine verspätete noch eine unvollständige Auskunft erteilt hat. 77

Die Prozessbevollmächtigten der Klägerin haben mit Schreiben vom 23.5.2022 (Anlage KGR 4, Bl. 138, 147 d.A.) Auskunft darüber gefordert, „*ob Sie unsere Mandantschaft betreffende personenbezogene Daten ... im Zusammenhang mit dem im April 2021 bekannt gewordenen Datenschutzvorfall verarbeiten*“. Insofern bezog sich das außergerichtliche klägerische Auskunftersuchen ausdrücklich nur auf den streitgegenständlichen Scraping-Vorfall. Zu diesem Auskunftersuchen hat die Beklagte in der Folgezeit mit Schreiben vom 21.6.2022 (Anlage KGR 5, Bl. 151 d.A.) Stellung genommen, wobei sie hinsichtlich der allgemein von ihr verarbeiteten Daten der Klägerin auf ihr Information-Tool verwiesen und hinsichtlich der konkret verlangten Auskünfte über den Scraping-Vorfall mitgeteilt hat, es handele sich dabei nicht um eine Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO, so dass das Auskunftsverlangen fehlgehe. Der Beklagten lägen keine Rohdaten vor, welche die durch Scraping abgerufenen Daten enthielten. 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 der Klägerin nicht – in denjenigen 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 der Klägerin vollständig abdeckt. Eine Verletzung von Art. 15 Abs. 1 DSGVO durch die Beklagte scheidet daran, dass sie die Auskunft hinsichtlich der allgemeinen Daten der Klägerin – soweit eine solche überhaupt verlangt worden sein sollte – (unstreitig) erfüllt hat und sich hinsichtlich der von der Klägerin primär begehrten Daten bezüglich des Scraping-Vorfalles – Namen der Scraper, Datum des Zugriffs etc. – jedenfalls von Anfang an auf Unmöglichkeit berufen konnte. 78

Soweit die Klägerin 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. 79

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, 80

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.

4. Der mit dem Antrag zu 4) gestellte Auskunftsantrag, den der Senat unter Berücksichtigung der Klagebegründung dahingehend auslegt, dass die Klägerin sich auf den hier streitgegenständlichen Scraping-Vorfall bezieht, ist ebenfalls unbegründet. Denn wie vorstehend ausgeführt, ist der Beklagten eine (weitere) Auskunft über die Empfänger oder den Zeitpunkt des Scrapings unmöglich. 81

5. Der auf Unterlassung gerichtete Antrag zu 5), mit welchem die Klägerin verhindern will, dass die Beklagte personenbezogene Daten „*unbefugten Dritten*“ über das CIT zugänglich macht, ist unzulässig. 82

a. Auch wenn die Klägerin sich bei diesem Unterlassungsantrag auf eine konkrete Verletzungsform, nämlich das „*sogenannte Facebook-Datenleak, das nach Aussage der Beklagten im Jahr 2019 stattfand*“ bezieht, hat der Senat Zweifel, ob der Antrag in dieser Form dem Bestimmtheitsgebot des § 253 Abs. 2 Nr. 2 ZPO genügt. 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 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 zweifelhaft, 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, was genau im Rahmen einer künftigen Titulierung unter „*unbefugten Dritten*“ zu verstehen ist. 83

b. Letztlich kann diese Frage aber auch offen bleiben, da dem Antrag der Klägerin jedenfalls das Rechtsschutzbedürfnis fehlt. 84

aa. Soweit sich der Antrag zu 5) nicht nur auf die ausdrücklich genannte Telefonnummer, sondern auch allgemein auf „*personenbezogene Daten der Klägerseite*“ bezieht, fehlt es an konkreten Darlegungen der Klägerin, auf welche personenbezogenen Daten sich dieser Antrag im Einzelnen erstrecken soll. Eine solche ausdrückliche Aufzählung der Daten ist schon deshalb erforderlich, weil auf dem Profil eines Nutzers unstreitig auch Daten von der Beklagten vorgehalten bzw. veröffentlicht werden (können), die nach den bei Registrierung akzeptierten Nutzungsbedingungen der Beklagten als „*immer öffentliche*“ Nutzerinformationen einzuordnen sind bzw. auch solche Daten, welche der Nutzer nach eigener Entscheidung als „*öffentlich*“ eingestellt hat. Soweit es sich um solche „*immer öffentliche*“ oder vom Nutzer freigegebene Daten handelt, mag zwar auch ein Interesse des jeweiligen Nutzers bestehen, dass diese Daten durch technische Sicherungen gegen einen Zugriff durch Kriminelle geschützt werden. Dies ist jedoch ein anderer Streitgegenstand als derjenige, den die Klägerin mit ihrer Bezugnahme auf die konkrete Verletzungsform („*wie geschehen anlässlich des sogenannten Facebook-Datenleaks, das nach Aussage der*“ 85

Beklagten im Jahr 2019 stattfand“) mit dem Unterlassungsantrag geltend macht.

bb. Das Rechtsschutzbedürfnis für den geltend gemachten Unterlassungsantrag fehlt 86
aber auch, soweit sich dieser dagegen wendet, dass die Beklagte die Telefonnummer der
Nutzer über eine Software zum Importieren von Kontakten zugänglich macht. Denn die
Klägerin ist, was sie nach dem Vortrag der Beklagten auch bereits im September 2020 getan
haben soll, ohne gerichtliche Hilfe selbst in der Lage, ihre Telefonnummer durch Änderung
der Suchbarkeitseinstellungen einer Veröffentlichung gegenüber Dritten zu entziehen.
Daneben bleibt es der Klägerin auch unbenommen, ihre 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 die
Klägerin stellt nicht in Abrede, dass die Beklagte dem Nutzer die einfache Möglichkeit
anbietet, eine Telefonnummer dauerhaft zu löschen. Den von der Klägerin beanstandeten
Zwischenfall in Form des massenhaften Zugriffs auf das CIT sowie die dabei erfolgte
Verbindung zwischen Telefonnummer und Nutzerprofil kann es künftig nicht mehr geben, da
die Beklagte das CIT technisch verändert und deutlich gemacht hat, es in der ursprünglichen
Form nicht mehr implementieren zu wollen. Insofern erschließt sich dem Senat nicht, woher
dann noch ein Bedürfnis gerade der Klägerin für einen entsprechenden, in die Zukunft
gerichteten Unterlassungstitel herrühren soll.

Ein Rechtsschutzbedürfnis für die Geltendmachung eines Unterlassungsanspruchs 87
zugunsten anderer Nutzer, die möglicherweise die Suchbarkeitseinstellungen wegen
mangelhafter Information der Beklagten nicht anpassen oder ihre Telefonnummer nicht
löschen, besteht ebenfalls nicht.

6. Auch der Antrag zu 6), mit welchem die Klägerin verhindern will, dass 88
personenbezogene Daten, insbesondere die Telefonnummer, ohne Einholung einer
Einwilligung oder Erfüllung sonstiger gesetzlicher Erlaubnistatbestände verarbeitet werden,
ist unabhängig von Bedenken gegen die hinreichende Bestimmtheit des Antrags jedenfalls
mangels Rechtsschutzbedürfnis unzulässig. Denn auch insoweit muss sich die Klägerin
entgegenhalten lassen, dass sie durch die ihr selbst mögliche Änderung der
Suchbarkeitseinstellung ohne gerichtliche Hilfe in der Lage ist, die Verarbeitung ihrer
Telefonnummer, wie sie bei dem streitgegenständlichen Scraping-Vorfall erfolgt ist, zu
verhindern. Eine allgemeine „Gesetzes- und Vertragstreue-Pflicht“ der Beklagten lässt sich in
diesem Zusammenhang ebensowenig titulieren wie ein Rechtsschutzbedürfnis besteht, im
Wege einer Popularklage Unterlassungsansprüche zu Gunsten anderer (künftiger) Nutzer der
Plattform der Beklagten geltend zu machen.

Im Hinblick auf die Unzulässigkeit der von der Klägerin gestellten Unterlassungsanträge 89
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.

7. Schließlich ist – ohne dass es auf die Fragen des § 86 VVG ankommen würde – 90
auch der mit dem Antrag zu 7) geltend gemachte Anspruch auf Erstattung der

außergerichtlichen Anwaltskosten unbegründet, die dadurch entstanden sein sollen, dass die Prozessbevollmächtigten der Klägerin sich mit Schreiben vom 23.5.2022 (Anlage KGR 4, Bl. 138 d.A.) an die Beklagte gewandt und Unterlassung, Schadensersatz sowie Auskunft über den „im April 2021 bekannt gewordenen Datenschutzvorfall“ verlangt haben. Ein solcher Erstattungsanspruch steht der Klägerin nicht zu.

Für die Anwaltskosten, die auf der außergerichtlichen Geltendmachung von Unterlassungs- und Schadensersatzansprüchen beruhen, folgt dies schon daraus, dass der Klägerin – wie oben ausgeführt – solche Ansprüche gegen die Beklagte nicht zustehen. 91

Für die außergerichtlichen Anwaltskosten, die auf den ebenfalls im obigen Schreiben außergerichtlich geltend gemachten Auskunftsanspruch entfallen, gilt im Ergebnis dasselbe: Soweit in dem Schreiben der Klägerin vom 23.5.2022 nähere Auskunft über den streitgegenständlichen Scraping-Vorfall verlangt wird, hängt ein auf Erstattung der Anwaltskosten für eine solche Tätigkeit gerichteter Anspruch zwar nicht davon ab, dass sich die Beklagte im Zeitpunkt der anwaltlichen Beauftragung in Verzug mit der Auskunftserteilung befand. Denn zwischen den Parteien besteht im Hinblick auf die Nutzung des sozialen Netzwerkes der Beklagten ein Vertragsverhältnis, so dass vertragliche Pflichtverletzungen grundsätzlich einen Schadensersatzanspruch und in diesem Zusammenhang auch einen Auskunftsanspruch begründen können. Jedoch führt auch dies nicht zu einem entsprechenden Erstattungsanspruch der Klägerin: 92

a. Sieht man die (unterstellten) Datenschutzverstöße der Beklagten in Form der datenschutzwidrigen Voreinstellungen zur Suchbarkeit des Profils bzw. in Form der unzureichenden Sicherung des CIT als Pflichtverletzung dieses Nutzungsvertrages an, so erwächst daraus zwar ein Auskunftsanspruch der Klägerin gemäß §§ 280 Abs. 1, 241 Abs. 2 BGB, um mögliche Ansprüche gegen die Beklagte aus diesen Pflichtverletzungen geltend machen zu können. Ein solcher (Hilfs-) Anspruch ist jedoch akzessorisch zu den Hauptansprüchen auf Schadensersatz und/oder Unterlassung, die der Klägerin nach den obigen Ausführungen gerade nicht zustehen. Etwas anderes gilt auch dann nicht, wenn man ein anwaltlich begleitetes Auskunftsbegehren als einen Teil der notwendigen Rechtsverfolgung nach einer objektiven Pflichtverletzung ansehen würde, denn auch dann fehlt es in der Sache an einem durchsetzbaren Hauptanspruch, insbesondere einem Schaden (§§ 249 ff. BGB). 93

b. Stützt man das Auskunftsbegehren der Klägerin alternativ auf die in der Rechtsprechung anerkannte Verpflichtung des Schuldners, im Rahmen einer Rechtsbeziehung nach § 242 BGB Auskunft zu erteilen, wenn der Berechtigte in entschuldbarer Weise über Bestehen und Umfang seines Rechts im Ungewissen ist und der Verpflichtete die zur Beseitigung der Ungewissheit erforderliche Auskunft unschwer geben kann, wobei die Auskunft dann unter Berücksichtigung der jeweiligen Umstände des Einzelfalls und unter Wahrung des Grundsatzes der Verhältnismäßigkeit zu erfolgen hat (vgl. BGH, Urt. v. 27.9.2023 – IV ZR 177/22, NJW 2023, 3490; BGH, Beschl. v. 1.6.2016 – IV ZR 507/15, VersR 2016, 1236; BGH, Urt. v. 2.12.2015 – IV ZR 28/15, VersR 2016, 173; BGH, Urt. v. 26.6.2013 – IV ZR 39/10, VersR 2013, 1381), kann auch dies vorliegend den Erstattungsanspruch der Klägerin wegen der anteiligen außergerichtlichen Anwaltskosten für das Auskunftsbegehren nicht stützen. Denn eine solche Ungewissheit auf Seiten der Klägerin, die eine Auskunft der Beklagten unter Wahrung des Grundsatzes der Verhältnismäßigkeit erforderlich machte, um mögliche Ansprüche durchsetzen zu können, bestand vorliegend gerade nicht. Bereits bei Erstellung des Auskunftsschreibens vom 23.5.2022 war der Klägerin nach eigenen Angaben bekannt, dass es auf der Plattform der 94

Beklagten einen Datenschutzvorfall gegeben hatte, der im April 2021 bekannt geworden war. Weiter war ihr bereits bekannt, dass bei diesem Vorfall personenbezogene Daten wie Name, Facebook-ID, Wohnort, Geburtsdatum und/oder Geburtsort und Mobilfunknummer erlangt und veröffentlicht worden waren; insofern ist in dem betreffenden Schreiben von einer „*eigenen Recherche*“ und davon die Rede, dass „*mindestens eine Information von ihr (die Telefonnummer) im vorbenannten Datensatz enthalten ist*“. Weitergehende Auskünfte über den Scraping-Vorfall, die Personen der Scraper sowie Art und Umfang der betroffenen Daten der Klägerin konnte – wie gezeigt – auch die Beklagte nicht geben, so dass die außergerichtliche Tätigkeit ihrer Prozessbevollmächtigten letztlich auch nicht dazu dienen konnte, mögliche Ansprüche der Klägerin gegen die Beklagte durchzusetzen. Jedenfalls war insofern eine anwaltliche Beauftragung (nur) mit dem Verfolgen des Auskunftsbegehrens nicht erforderlich.

c. Auch wenn man unterstellt, dass in dem betreffenden Schreiben der Klägerin die Forderung nach einer allgemeinen Datenauskunft im Sinne von Art. 15 Abs. 1 DSGVO zu sehen sein sollte – wovon der Senat allerdings im Hinblick auf die Fragestellung auf Bl. 147 d.A., die sich ausdrücklich nur auf den streitgegenständlichen Scraping-Vorfall bezieht, nicht ausgeht – können Anwaltskosten für eine solche Auskunft ebenfalls nicht geltend gemacht werden. Bei dem erstmaligen Verlangen einer Datenauskunft nach Art. 15 DSGVO handelt es sich im Regelfall – abweichende Umstände sind hier nicht geltend gemacht – um einen Bagatellfall, für den anwaltliche Hilfe nicht erforderlich ist. Anderes mag gelten, wenn der Verantwortliche die geforderte Auskunft nicht innerhalb der Frist des Art. 12 Abs. 3 DSGVO erteilt und damit bereits ein Verstoß gegen den Anspruch auf Datenauskunft vorliegt oder besondere Umstände des Einzelfalles hinzutreten, ohne dass es auf die im Termin diskutierte Rechtsfrage ankommen würde, ob in solchen Fällen nur unter den Voraussetzungen der §§ 280 Abs. 1 und 2, 286 BGB Anwaltskosten erstattungsfähig sein können oder nicht. Denn so liegt der Fall hier gerade nicht, da die Klägerin nicht geltend macht, die Beklagte bereits vor der Anfrage vom 23.5.2022 vergeblich um Auskunft ersucht zu haben und sie damit für dieses Auskunftsschreiben vom 23.5.2022 wegen Ablauf der Monatsfrist anwaltliche Hilfe in Anspruch hätte nehmen dürfen. 95

d. Selbst wenn man eine datenschutzrechtliche Pflichtverletzung der Beklagten unterstellt, ergibt sich der Anspruch auf Erstattung der anteiligen Anwaltskosten für das Auskunftsgesuchen auch nicht aus Art. 82 Abs. 1 DSGVO, der Rechtsverfolgungskosten als Teil eines materiellen Ersatzanspruchs umfassen kann (statt aller *Bergt*, in: Kühling/Buchner, DSGVO/BDSG, 4. Aufl. 2024, Art. 82 Rn. 19 m.w.N.; siehe auch OLG Stuttgart, Urt. v. 22.11.2023 – 4 U 20/23, GRUR-RS 2023, 32883 Rn. 286). Denn zum einen bestehen schon keine durchsetzbaren Hauptansprüche und zum anderen war die anwaltliche Beauftragung für die erstmalige Geltendmachung eines Auskunftsanspruchs – auch in Ansehung der eigenen Öffentlichkeitsarbeit der Beklagten zum Scraping-Vorfall – nicht erforderlich. 96

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

9. Die Revision war umfassend 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. 98

Berufungsstreitwert: **5.500 Euro** 99

(Antrag zu 1): 2.000 Euro, Antrag zu 2): 500 Euro, Antrag zu 3): 1.000 Euro, Antrag zu 4): 500 Euro, Antrag zu 5) und 6): insgesamt 1.500 Euro)

