

**Gericht:** Thüringer Oberlandesgericht 2. Zivilsenat  
**Entscheidungsdatum:** 21.05.2025  
**Aktenzeichen:** 2 U 583/23  
**Dokumenttyp:** Urteil  
**Quelle:** 

---

Verfahrensgang

vorgehend LG Meiningen, 24. Mai 2023, 2 O 427/22, Urteil

### **Tenor**

1. Die Berufung des Klägers gegen das Urteil des Landgerichts Meiningen vom 24.05.2023, Az. 2 O 427/22, wird zurückgewiesen.
2. Der Kläger hat die Kosten des Berufungsverfahrens zu tragen.
3. Dieses Urteil und das in Ziffer 1 genannte Urteil des Landgerichts Meiningen sind ohne Sicherheitsleistung vorläufig vollstreckbar.
4. Die Revision wird nicht zugelassen.

### **Gründe**

I.

- 1 Die Parteien streiten um Ansprüche auf Schadenersatz, Unterlassung und Auskunft wegen eines Scraping-Vorfalles im Zeitraum Januar 2018 bis September 2019 bei dem von der Beklagten betriebenen Dienst "F". Der Scraping-Vorfall wurde im April 2021 bekannt.
- 2 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 zugeordnet wurde.
- 3 Nach ihren Suchbarkeits-Einstellungen konnte die Klagepartei anhand der Mobiltelefonnummer bis 25.07.2019 von der Personengruppe "alle" gefunden werden.
- 4 Die Klagepartei hat behauptet, durch das Scraping seien auch ihre Telefonnummer, ihr Nachname, ihr Geschlecht, Wohnort, Email-Adresse und Arbeitgeber erlangt und veröffentlicht worden.
- 5 Der Kläger hat im Schriftsatz v. 15.12.2022, S. 14, Bl 177 LG, seinen Vortrag dahingehend konkretisiert, dass in einer u.a. im Darknet für jedermann abrufbaren Datenbank folgende Daten des Klägers enthalten gewesen seien:
- 6 „... , ... ,S ,G... ,male, L, SCG Funktionsmodellbau, ...“

- 7        Dabei handele es sich um die Telefonnummer, die Facebook-ID, Namen, Geschlecht, Wohnort und Arbeitgeber des Klägers.
- 8        Das Landgericht hat den Kläger persönlich angehört. Im Protokoll der mündlichen Verhandlung vom 05.03.2023 (Bl. 337 LG) findet sich hierzu folgendes:
- 9                Der Kläger erklärt, dass er nach der Datenpanne bei M im wesentlich größerem Umfang Spam-Mails erhalte, als dies zuvor der Fall gewesen sei. Er fühle sich jetzt unsicher, was letztlich auch Anlass gewesen sei, die hier vorliegende Klage zu erheben.
- 10        Das Landgericht hat die Klage mit dem angefochtenen Urteil abgewiesen. Mit Beschluss vom 29.06.2023, Bl. 383 - 386 LG, ist der Tatbestand in Einzelheiten berichtigt worden, weitere Berichtigungsanträge der Beklagten sind zurückgewiesen worden. Das Landgericht hat die Klageanträge für hinreichend bestimmt gehalten, einen Verstoß der Beklagten gegen Art. 5 Abs. 1a), Art. 13 DSGVO aber verneint. Die Beklagte habe ihre Nutzer hinreichend aufgeklärt über die Zwecke der Verarbeitung von Nutzerdaten. Die Klagepartei habe im April 2018 aktualisierten Nutzungsbedingungen zugestimmt und sei in diesem Zusammenhang von der Beklagten zur Überprüfung der Privatsphäre-Einstellungen aufgefordert worden. In den Privatsphäre-Einstellungen habe sich eine klar verständliche Einstellungsmöglichkeit zur Auffindbarkeit anhand der Telefonnummer befunden. Über das allgemeine Risiko eines potenziellen Missbrauchs durch Dritte bei offen zugänglichen Daten habe die Beklagte nicht aufklären müssen. Die initiale Einstellung der Such- bzw. Auffindbarkeit für alle Nutzer diene gerade dem Sozialaspekt und damit dem Verarbeitungszweck der Plattform. Eine unbefugte oder unrechtmäßige Verarbeitung sei nicht gegeben. Hinsichtlich der tatsächlichen Feststellungen wird ergänzend auf das landgerichtliche Urteil Bezug genommen, § 540 Abs. 1 Nr. 1 ZPO.
- 11        Der Kläger hat zwischenzeitlich den Auskunftsantrag (Ziff. 4.) zurückgenommen und die Anträge zu 1., 2. und 3.a) umformuliert; im Übrigen verfolgt er mit der Berufung seine erstinstanzlichen Anträge weiter.
- 12        Der Kläger macht geltend, das Landgericht habe die Höhe des Schadensersatzes für die von ihm erlittenen immateriellen Schäden unzutreffend bewertet. 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. Der Kläger ist der Ansicht, eine Änderung der Suchbarkeitseinstellungen auf seinem Profil könne die Gefahr des Scrapings nicht beseitigen. Sein Schaden habe sich in Spam-SMS, Spam-E-Mails und Spam-Anrufen manifestiert.
- 13        Der Kläger ist weiter der Ansicht, es bestehe ein Feststellungsinteresse für den Antrag zu 2), weil nicht abgesehen werden könne, welche Dritte Zugriff auf seine Daten hatten und wie sie die Daten missbrauchen könnten. Dazu macht er geltend, durch Trickbetrügereien sei bis September 2022 ein Schaden von fast 3,3 Millionen Euro entstanden, wovon ein Betrag von 780.000,- Euro auf sog. W-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.

- 14 Die Unterlassungsanträge zu 3a) und 3b) seien zulässig. Mit diesen Anträgen verfolge er das Ziel, die Sicherheitsmaßnahmen auf der Plattform der Beklagten zu verbessern. Ohne eine solche Verbesserung sei die Änderung der eigenen Suchbarkeitseinstellungen sinnlos.
- 15 Er bestreite, dass das Auffinden des Nutzerprofils und der Daten durch Eingabe der Telefonnummer im CIT nur dann möglich gewesen sei, wenn die Suchbarkeitseinstellung auf "Everyone" eingestellt gewesen sei, weil in Nutzerkonten anderer Nutzer die Suchbarkeitseinstellung bereits im Zeitraum von 2018 bis 2019 und insbesondere vor September 2019 als maßgeblichem Zeitpunkt des Datenklaus von "Everyone" auf "Friends of Friends" umgestellt worden sei.
- 16 Sein Auskunftsanspruch sei nicht vollständig erfüllt, weil die Beklagte ihm die konkrete Identität der Scraper nicht mitgeteilt habe, obwohl sie nach der Rechtsprechung des Europäischen Gerichtshofes dazu verpflichtet sei.
- 17 Mit SS v. 31.03.2025 hat der Kläger den Antrag zu 3.a) umformuliert und hierzu angegeben, es werde lediglich das ursprüngliche Begehren des Klägers konkretisiert im Hinblick auf eine möglicherweise ansonsten fehlende Bestimmtheit.
- 18 Er meint, das Urteil des BGH v. 18.11.2024 zeige, dass die klägerischen Ansprüche bestünden, insbesondere ein Kontrollverlust bereits einen Schaden darstelle, ebenso wie die über den Kontrollverlust hinausgehenden Beeinträchtigungen, und dass es insoweit keine Bagatellgrenze gebe. Es sei indes im Rahmen der haftungsausfüllenden Kausalität ggf. schadens erhöhend zu berücksichtigen, wenn über den Kontrollverlust hinaus ein weiterer Schaden in Form von - wie hier - Kontaktversuchen Dritter vorliege. Auf den Kausalzusammenhang zwischen dem Kontrollverlust und den Kontaktversuchen könne bereits dann geschlossen werden, wenn die Betroffenen - wie hier - darlegen könnten, dass sie in zeitlicher Hinsicht vor dem Scraping kaum bis keine und nach dem Scraping bzw. der Veröffentlichung der Daten einen merklichen Anstieg an Kontaktversuchen verzeichnen könnten. Das Scraping habe sich im Jahre 2019 ereignet, die Veröffentlichung der Daten im Jahre 2021, wie auch die Beklagte selbst berichtet habe (vgl. Anlage B 10). Vorsorglich bleibe und werde abweichender Vortrag der Beklagten ausdrücklich bestritten. In diesem Zeitraum hätten auch die Kontaktversuche Dritter begonnen, die die Klägerseite seitdem beeinträchtigten.
- 19 Aus der Entscheidung des EuGH vom 04.10.2024 (EuGH, Urteil v. 04.10.2024 - C-446/21 - zur 3. Vorlagefrage) ergebe sich, dass bereits ein ungutes Gefühl einen Schaden darstellen könne. Dieser weitergehende Schaden durch die Beeinträchtigungen aufgrund der tatsächlichen missbräuchlichen Verwendung der Daten im Rahmen der konkreten Spam- und Werbekontaktierungen sowie der Betrugsversuche stelle zudem den deutlich überwiegenden Teil des Schadens der Klägerseite dar, der sich bei jedem Kontaktversuch neu realisiere und manifestiere. Die Kontakt- und Betrugsversuche würden auch, wie die Vergangenheit - d. h. der Zeitraum seit Veröffentlichung der Daten - gezeigt habe, zukünftig weiter anhalten. Dieser Schaden wiege insoweit deutlich schwerer als "lediglich" der Kontrollverlust sowie die generelle Sorge vor einem Datenmissbrauch, ohne dass ein tatsächlicher Missbrauch ggf. erfolgen würde. Entsprechend seien im Rahmen der Schadensbemessung durch das Gericht die Qualität und Quantität der Kontaktversu-

che sowie die konkreten Auswirkungen auf die Klägerseite schadens erhöhend zu berücksichtigen.

- 20 Der geltend gemachte Schadenersatz sei vor diesem Hintergrund angemessen und notwendig, um den entstandenen und zukünftig zu erwartenden bzw. noch entstehenden Schaden auszugleichen.
- 21 Der vom BGH im Urteil vom 18.11.2024 (BGH, Urteil vom 18.11.2024 - VI ZR 10/24) angegebene Betrag von 100,- € bei Kontrollverlust stelle nur einen Mindestbetrag dar. Der EuG (EuG, Urt. v. 08.01.2025 - T - 354/22) habe für den Verlust der Herrschaft (nur) über die IP-Adresse 400,- € auf der Grundlage von Art. 82 DSGVO zugesprochen. Die gescrapten Daten seien auch weiterhin für jedermann im Internet abrufbar.
- 22 Soweit die Beklagte mit Verweis auf einen Screenshot der Suchbarkeitseinstellungen der Klägerseite (vgl. S. 15 d. Schriftsatzes der Beklagten vom 13.02.2023, Bl. 252 LG) vortragen lasse, dass die Einstellung zur Suchbarkeit auf "Everyone" eingestellt gewesen sei, sei klarstellend auszuführen: Es möge sein, dass die Suchbarkeitseinstellung seit dem 25.07.2019 auf "Everyone" gesetzt gewesen sei. Die Klägerseite könne sich hierzu – schon allein aufgrund der verstrichenen Zeit – nur mit Nichtwissen erklären. Es werde jedenfalls aus anwaltlicher Vorsicht bestritten, dass die Klägerseite diese Einstellung selbst vorgenommen habe.
- 23 Für den Feststellungsantrag reiche die bloße Möglichkeit eines künftigen Schadenseintritts. Soweit der BGH den Unterlassungsantrag zu 3.a) für zu unbestimmt gehalten habe, könne vom Kläger nicht verlangt werden, den Begriff "unbefugte Dritte" weiter zu konkretisieren, soweit die Beklagte nicht gehalten sein solle, im Rahmen des Auskunftsanspruchs die Empfänger der personenbezogenen Daten zu benennen.
- 24 Der Antrag sei im Übrigen auch auslegungsfähig. Das Vollstreckungsorgan müsse nach der Rechtsprechung des BGH eine unklare Bezeichnung im Vollstreckungstitel nach allgemeinen Grundsätzen auslegen; die Auslegung obliege dabei dem zuständigen Vollstreckungsorgan (AG Bad Hersfeld, Beschluss v. 16.10.2019 – 13 M 975/19 –, DGVZ 2020, 101; Stein/Jonas/Münzberg, vor § 704 Rn. 26), wobei in erster Linie der Tenor des Urteils maßgebend sei; gegebenenfalls seien der Tatbestand und die Entscheidungsgründe ergänzend heranzuziehen (MünchKomm/ZPO-Götz, § 704 Rn. 8). Spätestens hiermit sei es dem Vollstreckungsorgan sodann möglich, zu ermitteln, welche Daten den Dritten nicht zur Verfügung gestellt werden dürften. Dies ergebe sich insbesondere aus der Inbezugnahme des Contact-Import-Tools sowie des Datenlecks bei der Beklagten im Jahre 2019: Die Beklagte habe es zu unterlassen, Dritten die bei ihr gespeicherten personenbezogenen Daten der Klägerseite über eine Software zugänglich zu machen, die allein über die Eingabe der Telefonnummer der Klägerseite eine direkte Verknüpfung der Telefonnummer mit den weiteren personenbezogenen Daten der Klägerseite ermögliche, ohne hierfür ausreichende Sicherheitsmaßnahmen nach dem aktuellen Stand der Technik – wie nunmehr beispielhaft im Antrag benannt – zu implementieren. Der nunmehr weiter konkretisierte Unterlassungsantrag dürfte jedenfalls mit Hinblick auf die Rechtsprechung des OLG Stuttgart (etwa Urteil vom 26.06.2024, Az. 4 U 172/23) hinreichend bestimmt sein.
- 25 Vorsorglich und ergänzend sei dazu auszuführen, dass sich das Datenleck nach dem übereinstimmenden Vortrag der Parteien dergestalt ereignet habe, dass die Beklagte auf ihrer Plattform eine Software implementiert habe, mit der die Kontakte aus dem Telefon-

buch der Nutzer bzw. jedenfalls deren Rufnummern ausgelesen und mit der Datenbank der Beklagten abgeglichen worden seien. Sodann sei bei einer Übereinstimmung einer Telefonnummer das Nutzerprofil unmittelbar als "Treffer" angezeigt worden, sodass eine Zuordnung des nichtöffentlichen Datums der Telefonnummer zu den öffentlich einsehbaren Daten ermöglicht worden sein. Genau eine solche erneute Verwendung solle nunmehr zu unterlassen sein.

- 26 Der Antrag zu Ziff. 3 a) sei daher jedenfalls nach der erfolgten Konkretisierung und unter Bezugnahme auf den vorstehenden, ggf. im Tatbestand aufzunehmenden Sachverhalt auslegungsfähig und hinreichend bestimmbar.
- 27 Der zeitliche Anwendungsbereich der DSGVO sei vorliegend eröffnet. Neben dem konkreten – und mit dem Vortrag der Beklagtenseite teilübereinstimmenden, mithin insoweit unstreitigen – Vortrag der Klagepartei, dass sich das Scraping im Jahr 2019 ereignet habe, habe auch die Beklagte selbst in verschiedenen (eigenen) Medien- und Presseberichten von einem Datenleck im Jahre 2019 berichtet (vgl. Anlage B 10 der Beklagten). Dass der entscheidende Zeitraum nunmehr auch den Anfang des Jahres 2018, mithin vor Inkrafttreten der DSGVO, erfasse, erscheine als reine Schutzbehauptung, um Zweifel am zeitlichen Anwendungsbereich der DSGVO begründen zu können. Vielmehr deckten sich die Vorträge beider Parteien zum Zeitraum insoweit, als dass beide Parteien vortrügen, dass das Datenleck (jedenfalls auch) das Jahr 2019 umfasste. Substanziierter Vortrag der Beklagten dazu, dass das Scraping vor Inkrafttreten der DSGVO erfolgt sei, sei nicht zu erkennen. Auch wenn das Ausgangsgericht keine ausdrücklichen Feststellungen hierzu getroffen habe, bleibe es dabei, dass – erstinstanzlich unstreitig – das Scraping der Daten der Klägerseite erst nach Inkrafttreten der DSGVO erfolgt sei. Die Klagepartei dürfe daher auch weiterhin davon ausgehen, dass das Scraping, insbesondere der Daten des Klägers, im Jahre 2019 erfolgt sei.
- 28 Hilfsweise und höchst vorsorglich werde dazu noch vorgetragen, dass dieser Umstand im Zweifel seitens der Beklagten auch durch Auswertung der entsprechenden LOG-Dateien der Beklagten nachvollzogen werden könne.
- 29 Die Beklagte habe den Scraping-Vorfall generell in ihrer Pressemitteilung vom 06.04.2021 (Anl B10, Anl.heft Bekl., LG, Bl. 22 ff.) noch selbst in das Jahr 2019 datiert. Aus dem Kontext der eigenen Pressemitteilung der Beklagten ergebe sich, dass der vorher bezeichnete Zeitraum "vor September 2019" (siehe erster Absatz des Artikels) tatsächlich nur den Zeitraum "Januar 2019 bis jedenfalls Ende August 2019" umfasste.
- 30 Weiterhin habe die Beklagte das Scraping auch im explizit die Klägerseite betreffenden Auskunftsschreiben selbst auf den Zeitraum auf "bis September 2019" datiert:
- 31 Der Artikel der Beklagten sei zudem im April 2021 veröffentlicht worden, mithin mindestens 1 Jahr und 8 Monate nach der Kenntnis der Beklagten vom Datenleck auf ihrer Plattform. Die Beklagte habe bis zu diesem Zeitpunkt – insbesondere, da sie nach eigener Aussage das Datenleck bereits im September 2019 behoben habe – ausreichend Zeit gehabt, den Sachverhalt zu ermitteln. Es sei höchst unwahrscheinlich und unüblich, dass die Beklagte weitere Ermittlungen des Sachverhaltes und insbesondere des Zeitpunktes des Scrapings auch nach der Veröffentlichung des Artikels und mehr als 1 Jahr und 8 Monate nach dem Beheben des Sicherheitslecks weiterbetrieben habe. Dafür spreche auch, dass die Beklagte vortragen lasse, dass sie "keine Rohdaten" zum Scraping-Sachverhalt

mehr vorhalte. Zum Zeitpunkt der Veröffentlichung des Artikels sei die Sachverhaltsermittlung der Beklagten mithin vollständig abgeschlossen gewesen.

- 32 Die nunmehr im Prozess angeführte Verklärung des Sachverhaltes auf einen zufälligen Zeitraum auch vor Inkrafttreten der DSGVO – hier "Zwischen Januar 2018 und September 2019" – könne daher nicht verfangen und stelle sich vorliegend als reine Schutzbehauptung heraus. Dass das Datenleck der Beklagten bereits vor Inkrafttreten der DSGVO bestanden habe, müsste diese – insbesondere im Hinblick auf Ihre eigenen Pressemitteilungen – substantiiert darlegen und beweisen. Dies gelte einerseits für den nunmehr abweichenden Zeitraum und andererseits für die Umstände, weshalb der Zeitraum nun zufällig bereits früher begonnen haben sollte. Im Übrigen wäre der Vortrag der Beklagten bezüglich des früheren Zeitpunkts des Scrapings im Hinblick auf ihre eigene Pressemitteilung *venire contra factum proprium*.
- 33 Anzumerken sei zudem, dass auch nahezu alle Gerichte im Bundesgebiet – erstinstanzlich wie zweitinstanzlich – zutreffend davon ausgingen, dass das Scraping erst nach dem Inkrafttreten der DSGVO erfolgt sei, obgleich der Vortrag der Beklagten hinsichtlich des Scrapingzeitraums in allen Verfahren – auch dem vom BGH entschiedenen – identisch sei.
- 34 Der Kläger beantragt nach Rücknahme des ursprünglichen Auskunftsantrags zu 4. und Umformulierungen der Anträge zu 1., 2. und 3.a) nunmehr,
- 1.
- 35 Die Beklagte wird verurteilt, an die Klägerseite immateriellen Schadensersatz in angemessener Höhe wegen Verstößen gegen die Datenschutzgrundverordnung vor und im Nachgang zum streitgegenständlichen Scraping-Vorfall zu zahlen, dessen Höhe in das pflichtgemäße Ermessen des Gerichts gestellt wird, mindestens insgesamt jedoch 1.000,00 EUR nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.
- 2.
- 36 Es wird festgestellt, 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 Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte, entstanden sind und/oder noch entstehen werden.
- 3.
- 37 Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 EUR, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,
- a.

- 38 eine Verarbeitung personenbezogener Daten der Klägerseite, namentlich Telefonnummer, F-ID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt und Beziehungsstatus, über die Eingabe der Telefonnummer der Klägerseite in das Kontakt-Import-Tool und die darüber hergestellte Verknüpfung der eingegebenen Telefonnummer mit weiteren öffentlichen personenbezogenen Daten des Nutzerprofils der Klägerseite zu ermöglichen, ohne dass die Beklagte zum Zeitpunkt der Verwendung des Kontakt-Import-Tools unter Eingabe der Telefonnummer Sicherheitsmaßnahmen in Form einer Implementierung von Sicherheits-CAPTCHAs und der Überprüfung massenhafter IP-Abfragen oder vergleichbaren Sicherheitsmaßnahmen vorgehalten hat,
- b.
- 39 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
- 40 Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird,
- 4.
- 41 Die Beklagte wird verurteilt, an die Klägerseite vorgerichtliche Rechtsanwaltskosten in Höhe von 887,03 EUR zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.
- 42 Die Beklagte beantragt,
- 43 die Berufung zurückzuweisen.
- 44 Die Beklagte macht geltend, das Landgericht sei zu Unrecht davon ausgegangen, dass dem Scraping-Vorfall bzw. der Nutzung ihres sozialen Netzwerkes Datenschutzverstöße zugrunde lägen. Insbesondere sei keine Verletzung von Art. 25 Abs. 2 DSGVO gegeben, weil der Nutzer die Einstellungen für seine Telefonnummer im Rahmen der Suchbarkeit unstreitig habe ändern können. Im Übrigen sei die Suchbarkeit nach der Telefonnummer für den Unternehmenszweck der Beklagten bzw. für den Zweck des von ihr betriebenen Netzwerkes erforderlich und der Nutzer sei verpflichtet, sich mit den Gepflogenheiten des sozialen Netzwerkes vertraut zu machen und sich entsprechend zu verhalten. Ihr sei auch keine Verletzung der Pflicht zur Implementierung angemessener technischer und organisatorischer Maßnahmen nach Art. 32, 24, 5 Abs. 1 DSGVO vorzuwerfen, da die getroffenen Maßnahmen im Hinblick auf das geringe Risikopotential angemessen gewesen seien.
- 45 Weiter ist die Beklagte der Ansicht, der Kläger habe keinen Schaden erlitten. Zum einen müsse ein immaterieller Schaden objektivierbar sein, was hier nicht der Fall sei und zum anderen genügten schlichte Unannehmlichkeiten im Rahmen von Art. 82 DSGVO zur Zurbilligung eines immateriellen Schadensersatzes nicht. 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 ca. 6.000 Verfahren, mit denen gleichlautende Ansprüche in Bezug auf den streitgegenständlichen Scraping-Vorfall geltend gemacht würden, stets mit identischen Formulierungen benutzt hätten. Zu dem (bestrittenen) Empfang von Spam-SMS und Spam-Anrufen gebe es weder eine konkrete Darlegung noch einen Beweisantritt. Der vom Kläger beklagte Kontrollverlust sei nicht per se ein Schaden und daneben fehle es auch an Vortrag des Klägers zu den vermeintlichen Folgen dieses Kontrollverlustes.

- 46 Im Hinblick auf den geltend gemachten Auskunftsanspruch des Klägers ist die Beklagte der Ansicht, sie habe den Anspruch durch ihr außergerichtliches Schreiben (Anlage B 16) 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.
- 47 Mit neuem SS v. 25.03.2025 macht die Beklagte geltend, der Kläger habe nicht hinreichend dargelegt, dass seine Daten im zeitlichen Anwendungsbereich der DSGVO abgerufen worden seien. Sie, die Beklagte, bestreite dies mit Nichtwissen. Es sei ihr auch nicht möglich, den genauen Zeitpunkt des Scrapings der Daten des Klägers zu bestimmen. Sie sei zum einen nicht im Besitz der Rohdaten, welche die durch das Scraping abgerufenen Daten enthielten, und zum anderen halte sie aufgrund der seit dem Scraping vergangenen Zeit keine Logdateien vor, die es ihr ermöglichen würden, genau herauszufinden, wie das Scraping abgelaufen sei oder wann die Daten des Klägers gescrapt worden seien. Sie wäre auch nach der DSGVO nicht berechtigt, derartige Logdateien vorzuhalten. Sie wisse auch weder, wer die Scraper gewesen seien, noch welches F-Konto sie ggf. verwendet hätten, um das F-Profil des Klägers einzusehen.
- 48 Soweit der Kläger die Auffassung vertrete, aus verschiedenen Medien- und Presseberichten ergebe sich, dass von einem Datenleck in 2019 berichtet worden sei, sei dies nicht näher dargelegt und nicht zutreffend. Der Newsroom-Artikel der Beklagten vom 06.04.2021 (Anl. B10) habe nur dazu dienen sollen, die Reaktion der Beklagten auf den nur wenige Tage zuvor veröffentlichten Artikel zum Scraping zu beschreiben. Die Sachlage sei noch im Entstehen begriffen gewesen und untersucht worden, so dass sich die Angaben auf Informationen beschränkt hätten, von denen die Beklagte angenommen habe, dass sie korrekt gewesen seien. In dem Artikel sei eine Reihe von Verweisen auf den Zeitraum bis 2019 enthalten ("vor September 2019"). In der Gesamtschau hätten die Zitate vermitteln sollen, dass (i) die Methode, die zur Durchführung des Scraping-Sachverhalts verwendet worden sei, bis September 2019 realisierbar gewesen sei; (ii) der Scraping-Sachverhalt bis September 2019 stattgefunden habe; und (iii) die Beklagte im Jahr 2019 Änderungen vorgenommen habe, um zu verhindern, dass diese Methode für weiteres Scraping verwendet werde. Aus dem Artikel gehe nicht hervor, dass der Scraping-Sachverhalt erst im Jahr 2019 und nicht schon zu einem früheren Zeitpunkt aufgetreten sei.
- 49 Das Risiko der Nichterweislichkeit des genauen Abrufzeitpunkt gehe zu Lasten des Klägers.

- 50 Darüber hinaus liege auch kein Vorstoß gegen die DSGVO vor. Der BGH habe einen solchen in seiner Entscheidung vom 18.11.2024 - VI ZR 10/24 - auch nicht festgestellt, sondern ihn aus prozessualen Gründen unterstellt. Die Datenverarbeitung sei vorliegend nach Art. 6 Abs. 1 S. 1b) DSGVO rechtmäßig erfolgt, da sich der zwischen den Parteien geschlossene Nutzervertrag auf die Bereitstellung der F-Plattform als soziales Netzwerk beziehe und und letzterem immanent sei, dass die einzelnen Nutzer (so auch die Klagepartei) Freunde und generell ihnen bekannte Personen finden und sich miteinander vernetzen könnten. Solche Verknüpfungen würden durch die Verwendung von Funktionen, wie der Kontakt-Importer-Funktion, hergestellt, die, wie im Hilfebereich und in der Datenrichtlinie erläutert, die Telefonnummern von Nutzern erforderten. Die Kontakt-Importer-Funktion sei deswegen ein für Nutzer der Facebook-Plattform wesentliches Tool. Die Daten seien mithin für die Erfüllung des Nutzervertrags auf Grundlage von Art. 6 Abs. 1 S. 1 lit. b) DSGVO erhoben worden.
- 51 Ein Verstoß gegen Art. 25 Abs. 2 DSGVO oder den Datenminimierungsgrundsatz liege nicht vor, weil die streitgegenständliche Datenverarbeitung zur Vertragserfüllung erforderlich gewesen sei. Darin, dass die Telefonnummer standardmäßig suchbar gewesen sei, liege keine relevante Pflichtverletzung. Die Nutzung der Telefonnummer des Nutzers im Rahmen der Suchfunktion diene dem Unternehmenszweck der Beklagten, Menschen miteinander zu verbinden, und damit auch der Durchführung des Nutzungsvertrages. Hierzu verweist die Beklagte auf einen Aufsatz von Paal, in: NJW 2025, 261, 262, wonach Anhaltspunkte dafür bestünden, "dass der Kontakt-Importer-Funktion der legitime Zweck zugrunde lag, Nutzer des sozialen Netzwerks mit Personen zu verbinden, die ihre Telefonnummer bereits kannten [...]". Die Beklagte behauptet, der von ihr bereitgestellte F-Dienst habe weltweit ca. 2,8 Milliarden Nutzer, so dass eine Suchbarkeit allein anhand des Namens in der Regel nicht ausreiche, um den Nutzer zu identifizieren, den der suchende Nutzer finden wolle. Insofern weise die Angabe der Telefonnummer eine höhere Trefferwahrscheinlichkeit auf und diene damit dem Unternehmenszweck. Um die Suchbarkeit auf der F-Plattform anhand der Telefonnummer (oder der E-Mail-Adresse) zu ändern, habe die Klagepartei jederzeit entsprechende Änderungen ihrer Suchbarkeits-Einstellungen vornehmen können.
- 52 Die hier relevante Voreinstellung der Suchbarkeit des Nutzerprofils mittels der Telefonnummer machte diese zum einen bereits nicht anderen natürlichen Personen i.S.v. Art. 25 Abs. 2 Satz 3 DSGVO "zugänglich". Ein personenbezogenes Datum werde anderen Personen nach Art. 25 Abs. 2 Satz 3 DSGVO zugänglich gemacht, wenn diese Zugriff auf dieses personenbezogene Datum und Kenntnis hiervon erlangten. Dabei nehme die Vorschrift ihrem Schutzzweck nach auf die Veröffentlichung, mithin die Sichtbarkeit, von Daten Bezug. Daran fehle es hinsichtlich der Suchbarkeit anhand der Telefonnummer. Die Voreinstellung für deren Zielgruppenauswahl, also die Sichtbarkeit der Telefonnummer auf dem Nutzerprofil, habe gerade nicht "öffentlich" gelautet. Überdies habe die vorliegend relevante Suchbarkeit anhand der Telefonnummer keinen "Zugriff" auf diese eröffnet. Denn die Nutzung der Kontakt-Importer-Funktion habe vorausgesetzt, dass die Person, die die Funktion genutzt habe, bereits im Vorfeld der Suche über die Telefonnummer verfügt habe. Nur in diesem Falle habe das Nutzerprofil anhand der Telefonnummer aufgefunden werden können. Somit sei die Telefonnummer anderen Personen – auch im Rahmen der voreingestellten Suchbarkeit anhand der Telefonnummer durch "alle" – gerade nicht i.S.v. Art. 25 Abs. 2 Satz 3 DSGVO zur Kenntnis gebracht worden. Es fehle mithin an einem "Zugänglichmachen".

- 53 Die Beklagte habe die Telefonnummer im Rahmen der Suchbarkeit anhand der Telefonnummer jedenfalls auch keiner "unbestimmten" Zahl natürlicher Personen zugänglich gemacht. Von einer "unbestimmten" Zahl natürlicher Personen könne man grundsätzlich sprechen, wenn die Öffentlichkeit Zugriff auf personenbezogene Daten erhalte. Dies sei in Bezug auf die Telefonnummer nicht der Fall gewesen. Diese sei standardmäßig gerade nicht öffentlich einsehbar gewesen. Sähe man in der "Auffindbarkeit" des Nutzerkontos anhand der Telefonnummer mittels der Kontakt-Importer-Funktion ein "Zugänglichmachen", so habe dies jedenfalls nicht einen "unbestimmten" Personenkreis, sondern nur diejenigen Personen betroffen, denen die konkrete Telefonnummer im Vorfeld der Suche bereits bekannt gewesen sei. Bei der Kenntnis der jeweiligen Telefonnummer handele es sich um ein Kriterium, mit dem sich der Personenkreis i.S.v. Art. 25 Abs. 2 Satz 3 DSGVO durchaus "bestimmen" lasse.
- 54 Zudem liege ein Kontrollverlust im hiesigen Verfahren jedenfalls nicht vor. Der BGH habe in der Entscheidung vom 18.11.2024 (BGH, a.a.O., Rz. 39) zugrunde gelegt, dass der Kläger im dortigen Fall seine Telefonnummer "stets bewusst und zielgerichtet weiter [gab] und sie nicht wahllos im Internet einer Öffentlichkeit zugänglich" gemacht habe. Die Entscheidung setze also denklogisch voraus, dass die Klagepartei die Kontrolle über ihre Daten bis zum Scraping-Sachverhalt gehabt habe. Die Beklagte bestreite, dass die Klagepartei die Kontrolle über diese Daten (erst) durch den Scraping-Sachverhalt bzw. die Veröffentlichung von durch Scraping abgerufenen Daten verloren habe bzw. vor dem Scraping die Kontrolle innegehabt habe. Bereits bei "üblichem" Umgang mit einer Telefonnummer liege eine Kontrolle nicht vor angesichts des Risikos, dass Dritte die Daten nicht datenschutzkonform behandelten (OLG Hamm, Urteil vom 05.11.2024 - 7 U 52/24 -; Urteil vom 18.12.2024 - 11 U 168/23). Der Kläger habe bereits vor der Veröffentlichung der Daten aufgrund Scrapings keine Kontrolle mehr über seine Daten gehabt.
- 55 Die weite Verbreitung von SPAM lasse einen Rückschluss auf einen Kontrollverlust durch das Scraping nicht zu. SPAM des geschilderten Inhalts sei nicht ungewöhnlich und dem nicht zuzuordnen. Bzgl. der immer öffentlichen Nutzerinformationen, auf die bestimmungsgemäß auch Dritte außerhalb der F-Plattform zugreifen könnten, oder die aufgrund der individuellen Zielgruppenauswahl öffentlich einsehbar gewesen seien, scheide ein der Beklagten zuzurechnender Kontrollverlust ohnehin aus.
- 56 Abzustellen sei insofern entgegen der Annahme des BGH (Urteil vom 18.11.2024, a.a.O., Rz. 43 f.) nicht auf Art. 6 Abs. 1 S. 1a DSGVO, sondern auf Art. 6 Abs. 1 S. 1b) DSGVO. Für den Zweck der F-Plattform, es Menschen zu ermöglichen, sich miteinander zu verbinden, sei neben der Möglichkeit, nach Nutzern anhand der Telefonnummer zu suchen, ebenso erforderlich, dass jeder jedenfalls anhand der immer öffentlichen Nutzerinformationen erkennen könne, wem das gefundene F-Profil zuzuordnen sei.
- 57 Die Rechtsprechung des EuGH stütze die Ausführungen des BGH zum Kontrollverlust als Schaden nicht. Der EuGH unterscheide (EuGH, Urteil vom 04.10.2024 - C-200/23 -, *Agentsia po vprisvaniyata*, Rz. 156) zwischen einem Umstand, der einen Schaden verursachen könne, und dem Schaden selbst. Der EuGH habe deutlich gemacht, dass der Kontrollverlust an sich kein immaterieller Schaden sei, sondern eher etwas, das "ausreichen kann, um einen" immateriellen Schaden zu verursachen. Anderes ergebe sich auch nicht aus den Erwägungsgründen 75 und 85 DSGVO.

- 58 Im vorliegenden Fall fehle es auch an einem Kausalzusammenhang zwischen unterstellter Pflichtverletzung und vermeintlichem Kontrollverlust. Die Beklagte bestreite einen solchen Kausalzusammenhang zwischen unterstellter Pflichtverletzung und vermeintlichem Kontrollverlust und auch sonstigen angeblichen negativen Folgen für den Kläger ausdrücklich. Der Kläger habe dazu keinen belastbaren Vortrag gehalten. SPAM-Nachrichten und -Anrufe seien eine Alltagserscheinung, aus der sich weder auf einen Datenschutzverstoß, noch auf einen Kontrollverlust schließen lasse.
- 59 Hinsichtlich der Schadenshöhe lasse die Entscheidung des BGH vom 18.11.2024 die Möglichkeit einer Schadenshöhe von 10,- € bis 100,- € offen. Ein eventueller Schaden wäre hier im unteren Bereich anzusetzen, zumal die Beklagte Maßnahmen zur Eindämmung von Scraping ergriffen habe, das Scraping durch Dritte verursacht worden sei und ein immaterieller Schaden allenfalls in Form eines Kontrollverlusts bzgl. solcher Daten eingetreten sein könnte, die im Einklang mit den Einstellungen des Klägers öffentlich gewesen seien.
- 60 Da der Kläger seine Telefonnummer nicht geändert habe, sei zudem von Mitverschulden des Klägers im Sinne von § 254 BGB auszugehen.
- 61 Dementsprechend scheitere auch der Feststellungsantrag, der Unterlassungsantrag zu Ziff. 3.a) sei unzulässig und der Auskunftsanspruch erfüllt.
- 62 Der Unterlassungsantrag zu Ziff. 3.b) sei unzulässig und unbegründet. Es fehle bereits am Rechtsschutzbedürfnis, da es dem Kläger unbenommen sei, die Suchbarkeitseinstellung Zielgruppenauswahl zur Telefonnummer jederzeit selbst entsprechend seinen Vorstellungen anzupassen. Die Beklagte bestreite auch weiterhin, dass während des Scraping-Zeitraums Nutzer über die Kontakt-Importer-Funktion oder über die Messenger-Kontakt-Importer-Funktion unter Bezugnahme auf eine Telefonnummer hätten identifiziert werden können, wenn die Telefonnummer ausschließlich für die Zwei-Faktor-Authentifizierung hinterlegt gewesen sei. Es sei nicht erforderlich, dass der Kläger seine Telefonnummer aus dem Nutzerkonto entferne. Der Kläger sei spätestens durch die Lektüre der Schriftsätze über die relevanten Einstellungsmöglichkeiten informiert und könne seine Telefonnummer außerdem zunächst aus dem Nutzerkonto löschen und sodann ausschließlich für die Zwei-Faktor-Authentifizierung erneut hinterlegen. Ob und für welche Zwecke die Beklagte die Telefonnummer verwende, hänge - auch nach zur Verfügung gestellten Hilfeinformationen - davon ab, wofür der Kläger diese hinterlege und welche diesbezüglichen Einstellungen er vorgenommen habe. Dies habe der BGH in der Entscheidung vom 18.11.2024 nicht in Erwägung gezogen. Zudem fehle es an der Erstbegehungs- oder Wiederholungsgefahr.
- 63 Mit neuem Schriftsatz vom 04.04.2025 rügt die Beklagte den Schadenersatzantrag des Klägers in der neuen Formulierung "Verstöße ... vor und im Nachgang zum Scraping-Vorfall" als unbestimmt und unzulässig. Damit verlange der Kläger gerade keinen Schadenersatz aufgrund des streitgegenständlichen Scraping-Vorfalles. Es gehe nicht hervor, auf welche Verstöße der Kläger abziele. Auch bei der Bestimmung der materiellen Rechtskraft ergäben sich Schwierigkeiten.
- 64 Ein Kontrollverlust sei im Übrigen weder dargelegt noch bewiesen. Personenbezogene Daten des Klägers, darunter vollständiger Name, Wohnort, Email-Adresse und Mobiltelefonnummer seien im Internet bereits (anderweit) öffentlich zugänglich über eine google-

Suche, so auf Linkln, Facebook, Youtube (vgl. Screenshots, Bl. 294 f.). Die erneute Veröffentlichung könne denkllogisch keinen Kontrollverlust begründen und wirke sich nicht wesentlich auf das für den Kläger ohnehin bestehende Risikopotenzial aus.

- 65 Der Klageänderung in Bezug auf die Unterlassung der Zugänglichmachung der Telefonnummer stimme die Beklagte nicht zu. Es handele sich dabei auch nicht um eine bloße Präzisierung. Der neue Unterlassungsantrag sei zudem unzulässig und unbegründet. "Vergleichbare Sicherheitsmaßnahmen" sei unbestimmt und würde zu erheblichen Schwierigkeiten im Vollstreckungsverfahren führen. Auch die beispielhafte Bezugnahme auf "Sicherheits-Captchas" und die "Überprüfung massenhafter IP-Abfragen" bringe keine hinreichende Konkretisierung.
- 66 Diese rein schlagwortartigen Umschreiben ließen nicht ansatzweise erkennen, welches konkrete Verhalten der Beklagte der Kläger begehre.
- 67 Zudem handele es sich um einen verkappten Leistungsantrag, da faktisch die aktive Implementierung von nicht hinreichend konkret benannten Sicherheitsmaßnahmen verlangt werde. Es fehle dem neuen Antrag auch am Rechtsschutzbedürfnis und jeglicher Wiederholungsgefahr. Die Suchbarkeit über die Telefonnummer könne vom Kläger jederzeit selbst und ohne gerichtliche Hilfe geändert werden. Da der Antrag allein auf das - längst durch die People you may know-Funktion ersetzte - Kontakt-Import-Tool (CIT) abstelle, fehle das Rechtsschutzbedürfnis. Die Beklagte verweist insoweit auch auf ihre bereits dargestellten Maßnahmen gegen Scraping.
- 68 Die von der Klagepartei im neuen Antrag genannten Datenpunkte ("[...] namentlich Telefonnummer, Facebook-ID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt und Beziehungsstatus") stimmten im Übrigen nicht mit den vom Scraping-Sachverhalt betroffenen Datenpunkten überein. Es sei auch nicht dargelegt, dass sie die im Antrag genannten Datenpunkte überhaupt alle in ihrem F Profil hinterlegt habe. Insofern sei schon nicht klar, wie es zu einer Verarbeitung dieser Datenpunkte durch die Beklagte kommen solle. Die Beklagte bestreite mit Nichtwissen, dass die durch Scraping abgerufenen Daten tatsächlich heruntergeladen worden seien.
- 69 Soweit der Kläger für das Scraping auf 2019 abstelle, handele es sich um Vortrag "ins Blaue hinein".
- 70 Der Senat hat den Kläger persönlich im Termin am 09.04.2025 angehört. Auf das Terminprotokoll vom 09.04.2025, Bl. 304 - 307 d.A., wird Bezug genommen.
- 71 Im Rahmen der auf den Schriftsatz der Beklagten vom 04.04.2025 gewährten Schriftsatzfrist hat der Kläger neuen Tatsachenvortrag der Beklagten als verspätet gerügt und - insoweit nicht nachgelassen - einen Aussetzungsantrag bis zur Entscheidung im Vorabentscheidungsverfahren des EuGH, Az. C - 273/25, gestellt. Die Aussetzung sei geboten, weil die Frage der Auslegung des Schadensbegriffs nach Art. 82 DSGVO auch für das vorliegende Verfahren entscheidungserheblich sei.

## II.

- 72 Die Berufung der Klagepartei ist unbegründet. Die Unterlassungsanträge zu Ziffer 3a) und 3b) sind unzulässig und die Klage hinsichtlich der weiteren Anträge unbegründet.

- 73 A) Klageantrag zu Ziffer 1.
- 1.
- 74 Ein Anspruch der Klagepartei auf Ersatz immateriellen Schadens aus Art. 82 Abs. 1 DSGVO besteht nicht.
- a)
- 75 Der Kläger macht mit seinem Antrag auf Zahlung eines immateriellen Schadensersatzes in Höhe von 1.000,- € nicht mehrere selbständige, auf verschiedene Datenschutzverstöße gestützte prozessuale Ansprüche alternativ geltend, sondern vielmehr einen einheitlichen Anspruch auf Ersatz eines immateriellen Schadens, der sich aus mehreren Datenschutzverstößen der Beklagten ergeben soll (BGH, Urteil vom 18.11.2024 - VI ZR 10/24 -, juris, Rz. 16). Insoweit ist die neue Formulierung im Schadenersatzantrag "wegen Verstößen gegen die DSGVO vor und im Nachgang zum streitgegenständlichen Scraping-Vorfall" geeignet, dies klarzustellen, und bezieht sich auf die aktuelle Rechtsprechung des BGH zu beziehen.
- aa)
- 76 Der Streitgegenstand wird bestimmt durch das Rechtsschutzbegehren (Antrag), in dem sich die vom Kläger in Anspruch genommene Rechtsfolge konkretisiert, und den Lebenssachverhalt (Anspruchsgrund), aus dem der Kläger die begehrte Rechtsfolge herleitet (§ 253 Abs. 2 Nr. 2 ZPO). Zum Anspruchsgrund sind alle Tatsachen zu rechnen, die bei einer natürlichen, vom Standpunkt der Parteien ausgehenden und den Sachverhalt seinem Wesen nach erfassenden Betrachtung zu dem zur Entscheidung gestellten Tatsachenkomplex gehören. Vom Streitgegenstand werden damit alle materiell-rechtlichen Ansprüche erfasst, die sich im Rahmen des gestellten Antrags aus dem zur Entscheidung unterbreiteten Lebenssachverhalt herleiten lassen (BGH, Urteil vom 18.11.2024 - VI ZR 10/24 -, juris, Rz. 17; BGH, Urteil vom 14. März 2017 - VI ZR 605/15, NJOZ 2018, 1982 Rn. 17 mwN).
- bb)
- 77 Der geltend gemachte Anspruch auf Ersatz immateriellen Schadens in angemessener Höhe, mindestens aber von 1.000,- €, den der Kläger auf den behaupteten Scraping-Vorfall und die damit in unmittelbarem Zusammenhang stehende behauptete fehlerhafte Umsetzung der Benachrichtigungs- und Auskunftspflichten durch die Beklagte stützt, bildet einen einheitlichen Streitgegenstand. Von ihm werden sämtliche mit der inkriminierten Datenverarbeitung im Zusammenhang stehenden gerügten Verstöße gegen die Datenschutz-Grundverordnung umfasst. Denn bei natürlicher Betrachtung können die Verstöße gegen die Datenschutz-Grundverordnung nicht isoliert beurteilt werden, da sie sämtlich in einem einheitlichen Geschehen wurzeln, das hinsichtlich der damit verbundenen Folgen nicht in einzelne Datenschutzverstöße aufgespalten werden kann. Auch bildet der geltend gemachte Ersatzanspruch keinen teilbaren Streitgegenstand in dem Sinne, dass auf die verschiedenen vom Kläger behaupteten Datenschutzverstöße unterschiedliche Beträge entfielen und diese einer gesonderten rechtlichen Beurteilung zugänglich wären. Nach der Rechtsprechung des Gerichtshofes der Europäischen Union kommt dem in Art. 82 Abs. 1 DSGVO niedergelegten Schadensersatzanspruch ausschließlich eine Ausgleichsfunktion zu. Er erfüllt keine Abschreckungs- oder gar Straf-

funktion, weshalb auch das Vorliegen mehrerer auf denselben Verarbeitungsvorgang bezogener Verstöße nicht zu einer Erhöhung des Schadensersatzes führt (vgl. EuGH, Urteil vom 11. April 2024 - C-741/21, NJW 2024, 1561 Rn. 59 f., 64 f. - juris). Diese Wertung würde unterlaufen, wenn unterschiedliche, aber sämtlich auf den Scraping-Vorfall bezogene Datenschutzverstöße in gesonderte Lebenssachverhalte aufgespalten würden und damit kumulativ geltend gemacht werden könnten (BGH, Urteil vom 18.11.2024 - VI ZR 10/24 -, juris, Rz. 18).

b)

78 Die Datenschutz-Grundverordnung ist räumlich (Art. 3 Abs. 1 DSGVO) und, da die bei der Beklagten gespeicherten Informationen des Klägers ohne Weiteres personenbezogene Daten des Klägers enthalten, auch sachlich (Art. 2 Abs. 1 DSGVO) anwendbar.

79 Dass der Kläger ein von dem im angefochtenen Urteil dargestellten Scraping-Vorfall betroffener Nutzer ist, ergibt sich aus dem unstreitigen Tatbestand des angegriffenen Urteils (dort S. 5).

c)

80 Der - insoweit darlegungs- und beweisbelastete - Kläger hat nicht schlüssig dargelegt, dass der zeitliche Anwendungsbereich der DSGVO eröffnet ist.

aa)

81 Gemäß Art. 99 Abs. 2 DSGVO ist die DSGVO ab dem 25.05.2018 anwendbar (auch wenn sie gem. Art. 99 Abs. 1 DSGVO bereits am 25.05.2016 in Kraft getreten ist), d.h. ab diesem Zeitpunkt können Betroffene ihre sich aus der DSGVO ergebenden Rechte ausüben (Piltz in Gola, DS-GVO, 2. Aufl., Art. 99 Rz. 7).

82 Für die Geltendmachung von Rechten, die einem Betroffenen auf Basis der DSGVO zustehen, differenziert der EuGH (vgl. EuGH Urteil vom 22.06.2023 - C-579/21, NZA 2023, 889,

83 beck-online, Rz. 32) danach, ob materielle Rechte oder Verfahrensrechte geltend gemacht werden. Bei Verfahrensvorschriften ist im Allgemeinen davon auszugehen, dass sie ab dem 25.05.2018 Anwendung finden, so dass z.B. ein Auskunftersuchen nach Art. 15 DSGVO ab dem 25.05.2018 möglich ist, selbst wenn es sich auf Verarbeitungsvorgänge bezieht, die vor dem 25.05.2018 ausgeführt wurden (EuGH, a.a.O.).

84 Bei materiellen Rechtspositionen ist das neue Recht nicht auf unter dem alten Recht entstandene und endgültig erworbene Rechtspositionen anwendbar, findet aber auf deren künftige Wirkungen sowie auf neue Rechtspositionen Anwendung. Etwas anderes gilt nur - und vorbehaltlich des Verbots der Rückwirkung von Rechtsakten -, wenn zusammen mit der Neuregelung besondere Vorschriften getroffen werden, die speziell die Voraussetzungen für ihre zeitliche Geltung regeln (EuGH, Urteil vom 15.06.2021 - C-645/19 -, juris, Rz. 100).

85 Auch wenn der EuGH in diesem Zusammenhang z.T. allgemein und nicht zwischen Rechtskraft und Anwendbarkeit differenzierend davon spricht, dass materiell-rechtliche Vorschriften in der Regel auf vor ihrem Inkrafttreten entstandene und endgültig erworbene Rechtspositionen keine Anwendung finden (EuGH, C-579/21, a.a.O. Rz. 32;

C-645/19, a.a.O., Rz. 100), ergibt sich aus den Entscheidungen, dass der EuGH bei einem Abweichen des Anwendungszeitraums vom Zeitpunkt des Inkrafttretens jeweils auf die zeitliche Anwendbarkeit abstellt. So differenziert er in der Entscheidung vom 15.06.2021 (EuGH, Urteil vom 15.06.2021 - C-645/19 -, juris, Rz. 101, 103 f.) nach dem Stichtag 25.05.2018 für die Geltung der DSGVO und benennt auch in der Entscheidung vom 22.06.2023 (EuGH, Urteil vom 22.06.2023 - C-579/21 - a.a.O., Rz. 35 f.) als zeitliche Abgrenzung "ab der Anwendung" der DSGVO.

- 86 Mag der Betroffene dementsprechend also nach Inkrafttreten der DSGVO gemäß Art. 15 Abs. 1 DSGVO Auskunft über Verarbeitungsvorgänge verlangen können, die vor dem 25.05.2018 ausgeführt wurden (so EuGH, a.a.O.), weil das Auskunftsrecht als Verfahrensrecht nicht die Rechtmäßigkeit der Verarbeitung betrifft, können materielle Rechtspositionen aus der DSGVO grds. erst für die Zeit ab 25.05.2018 hergeleitet werden.
- 87 Wortlaut, Zielsetzung oder Aufbau der DSGVO bietet dabei keine Grundlage für eine ausnahmsweise "Vorverlagerung" der Begründung materieller Rechtspositionen wie Schadenersatzansprüche auf den Zeitraum vor Anwendbarkeit der DSGVO. Davon geht auch der BGH (BGH, Urteil v. 18.11.2024 - VI ZR 10/24 -, juris, Rz. 19) ersichtlich nicht aus. Auch ein Verstoß gegen Normen des (bis zur Geltung der DSGVO geltenden) BDSG 2016 würde als solcher keine Verpflichtung zum Ersatz immaterieller Schäden nach DSGVO begründen (LAG Baden-Württemberg, Urteil vom 25.02.2021 - 17 Sa 37/20 - (n.r.), beck-online, Rz. 67). Dies greift auch das BAG im Vorlagebeschluss vom 22.09.2022 - 8 AZR 209/21 (A), Rz. 20, modifiziert mit Beschluss vom 25.04.2024, 8 AZR 209/21 (B) (jeweils unter <https://www.bundesarbeitsgericht.de>) nicht an, sondern geht nur im konkreten Fall davon aus, dass sich aus Handeln vor Geltung der DSGVO eine fortbestehende Verantwortlichkeit für persönliche Daten des Klägers und eine Pflichtenlage auch im Sinne der DSGVO für die Zeit ab dem 25.05.2018 ergibt, die Ansprüche begründen kann (bzgl. der Vorlagefragen: EuGH, Urteil vom 19.12.2024 - C-65/233 -, ECLI:EU:C:2024:1051 unter <https://curia.europa.eu>).
- bb)
- 88 In Bezug auf das hier in Rede stehende Scraping ist für die zeitliche Anwendbarkeit der DSGVO nicht maßgeblich der Zeitpunkt der Registrierung eines Nutzerkontos im sozialen Netzwerk der Beklagten, sondern der Zeitpunkt des Scraping-Vorfalles (BGH, Urteil vom 18.11.2024 - VI ZR 10/24 -, juris, Rz. 19). Ebenfalls nicht maßgeblich ist dementsprechend der Zeitpunkt der Veröffentlichung von Nutzerdaten im Jahr 2021.
- cc)
- 89 Die zeitliche Anwendbarkeit der DSGVO ist im vorliegenden Fall nicht gegeben.
- 90 Der Kläger hat erstinstanzlich Verstöße der Beklagten gegen Datenschutzbestimmungen, Scraping bzw. das Ausnutzen von Sicherheitslücken im Jahr 2019 behauptet und entsprechend auch im Feststellungsantrag (S. 2, Bl. 4 LG) von Zugriffen Dritter gesprochen, die nach Aussage der Beklagten im Jahr 2019 erfolgt seien. Die Beklagte hat demgegenüber seit der Klageerwidern als Zeitraum des Datenscrapings durchgängig den Zeitraum Januar 2018 bis September 2019 benannt (Klageerwidern v. 01.12.2022, S. 11, Bl. 78 LG). Dementsprechend hat das Landgericht in seinem Urteil den Zeitraum des Scrapings mit Januar 2018 bis September 2019 aufgenommen. Dies entspricht auch dem Vortrag des Klägers in der Berufung (Berufungsbegründung, S. 5, Bl. 13 d.A.). In der

Argumentation der Beklagten (Klageerwiderung, Seite 42, Bl. 109 LG), ein Vermögensschaden sei fernliegend, zumal nach dem Vortrag des Klägers der Zugriff bereits 2019 erfolgt sei, die Daten aber bislang nicht zu kriminellen Zwecken genutzt worden seien, liegt kein Unstreitigstellen des Datenzugriffs im Jahr 2019, da die Beklagte in der Klageerwiderung selbst von einem anderen Zeitraum ausgeht.

- 91 Eine Partei darf auch nur vermutete Tatsachen vortragen und unter Beweis stellen, wenn sie darüber keine genaueren Kenntnisse hat oder haben kann, sofern sie die Tatsachen nach Lage der Dinge für wahrscheinlich hält (BGH NJW 2021, 1759 [1761 Rn. 18]; BGHZ 216, 245 [257 Rn. 33]). Unzulässig wird ein solches Vorgehen erst dort, wo die Partei ohne greifbare Anhaltspunkte für das Vorliegen eines bestimmten Sachverhalts willkürlich Behauptungen "aufs Geratewohl" oder "ins Blaue hinein" aufstellt. Bei der Annahme von Willkür in diesem Sinne ist Zurückhaltung geboten; in der Regel wird sie nur bei Fehlen jeglicher tatsächlicher Anhaltspunkte gerechtfertigt werden können (BGH NJW-RR 2015, 829 [830 Rn. 13]). Erforderlich ist insgesamt, dass klargestellt wird, welche Behauptungen gelten sollen. Ausgehend davon ist der Vortrag der Klagepartei zum Zeitpunkt des Abgriffs ihrer Daten als schlüssig anzusehen, da zum Zeitpunkt der letzten mündlichen Verhandlung klargestellt war, dass von einem Datenabgriff im Jahr 2019 und damit nach Inkrafttreten der DSGVO ausgegangen werden soll. Der als schlüssig zu behandelnde Vortrag führt für sich allein gesehen jedoch nicht dazu, dass von einem Datenabgriff während der zeitlichen Geltung der DSGVO auszugehen ist, denn die Klagepartei trägt für diesen Umstand die Beweislast und ist – nach dem nun gehaltenen sekundären Vortrag der Beklagten – beweisfällig. Der Vortrag der Beklagten ist auch nicht präkludiert nach §§ 529, 531 ZPO, da die Frage der zeitlichen Anwendbarkeit der DSGVO in erster Instanz nicht thematisiert wurde, geschweige denn die Frage von diesbezüglichen Darlegungslasten, und das Landgericht insoweit auch keine Hinweise erteilt hat.
- 92 Grundsätzlich trifft die Klagepartei die Darlegungs- und Beweislast dafür, dass der zeitliche Anwendungsbereich der DSGVO eröffnet ist. Dieser Grundsatz bedarf der Einschränkung, da die Klagepartei als primär darlegungsbelastete Partei außerhalb des maßgeblichen Geschehensablaufs steht und keine Kenntnisse von den maßgeblichen Tatsachen besitzt und den Sachverhalt von sich aus nicht ermitteln kann, während dem Prozessgegner die erforderliche tatsächliche Aufklärung ohne weiteres möglich und auch zuzumuten ist. Dabei obliegt es dem Bestreitenden im Rahmen der sekundären Darlegungslast auch, zumutbare Nachforschungen zu unternehmen (BGH, Urteil vom 05.10.2023, III ZR 216/22 Rn. 31; BGH, Urteil vom 04.02.2021, III ZR 7/20 Rn. 19, NJW 2021, 1759; BGH BeckRS 2020, 36575 Rn. 26; BGH NJW 2016, 3244 [3245 Rn. 18]; vergleiche auch BGH NJW 1997, 128 [129]; BGH NJW 1996, 315 [317]). Die "Last" besteht in der Pflicht, das pauschale Vorbringen des darlegungsbelasteten Gegners (ausnahmsweise) mit weiteren Einzelheiten bestreiten zu müssen. Es ist also am Gegner – hier also der Beklagten –, Einzelheiten zu der Behauptung des Datenabgriffs im Jahr 2019 darzustellen und sich zumindest substantiiert zu den Behauptungen zu äußern. Der Umfang der sekundären Darlegungslast richtet sich nach den Umständen des Einzelfalls. Die Darlegungen müssen so konkret sein, dass der beweisbelasteten Partei eine Widerlegung möglich ist (BGH, Urteil vom 04.02.2021, III ZR 7/20 Rn. 19, NJW 2021, 1759).
- 93 Die Beklagte hat der sie treffenden sekundären Darlegungslast jedenfalls mit dem Vorbringen im Schriftsatz vom 25.03.2025 (S. 5, Bl. 232 d.A.) genügt. Die Klagepartei bleibt danach für den Zeitpunkt des Abgriffs beweisfällig.

- 94 So ergibt sich aus der Pressemitteilung der Beklagten vom 06.04.2021 nicht, dass der Abgriff nur im Jahr 2019 erfolgt sein kann. Darin wird mitgeteilt, dass "böswillige Akteure die Daten vor September 2019 von der Plattform gescrapt" hätten, in dem sie "den Kontakt-Importer vor September 2019 verwendet" hätten und "das Problem im Jahr 2019 behoben" worden sei. Ein Abgriff "vor September 2019" - von dem zweimal die Rede ist - kann aber bereits im Jahr 2018 geschehen sein, wodurch diese Formulierung hinsichtlich des genauen Zeitpunkts offenbleibt.
- 95 Auch kann der Beklagten nicht verwehrt werden (insbesondere nach dem Gewinn weiterer tatsächlicher Erkenntnisse) in einem Prozess einen anderen (ergänzten, geänderten, korrigierten) Vortrag zu halten, zumal wenn dies nachvollziehbar damit begründet wird, dass sich der Sachverhalt zum Zeitpunkt der Erstellung der Pressemitteilung noch in der Aufklärung befunden hat und es damals darum gegangen sei, auf verschiedene Medienberichte zeitnah zu reagieren. Die Behauptung, bei Veröffentlichung des Artikels im April 2021 sei die "Sachverhaltsermittlung" der Beklagten bereits abgeschlossen gewesen, weil die Beklagte dafür seit 2019 Zeit gehabt habe, lässt keinen hinreichenden Bezug zur Frage der Ermittlung des Zeitpunkts des Scrapings bestimmter Datensätze, hier derjenigen des Klägers, erkennen, zumal die Beklagte vorgetragen hat, sie habe bereits seit März 2018 verschiedene Anstrengungen unternommen, auf Scraping zu reagieren und dieses zu verhindern.
- 96 Es kann auch nicht von einem Dauerdelikt ausgegangen werden, denn der Abgriff von Daten zu einem bestimmten Profil von dem CIT kann bei einem Treffer bezüglich der Telefonnummer nur zu einem ganz bestimmten Zeitpunkt erfolgen, nämlich dann, wenn der konkrete Datensatz aus dem Tool abgerufen wird. Wurde der Datensatz vor der zeitlichen Geltung des DSGVO abgegriffen, können mögliche Verstöße gegen die Vorschriften der DSGVO dafür nicht ursächlich sein.
- 97 Die Beklagte hat mitgeteilt, dass sie nicht im Besitz der Rohdaten sei, welche die durch das Scraping abgerufenen Daten enthielten und aufgrund der seit dem Sachverhalt vergangenen Zeit würden auch keine Log-Dateien oder Ähnliches vorgehalten, die ihr die Aufklärung ermöglichen könnten, wie der Scraping-Sachverhalt genau abgelaufen sei und wann die Daten der jeweiligen Klagepartei abgegriffen worden seien. Nach den Vorgaben der DSGVO sei sie auch gar nicht berechtigt, derartige Log-Dateien vorzuhalten. Ihr sei daher auch nicht bekannt, wer die Scraper gewesen seien und auch nicht, welches F-Konto verwendet wurde, um die F-Profile der Nutzer einzusehen.
- 98 Damit hat die Beklagte der sie treffenden sekundären Darlegungslast genügt und das ihrerseits Erforderliche getan, um den Vortrag der Klagepartei qualifiziert zu bestreiten.
- 99 Soweit der Kläger nunmehr im Schriftsatz vom 31.03.2025 darauf verweist, aus den LOG-Dateien lasse sich der Zeitpunkt des Scrapings ablesen, kann dies dahinstehen, da die Beklagte vorgetragen hat, dass sie über die LOG-Dateien nicht mehr verfügt.
- 100 Konkrete Anhaltspunkte dafür, dass die Daten des Klägers tatsächlich nach dem 24.05.2018 abgegriffen wurden, legt der Kläger nicht dar und sind auch nicht ersichtlich.
- 101 Der Kläger meint, die Darlegungs- und Beweislast für die zeitliche Nichtanwendbarkeit der DSGVO obliege der Beklagten. Über eine mögliche sekundäre Darlegungslast hinaus, die vorliegend aber zu verneinen ist, ist dem nicht zu folgen.

- 102 Verschiedentlich hat die Rechtsprechung den Grundsatz, dass der Gläubiger die Pflichtverletzung zu beweisen hat, aufgeweicht. Ausschlaggebend dafür ist häufig, dass die Umstände, mittels derer der Gläubiger die Pflichtverletzung beweisen müsste, ganz oder teilweise in der Sphäre des Schuldners liegen. Dem Gläubiger wird in diesen Konstellationen die Beweislast nicht vollständig genommen, sondern nur insoweit, wie er unangemessen belastet wäre (Erman - Ulber, BGB, 17. Aufl., 09/2023, § 280 BGB, Rz. 122). Vorliegend geht es nicht um die Pflichtverletzung, sondern um den zeitlichen Anwendungsbereich der DSGVO. Über eine mögliche sekundäre Darlegungslast hinaus der Beklagten Beweislasten aufzuerlegen, besteht keine Veranlassung, zumal die Beklagte nach Datenschutzvorschriften gehalten ist, nicht benötigte Daten zu löschen, die benötigten Daten damit in ihrer Sphäre bei datenschutzkonformem Verhalten gar nicht mehr vorhanden sind und sein sollen.
- 103 Auch ein Verstoß gegen die Grundsätze von Treu und Glauben (§ 242 BGB) wegen widersprüchlichen Verhaltens (*venire contra factum proprium*) ergibt sich noch nicht daraus, dass die Beklagte, die seit der Klageerwiderung den Zeitraum des Scrapings mit Januar 2018 bis September 2019 benannt hat, sich auf die zeitliche Unanwendbarkeit der DSGVO beruft. Eine dem widersprechende eindeutige und abschließende zeitliche Zuordnung im Jahr 2019 in der Anlage B16 oder ansonsten im vorgerichtlichen Bereich ist nicht ersichtlich. Insbesondere ist die Aussage "im Zeitraum bis September 2019" (Anl. B16, S. 2, Bl. 46 Anl.h. Bekl., LG) nicht identisch mit "zwischen Januar und September 2019".
- 104 Die Unaufklärbarkeit der zeitlichen Einordnung des Scraping-Falls geht zu Lasten des Klägers und führt dazu, dass nicht hinreichend sicher festgestellt werden kann, dass der konkrete Abgriff der Daten nach dem Inkrafttreten der DSGVO zum 25.05.2018 erfolgt ist.
- 105 Da die DSGVO nicht anwendbar ist, kommen nur noch Schadenersatzansprüche nach nationalem Recht, sei es aufgrund § 7 BDSG 2016 oder aus nationalem Vertrags- oder Deliktsrecht in Betracht.
- 2.
- 106 Der bis zur Anwendbarkeit des Art. 82 DSGVO geltende § 7 BDSG sah einen Schadenersatzanspruch vor, wenn eine verantwortliche Stelle durch eine nach Datenschutzvorschriften unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten des Betroffenen einen Schaden zufügt. Allerdings war dort ein immaterieller Schaden nicht genannt, anders als im Schadenersatzanspruch gegenüber öffentlichen Stellen nach § 8 Abs. 2 BDSG, demzufolge bei schwerer Persönlichkeitsverletzung auch ein Nichtvermögensschaden in Geld zu ersetzen war. Ein Anspruch auf Ersatz immaterieller Schäden aus § 7 BDSG ist dementsprechend - und auch gemäß § 253 Abs. 1 BGB - zu verneinen (Auernhammer - Eßer, DSGVO/BDSG, 5. Aufl., 2017, § 7 BDSG, Rz. 24; Plath - Becker, BDSG/DSGVO, 2. Aufl., 2016, § 7 BDSG, Rz. 14; OLG Zweibrücken, Urteil vom 21.02.2013 - 6 U 21/12 -, juris, Rz. 69, aber letztlich offengelassen; OLG München, Beschluss vom 13.02.2025 - 24 U 3020/24 -, juris, Rz. 28).
- 3.

- 107 Ebenfalls besteht kein Schadenersatzanspruch aus § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1 und Art. 1 Abs. 1 GG wegen Verletzung des allgemeinen Persönlichkeitsrechts als eines anderen gleichwertigen Rechtsguts.
- 108 Dies setzt eine schwerwiegende Beeinträchtigung des allgemeinen Persönlichkeitsrechts voraus, bei der die Beeinträchtigung nach Art der Verletzung nicht in anderer Weise (Genugtuung durch Unterlassen, Gegendarstellung oder Widerruf) befriedigend ausgeglichen werden kann; der Anspruch beinhaltet Genugtuungs- und Präventionsfunktion (Grüneberg - Prau, BGB, 85. Aufl., 2025, § 823 Rz. 111, Erman - Klass, BGB, 17. Aufl., 2023, Anh. zu § 12 Rz. 315 ff.). Der Anspruch ergibt sich dann unmittelbar aus § 823 I BGB i.V.m. GG (Grüneberg - Grüneberg, BGB, 84. Aufl., 2025, § 253 Rz. 10).
- 109 Voraussetzungen für einen Anspruch auf Geldentschädigung sind zum einen eine schwere Persönlichkeitsrechtsverletzung, Verschulden und jedenfalls Subsidiarität (BGH, Urteil vom 17.12.2013 - VI ZR 211/12 -, "Sächsische Korruptionsaffäre", juris, Rz. 38; BGH, Urteil vom 01.12.1981 - VI ZR 200/80 -, "Rudimente der Fäulnis", juris, Rz. 33). Ob eine schwere Persönlichkeitsrechtsverletzung zu bejahen ist, kann dabei nur aufgrund der gesamten Umstände des Einzelfalles (BGH 24.11.2009 - VI ZR 219/08, AfP 2010, 75, 76 - Esra) beurteilt werden, wobei besonders die Art sowie die Schwere der zugefügten Beeinträchtigung, und der Grad des Verschuldens, aber auch Anlass und Beweggrund des Handelns zu berücksichtigen sind (Erman - Klass, a.a.O., Rz. 313).
- 110 Die Zubilligung einer Geldentschädigung unter den genannten Voraussetzungen findet ihre sachliche Berechtigung in dem Gedanken, dass das Persönlichkeitsrecht gegenüber schwerwiegenden Beeinträchtigungen anderenfalls ohne ausreichenden Schutz bliebe mit der Folge, dass der Rechtsschutz der Persönlichkeit verkümmern würde (BGH Urt. v. 12.3.2024 - VI ZR 1370/20, BeckRS 2024, 14074 Rn. 70 m.w.N.; vgl. auch BGH Urt. v. 5.10.2004 - VI ZR 255/03, NJW 2005, 215, 216 m.w.N.).
- 111 Nach diesen Grundsätzen erscheint die Zahlung einer Geldentschädigung nicht erforderlich (so auch OLG Hamm, Urteil vom 28.11.2024 - 7 U 52/24 -, juris, Rz. 60; OLG Hamm, Urt. v. 15.8.2023 - 7 U 19/23, GRUR-RS 2023, 22505 = juris Rn. 204; OLG München, Beschluss v. 13.02.2025 - 24 U 3020/24e, juris, Rz. 27).
- 112 Offenbleiben kann in diesem Zusammenhang, ob der Kontrollverlust an den im vorliegenden Fall in Rede stehenden Daten überhaupt eine Verletzung des allgemeinen Persönlichkeitsrechts des Klägers darstellt. Jedenfalls wiegt die Beeinträchtigung nicht hinreichend schwer. Es kann dahinstehen, dass der Kläger bzgl. der in der Anhörung genannten Email-Adresse Scraping nicht substantiiert dargelegt hat, da in der vom Kläger zitierten Veröffentlichung die
- 113 Email-Adresse gerade nicht enthalten war.
- 114 Die Daten betreffen sämtlich nicht die Privat- oder Intimsphäre des Klägers, sondern lediglich die Sozialsphäre. Das gilt auch für die Angabe zum Geschlecht, das nach immer noch gängiger Anschauung in Deutschland – was sich etwa durch die Ableitbarkeit aus dem Vornamen oder durch die Anrede mit "Frau" oder "Herr" ausdrückt – der Sozialsphäre zuzuordnen ist. Zur Sozialsphäre gehört dabei auch die berufliche Tätigkeit, d.h. ein Bereich, in dem sich die persönliche Entfaltung des Betroffenen von vornherein im Kontakt mit der Umwelt vollzieht (BGH, Urteil vom 20.02.2018 - VI ZR 30/17 -, beck-online, Rz. 14). Die Telefonnummer ist (ebenso wie die Email-Adresse) ein Datum, das auf Kom-

munikation und deshalb auf Weitergabe angelegt ist. Die Intimsphäre als unantastbarer Kernbereich höchstpersönlicher, privater Lebensgestaltung oder Daten aus dem innersten Kern der Lebensführung wie medizinische Daten, persönliche Kommunikation, eigenes Bild o.ä. sind nicht betroffen.

- 115 Hinzu kommt, dass F unstreitig auf Kommunikation unter Nutzern angelegt und Vernetzung und Kommunikation gerade das Ziel der Nutzung sind. In diesem Zusammenhang hat die Beklagte unbestritten vorgetragen, dass Grunddaten wie Name, Geschlecht und Nutzer-ID immer öffentlich und auch für Dritte einsehbar sind. Dies gehört dementsprechend zum Grundprinzip der (freiwilligen) F-Nutzung.
- 116 Die Beklagte hat die Daten nicht vorsätzlich weitergegeben an Dritte zu anderen als den Kommunikationszwecken von F.
- 117 In dieser Gesamtkonstellation ist ein derart schwerwiegender Verstoß zu verneinen, geschweige denn eine Geldzahlung erforderlich.
- 4.
- 118 Ein Anspruch auf Schadensersatz folgt auch nicht aus § 280 Abs. 1, § 241 Abs. 2 BGB im Hinblick auf den zwischen den Parteien bestehenden Nutzungsvertrag (vgl. zum Nutzungsvertrag auch BGH Urt. v. 18.11.2024 – VI ZR 10/24, Rn. 83 m.w.N., Rn. 50).
- 119 Unabhängig davon, ob ein immaterieller Schaden des Klägers überhaupt vorliegt, fehlt es auch im Rahmen von § 253 Abs. 2 BGB an der erforderlichen schweren Verletzung des allgemeinen Persönlichkeitsrechts (so auch OLG Hamm, – 7 U 52/24 –, juris, Rz. 60). Auf die Ausführungen zu 3. wird Bezug genommen.
- 120 B) Feststellungsantrag zu Ziff. 2.
- 1.
- 121 Der Feststellungsantrag ist zulässig, da er dahingehend zu verstehen ist, dass er sich auf künftige materielle sowie auf künftige derzeit noch nicht vorhersehbare immaterielle Schäden bezieht (vgl. BGH, Urteil vom 18.11.2024 – VI ZR 10/24 –, juris, Rz. 47). Der Kläger hat den Feststellungsantrag inzwischen in der Formulierung entsprechend der aktuellen BGH-Rechtsprechung konkretisiert.
- a)
- 122 Die bloße Möglichkeit des künftigen Eintritts der geltend gemachten Schäden ist Maßstab für die Annahme eines Feststellungsinteresses; eine darüberhinausgehende hinreichende Schadenswahrscheinlichkeit ist nicht erforderlich. Die Möglichkeit künftiger Schäden reicht hier aus, weil es nicht um reine Vermögensschäden geht, sondern um Schäden, die aus der vom Kläger behaupteten Verletzung seines Rechts auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG, mithin seines allgemeinen Persönlichkeitsrechts als einem sonstigen absolut geschützten Rechtsgut im Sinne von § 823 Abs. 1 BGB, resultieren (BGH, Urteil vom 18.11.2024 – VI ZR 10/24 –, juris, Rz. 48; BGH, Urteile vom 5. Oktober 2021 – VI ZR 136/20, VersR 2022, 1184 Rn. 28; vom 29. Juni 2021 – VI ZR 10/18, ZUM 2022, 311 Rn. 30).
- 123 Auch die primär als Anspruchsgrundlage herangezogene Vorschrift des Art. 82 DSGVO hat jedenfalls dann, wenn – wie hier – mit einem möglichen Verstoß gegen Art. 5 DSGVO

auch eine unrechtmäßige Datenverarbeitung gerügt wird, eine Verletzung des Rechts auf Schutz der personenbezogenen Daten gemäß Art. 8 GRCh zum Inhalt (vgl. Art. 1 Abs. 2 DSGVO). Dabei kann die Möglichkeit ersatzpflichtiger künftiger Schäden ohne Weiteres zu bejahen sein, wenn ein deliktsrechtlich geschütztes absolutes Rechtsgut verletzt wurde und bereits ein Schaden eingetreten ist (BGH, Urteil vom 18.11.2024 - VI ZR 10/24 -, juris, Rz. 48; BGH, Urteil vom 30. Juli 2020 - VI ZR 397/19, NJW 2020, 2806 Rn. 29; vgl. eingehend Senat, Urteil vom 17. Oktober 2017 - VI ZR 423/16, BGHZ 216, 149 Rn. 49 mwN).

b)

- 124 Der Feststellungsantrag ist unbegründet, da ein Schadenersatzanspruch weder nach DSGVO, noch aus einem anderen Rechtsgrund gegeben ist (vgl. die Ausführungen zu A)).
- 125 C) Unterlassungsanträge zu Ziffer 3.a) und Ziffer 3.b)
- 126 Die Unterlassungsanträge sind unzulässig, da jedenfalls das erforderliche Rechtsschutzbedürfnis des Klägers jeweils nicht besteht.
- 127 Eine Klage ist als unzulässig abzuweisen, wenn für sie kein Rechtsschutzbedürfnis besteht. Das Erfordernis des Rechtsschutzbedürfnisses soll verhindern, dass Rechtsstreitigkeiten in das Stadium der Begründetheitsprüfung gelangen, für die eine solche Prüfung nicht erforderlich ist. Grundsätzlich haben Rechtssuchende allerdings einen Anspruch darauf, dass die staatlichen Gerichte ihr Anliegen sachlich prüfen und darüber entscheiden. Das Rechtsschutzbedürfnis fehlt jedoch, wenn eine Klage oder ein Antrag objektiv schlechthin sinnlos ist, wenn also der Kläger oder Antragsteller unter keinen Umständen mit seinem prozessualen Begehren irgendeinen schutzwürdigen Vorteil erlangen kann (BGH, Urteil vom 29. September 2022 - I ZR 180/21, ZIP 2022, 2460 Rn. 10 mwN; vgl. bereits Senat, Urteil vom 14. März 1978 - I ZR 68/76, NJW 1978, 2031, 2032 [unter II. 2. a])).
- 128 Dies ist etwa dann der Fall, wenn ein einfacherer oder billigerer Weg zur Erreichung des Rechtsschutzziels besteht oder der Antragsteller kein berechtigtes Interesse an der beantragten Entscheidung hat. Dafür gelten allerdings strenge Maßstäbe. Das Rechtsschutzbedürfnis fehlt (oder entfällt) nur dann, wenn das Betreiben des Verfahrens eindeutig zweckwidrig ist und sich als Missbrauch der Rechtspflege darstellt (Senat, Beschluss vom 24. September 2019 - VI ZB 39/18, BGHZ 223, 168 Rn. 28; Urteil vom 14. März 1978 - VI ZR 68/76, NJW 1978, 2031, 2032 [unter II. 2. a])).
- 129 Beide Unterlassungsanträge knüpfen an die Verwendung des Kontakt-Importer-Tools (CIT) durch die Beklagte.
- 130 Eine erneute Verwendung der Telefonnummer im CIT (Kontakt-Importer-Tool) scheidet jedoch bereits deshalb aus, weil dieses Tool in dieser Form unstreitig nicht mehr existiert. Eine Funktion auf der Plattform der Klagepartei, die eine eindeutige Zuordnung einer Telefonnummer zu einem Profil ermöglichen würde, gibt es nicht mehr. Es ist zwar noch möglich, Telefonnummern und Kontaktlisten hochzuladen. Der Nutzer erhält mit dieser Funktion jedoch als Ergebnis nur eine Liste der Profile von Personen, die er, auch aufgrund anderer Zuordnungskriterien (zum Beispiel Namen) kennen könnte (people-you-may-know-Funktion) (unstreitiger TB des Urteils, S. 5, Bl. 345 LG). Von weiteren Missbrauchsfällen nach 2019 und dem Bekanntwerden der Scraping-Vorfälle im Jahr 2021 wurde nichts berichtet. Solches trägt auch der Kläger nicht vor. Nachdem die Be-

klagte die Veränderungen der Nutzungsmöglichkeiten gerade deswegen vorgenommen hat, um einen Missbrauch, wie in der Vergangenheit durch die Scraping-Vorfälle geschehen, zu vermeiden und außerdem von der irischen Datenschutzbehörde wegen der hier gegenständlichen Scraping-Vorfälle mit einer empfindlichen Strafe belegt wurde (mag diese nun rechtskräftig sein oder nicht), ist auch nicht ernsthaft damit zu rechnen, dass die Beklagte wieder ein der Kontakt-Importer-Funktion entsprechendes Tool einführen wird (vgl. OLG München, Beschluss vom 13.02.2025 - 24 U 3020/24 e -, juris, Rz. 31 ff.; siehe zum Ganzen und den durchgeführten technischen Änderungen auch: OLG Dresden, 10.12.2024, 4 U 808/24 Rn. 45 ff.).

- 131 Es kann dahinstehen, ob und wieweit der Kläger auch leicht selbst die Möglichkeit hat, Abhilfe zu schaffen derart, dass eine unrechtmäßige Verarbeitung seiner Telefonnummer jenseits der 2-Faktor-Authentifizierung verhindert wird (vgl. dazu OLG München, Beschluss vom 13.02.2025 - 24 U 3020/24 e -, juris, Rz. 37; schon vor der BGH-Entscheidung OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23 - juris, Rz. 237).
- 132 Aus nämlichen Gründen kommt auch ein Unterlassungsanspruch aus §§ 1004, 823 I BGB oder anderen Rechtsgründen nicht in Betracht (vgl. auch OLG Dresden, Urteil vom 10.12.2024 - 4 U 808/24 -, juris, unter B.3.b))
- 133 D) Klageantrag zu Ziffer 4.
- 134 Die Beklagte war zum Zeitpunkt der Beauftragung eines Anwalts nicht in Verzug. In Betracht kommt insofern nur eine Erstattung von Anwaltskosten als Teil eines materiellen Schadenersatzanspruchs nach §§ 249 ff. BGB. Ein derartiger materieller Schadenersatzanspruch besteht jedoch - wie dargelegt - nicht.
- E)
- 135 Für eine Aussetzung des Verfahrens analog § 148 ZPO besteht keine Veranlassung. Im vorliegenden Fall ist der zeitliche Anwendungsbereich der DSGVO für Schadenersatzforderungen nicht eröffnet, Fragen des immateriellen Schadenersatzes nach Art. 82 DSGVO stellen sich dementsprechend nicht.
- F)
- 136 Die Kostenentscheidung beruht auf § 97 ZPO. Die Entscheidung zur vorläufigen Vollstreckbarkeit ergibt sich aus §§ 708 Ziff. 10, 713 ZPO.
- 137 Die Revision war nicht zuzulassen. Die Voraussetzungen des § 543 Abs. 2 ZPO liegen nicht vor. Die Rechtsprechung des BGH, insbesondere das Urteil vom 18.11.2024 - VI ZR 10/24 -, ist im Rahmen dieser Entscheidung berücksichtigt.