OLG München, Hinweisbeschluss v. 11.03.2024 – 21 U 2766/23 e

Titel:

Dsgvo, Personenbezogene Daten, Technische und organisatorische Maßnahmen, Vorgerichtliche Rechtsanwaltskosten, Auskunftsanspruch, Verletzungshandlung, Unterlassungsklage, DS-GVO, Facebook, Prozeßbevollmächtigter, Feststellungsantrag, Leistungsklage, Verantwortlichkeit, Rechtshängigkeit, Persönliche Anhörung, Telefonnummer, Vertretbare Handlung, Landgerichte, Ermäßigung der Gerichtsgebühr, Feststellungsinteresse

Schlagworte:

Datenschutzverletzung, Immaterieller Schadensersatz, Kontrollverlust, Daten-Scraping, Privatsphäre-Einstellungen, Unterlassungsanspruch, Auskunftsanspruch

Vorinstanz:

LG Ingolstadt, Endurteil vom 01.06.2023 – 81 O 549/22

Fundstelle:

GRUR-RS 2024, 47587

Tenor

1. Der Senat beabsichtigt, die Berufung gegen das Urteil des Landgerichts Ingolstadt vom 01.06.2023, Az. 81 O 549/22, gemäß § 522 Abs. 2 ZPO zurückzuweisen.

2. Hierzu besteht Gelegenheit zur Stellungnahme binnen drei Wochen nach Zustellung dieses Beschlusses.

Entscheidungsgründe

I.

1
Der Kläger, der von Beruf Softwareentwickler ist, macht Schadensersatz-, Unterlassungs- und Auskunftsansprüche wegen der Verletzung von Vorschriften der DSGVO seitens der Beklagten aus und im Zusammenhang mit dem sog. im April 2021 öffentlich bekannt gewordenen „Scraping-Vorfall“ bei Facebook geltend.

2
Der Kläger ist seit etwa 10 bis 15 Jahren und bis heute Nutzer des sozialen Online-Netzwerkes Facebook. Für die Nutzer in der Europäischen Union wird die Facebook-Plattform von der Beklagten, einem Unternehmen nach dem Recht der Irischen Republik mit Sitz in Dublin, Irland, betrieben. Die Beklagte stellt das Netzwerk, das mit Hilfe von personenbezogenen Daten die Kommunikation, das Finden von Personen und das Teilen von Informationen ermöglicht, den Nutzern kostenlos zur Verfügung. Die Finanzierung erfolgt über Werbeeinnahmen.

3
Zwischen Januar 2018 bis September 2019 kam es zu einem sog. „Scraping-Vorfall“, in dessen Rahmen Dritte bei der Beklagten als „öffentlich“ hinterlegte Informationen von Nutzern auslasen und einen sog. Leak-Datensatz im April 2021 im Darknet veröffentlichten. Der den Kläger betreffende Datensatz enthält seine Telefonnummer, die FacebookID, seinen Namen und sein Geschlecht. Vermutlich erfolgte das Data Scraping bei der Beklagten durch die damals zur Verfügung gestellte Kontakt-Import-Funktion, mit deren Hilfe die Nutzer Telefonkontakte von ihren Mobilgeräten auf Facebook hochladen konnten, um mit der Telefonnummer weitere „Freunde“ finden zu können, auch wenn das Profil der jeweiligen Personen die Telefonnummer nicht anzeigte. Die Scraper gaben eine Vielzahl von Kontakten mit automatisch erzeugten Telefonnummern in ein virtuelles Adressbuch ein und versuchten diese selbst generierten Telefonnummern einem konkreten Facebook-Profil zuzuordnen. Wurde mit einer der automatisch generierten „fiktiven“ Telefonnummer eine Übereinstimmung mit einer bei Facebook hinterlegten Telefonnummer erzielt, wurde sodann der jeweils zugehörige Facebook-Nutzer angezeigt. Auf diese Weise konnten die öffentlich

einsehbaren Daten des jeweiligen Nutzers abgegriffen und mit dessen Telefonnummer korreliert werden, vgl. Anlage B 11.

4
Aufgrund dieses Vorfalls ersetzte die Beklagte die Kontakt-Import-Funktion durch die Funktion „people you may know“. Das Sammeln von Daten mit Hilfe automatisierter Tools und Methoden war und ist nach den Nutzungsbedingungen der Beklagten untersagt.

5
Bei der Registrierung musste der Kläger seinen Namen, sein Geschlecht und seine NutzerID angeben, die als Teil seines Nutzerprofils immer öffentlich einsehbar sind, vgl. Anlage B 15. Daneben gab der Kläger freiwillig seine E-Mail Adresse, seinen Wohnort und seine Telefonnummer an, wobei er hier die Möglichkeit hatte, festzulegen, wer diese Angaben sehen kann. Bei der Registrierung wurde der Kläger auf die Nutzungsbedingungen der Beklagten, die Datenrichtlinie und die Cookie-Richtlinie hingewiesen. Informationen zu den Privatsphäre-Einstellungen konnten auch im „Hilfe-Bereich“ gefunden werden. Bei der sog. Zielgruppenauswahl legt der Nutzer fest, wer einzelne Informationen (z.B. die Telefonnummer) seines Facebook-Profils einsehen kann, die Suchbarkeits-Einstellungen legen fest, wer das Profil eines Nutzers z.B. anhand der Telefonnummer finden kann. Die Beklagte hatte im fraglichen Zeitraum in Bezug auf die Suchbarkeit des Klägers durch die Telefonnummer eine Voreinstellung auf „alle“ vorgenommen, vgl. Screenshot, Seite 36 der Klageerwiderung. Diese Voreinstellung konnte von den Nutzern auf „Freunde von Freunden“, „Freunde“ oder ab Mai 2019 auf „nur ich“ eingeschränkt werden. Hierzu wurden Informationen über die entsprechenden Optionen zur Änderung der Benutzereinstellungen bereit gestellt, Anlage B 5. Die Suchbarkeits-Einstellungen befinden sich im Abschnitt „Privatsphäre“ des Haupteinstellungsmenüs im Konto eines Nutzers, zu dem man direkt von der Startseite aus nach der Anmeldung im Konto gelangen kann. Im „Hilfe-Bereich“ wurde u.a. darauf hingewiesen, dass man kontrollieren kann, wer die Telefonnummer sehen kann. Außerdem konnte ein sog. „Privatsphäre-Check“ durchgeführt werden, vgl. Seite 11 der Klage, Anlage B 8. Nutzer wurden im Hilfebereich zudem darüber informiert, zu welchen Zwecken ihre Telefonnummer verarbeitet werden kann, Anlage B 6. Die Nutzer wurden weiter darüber informiert, dass sie ihre Telefonnummer auch jederzeit entfernen können, Anlage B 7.

6
Die irische Datenschutzbehörde (Data Protection Commission) leitete im April 2021 ein Verfahren gegen die Beklagte ein und verhängte im November 2022 auf der Grundlage von Art. 83 DSGVO ein Bußgeld gegen die Beklagte, da aus ihrer Sicht die Beklagte gegen Art. 25 DSGVO verstoßen habe. Die Beklagte legte dagegen Berufung ein, über die noch nicht entschieden ist.

7
Der Kläger trägt vor, dass die Beklagte gegen eine Vielzahl von Vorschriften der DSGVO verstoßen habe und deshalb die von ihm geltend gemachten Ansprüche begründet seien. Die Beklagte stellt dies in Abrede und verweist insbesondere darauf, dass sie im fraglichen Zeitraum ausreichende Sicherheitsmaßnahmen ergriffen hätte, um sog. Scraping zu verhindern.

8
Hinsichtlich der weiteren Einzelheiten des Sach- und Streitstandes wird auf die tatsächlichen Feststellungen im landgerichtlichen Urteil Bezug genommen, § 540 Abs. 1 ZPO.

9
Das Landgericht Ingolstadt hat mit Urteil vom 01.06.2023 nach Anhörung des Klägers die Klage abgewiesen. Es konnte sich auf der Grundlage des schriftsätzlichen Vorbringens in Verbindung mit der persönlichen Anhörung des Klägers keine Überzeugung vom Vorhandensein eines immateriellen Schadens bilden.

10
Dagegen richtet sich die Berufung des Klägers, der seine erstinstanzlich geltend gemachten Ansprüche mit dem Rechtsmittel vollumfänglich weiter verfolgt. Er ist der Meinung, dass die Beklagte diverse Verstöße gegen die DSGVO begangen habe, was beim Kläger zu einem Kontrollverlust über seine Daten geführt habe. Der Kontrollverlust habe bei ihm ein Gefühl des Unbehagens und der Sorge vor einem möglichen Missbrauch seiner persönlichen Informationen hinterlassen. Seit dem Vorfall erhalte der Kläger unregelmäßig unbekannte Kontaktversuche über sein Telefon, die Betrugsversuche und potentielle

Virenlinks enthielten. Die Beklagte habe insbesondere gegen die Verpflichtung zur Implementierung angemessener technischer und organisatorischer Maßnahmen zum Schutz der personenbezogenen Daten verstoßen und durch die Voreinstellung der Suchbarkeit über die Telefonnummer auf „alle“ gegen die Verpflichtung einer datenschutzfreundlichen Verarbeitung der Daten verstoßen. Hinsichtlich der weiteren Einzelheiten des Berufungsvorbringens wird auf die Berufungsbegründung vom 31.07.2023 und den Schriftsatz vom 06.11.2023 Bezug genommen.

11
Der Kläger beantragt in der Berufung unter Aufhebung des am 01.06.2023 zugestellten Urteils des Landgerichts Ingolstadt (81 O 549/22) wie folgt zu erkennen:

1. Die Beklagte wird verurteilt, an die Klägerseite immateriellen Schadensersatz in angemessener Höhe zu zahlen, dessen Höhe in das pflichtgemäße Ermessen des Gerichts gestellt wird, mindestens jedoch 1.000,00 EUR nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klägerseite alle zukünftigen 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 wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu EUR 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. personenbezogenen Daten der Klägerseite, namentlich Telefonnummer, FacebookID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern,

b. die Telefonnummer der Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Information darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls die Berechtigung verweigert wird.

4. Die Beklagte wird verurteilt, der Klägerseite Auskunft über die Klägerseite betreffende personenbezogene Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten.

5. Die Beklagte wird verurteilt, an die Klägerseite vorgerichtliche Rechtsanwaltskosten in Höhe von 887,03 € zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

12
Die Beklagte beantragt,

die Berufung zurückzuweisen.

13
Die Beklagte bestreitet Verstöße gegen die DSGVO und sieht die angeblichen Gesetzesverletzungen schon nicht vom Schutzbereich des Art. 82 DSGVO umfasst. Auch sei beim Kläger kein Schaden entstanden. Der Auskunftsanspruch sei erfüllt. Hinsichtlich der Einzelheiten der Berufungserwiderung wird auf den Schriftsatz der Beklagten vom 26.10.2023 verwiesen.

II.

14
Der Senat beabsichtigt, die Berufung der Klagepartei gegen das Urteil des Landgerichts Ingolstadt vom 01.06.2023 gemäß § 522 Abs. 2 ZPO zurückzuweisen, weil er einstimmig der Auffassung ist, dass die

Berufung offensichtlich keine Aussicht auf Erfolg hat, der Rechtssache keine grundsätzliche Bedeutung zukommt, weder die Fortbildung des Rechts- noch die Sicherung einer einheitlichen Rechtsprechung eine Entscheidung des Berufungsgerichts erfordert und die Durchführung einer mündlichen Verhandlung nicht geboten ist.

15
Gemäß § 513 Abs. 1 ZPO kann die Berufung nur darauf gestützt werden, dass das angefochtene Urteil auf einer Rechtsverletzung im Sinne von § 546 ZPO beruht oder nach § 529 ZPO zugrunde zu legende Tatsachen eine andere Entscheidung rechtfertigen. Dies zeigt die Berufungsbegründung nicht auf.

16
Das Urteil des Landgerichts wird im Ergebnis vom Senat vollumfänglich geteilt.

17
Im Hinblick auf die Berufungsbegründung der Klagepartei sind folgende Ausführungen veranlasst.

1. Zum Antrag 1, Anspruch auf Zahlung eines immateriellen Schadensersatzes, Art. 82 DSGVO:

18
1.1. Der Anwendungsbereich der DSGVO ist in zeitlicher Hinsicht zumindest teilweise und in sachlicher und räumlicher Hinsicht eröffnet, Art. 99 Abs. 2, Art. 2 Abs. 1, Art. 4 Nr. 7 DSGVO. Dies stellt auch die Beklagte nicht in Abrede. Der Kläger ist aktivlegitimiert, da er vom Data Scraping datenschutzrechtlich betroffen ist und die Beklagte passivlegitimiert, da sie als Betreiberin der Plattform Facebook Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO ist.

19
1.2. Zweifel bestehen jedoch, ob der Beklagten tatsächlich eine relevante Verletzungshandlung zur Last gelegt werden kann, die zu einem Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO führt, wobei der Senat zugunsten der Klagepartei davon ausgeht, dass schon jeglicher Verstoß gegen die DSGVO ausreicht und nicht zusätzlich eine der DSGVO zuwiderlaufende Verarbeitung erforderlich ist (zum Streitstand und zur vorstehenden Auslegung vgl. BeckOK, DatenschutzR/Quaas 46. Ed. 1.11.2023, DS-GVO Art. 82 Rn. 14 - 16, Kühling/Buchner/Bergt DS-GVO Art. 82 Rn. 23, 24; Paal/Pauly/Frenzel, 3. Auflage 2021, DS-GVO, Art. 82 Rn. 6; aA Ehmann/Selmayr/Nemitz, 2. Auflage 2018, DS-GVO, Art. 82 Rn. 8; Sydow/Marsch DS-GVO/BDSG/Kreße, 3. Auflage 2022, DS GVO Art. 82 Rn. 7). Die Frage, ob eine relevante Verletzungshandlung vorliegt, kann hier letztlich dahinstehen bzw. zugunsten des Klägers unterstellt werden, weil der geltend gemachte Zahlungsanspruch schon deshalb nicht gegeben ist, da der Senat – wie das Landgericht – nicht davon überzeugt ist, dass dem Kläger ein Schaden entstanden ist. Gleichwohl geht der Senat in Bezug auf die von der Klagepartei behaupteten Verstöße gegen die DSGVO auf die wesentlichen Aspekte ein:

20
1.2.1. Ein Verstoß gegen Informationspflichten sowie der Vorwurf einer mangelnden Transparenz der Information dürfte nicht gegeben sein, Art. 5 Abs. 1 a, Art. 13, Art. 14 DSGVO. Die Beklagte hat ihre Nutzer im streitgegenständlichen Zeitraum im Rahmen ihrer Datenrichtlinie, dem Hilfebereich und in Bezug auf die Verwendung der Daten, insbesondere auch die Verwendung der Telefonnummer sowie die damals noch bestehenden Kontakt-Import Funktion aufgeklärt. Sie hat klare Informationen zur Verfügung gestellt, die verständlich und zugänglich waren. Diese sind sinnvoll in mehreren Ebenen und mit verlinkten Einstellungsmöglichkeiten angelegt und geben Auskunft über sämtliche Nutzungs- und Suchbarkeitsoptionen. Der Nutzer von Facebook wird darauf aufmerksam gemacht, dass er die Privatsphäre-Einstellungen individuell anpassen kann. Die Datenschutzinformationen sind zwar unvermeidlich umfangreich, gleichwohl aber nicht unübersichtlich. Über die Zwecke der Datenverarbeitung dürfte die Beklagte ausreichend aufgeklärt und eine selbstbestimmte Nutzung der Dienste ermöglicht haben, gerade auch durch die Zusatzfunktion „Privatsphäre-Check“. In diesem Zusammenhang wird auf den von der Klagepartei selbst in die Klage auf Seite 11 eingefügten Screenshot verwiesen, worin über die Frage aufgeklärt wird „Wer kann dich anhand der angegebenen Telefonnummer finden ?“. Die Befassung mit den Privatsphäre-Einstellungen vor dem Hintergrund des Schutzes eigener Daten kann von den Nutzern der Beklagten, die selbst auch eine gewisse Verantwortung für den Umgang ihrer persönlichen Daten in sozialen Netzwerken oder im Internet im Allgemeinen haben, durchaus verlangt werden; so auch LG Detmold, Urteil vom 28.03.2023 – 02 O 85/22, Rn. 28, juris.

21
1.2.2. Der Senat hat weiter auch Zweifel, ob die Beklagte gegen die Pflicht zur Implementierung angemessener technischer und organisatorischer Maßnahmen verstoßen hat, Art. 5 Abs. 1 f, Art. 24, Art. 25, Art. 32 DSGVO. Diese Normen verlangen vom Verantwortlichen, der auch eine dahingehende Beweislast hat (vgl. Urteil des EuGH vom 14.12.2023 – C-340/21, Rn. 52), einen rechtmäßigen und verantwortungsbewussten Umgang mit der Verarbeitung der Daten. Ein Verstoß gegen diese Normen wäre nur dann begründet, wenn die Beklagte aus der Sicht ex ante nach dem damaligen Stand der Technik strengere Maßnahmen hätte ergreifen müssen. Ein Verstoß gegen Art. 32 DSGVO könnte schon deshalb ausscheiden, weil die betroffenen Daten unstreitig öffentlich einsehbar waren, so LG Aachen, Urteil vom 22.02.2023 – 8 O 177/22, GRUR-RS 2023, 2621. Zudem ist Art. 32 DSGVO nicht als absolute Gewährleistung der Datensicherheit konzipiert.

22
Auch mussten von der Beklagten nicht alle theoretisch denkbaren Missbrauchspotenziale und -konstellationen präventiv antizipiert werden. Es kann zwar davon ausgegangen werden, dass mit der Kontakt-Import-Funktion gewisse Risiken einer Verletzung des Schutzes personenbezogener Daten einhergingen, allerdings gab es in der Vergangenheit vor dem streitgegenständlichen Vorfall unstreitig bei der Beklagten keinerlei derartige Data-Scraping Vorfälle, so dass die Eintrittswahrscheinlichkeit aus der Sicht ex ante gering eingeschätzt werden durfte. Die Schwere der möglichen Risiken durfte ebenfalls als gering eingeschätzt werden, weil es sich bei den von den Scrapern abgegriffenen Daten nur um öffentlich zugängliche Informationen handelt, die von Nutzern der Beklagten, wie auch dem Kläger, freiwillig preisgegeben worden sind. Die Beklagte hat in der Wahl der Mittel zur Risikobegrenzung zudem einen Ermessensspielraum, vgl. Kühling/Buchner/Jandt, 4. Aufl. 2023, DS-GVO Art. 32 Rn. 8, der mit den von der Beklagten vorgetragenen (von der Klagepartei mit Nichtwissen bestrittenen und hier als zutreffend unterstellten) Maßnahmen, wie Übertragungsbegrenzungen und Bot-Erkennung durch Captcha-Abfragen jedenfalls nicht offensichtlich fehlerhaft ausgenutzt worden sein dürfte. Die Beklagte beschäftigte zudem schon damals ein Team von Datenanalysten und Softwareingenieuren zur Verhinderung von Scraping-Aktivitäten. Das Data-Scraping frei bzw. öffentlich zugänglicher Informationen hätte durch die individuellen Entscheidungen des Klägers in den Suchbarkeitseinstellungen ohne Weiteres verhindert werden können. Entsprechende Anleitungen zur Änderung der Optionen wurden von der Beklagten bereit gestellt.

23
Der Kläger verhält sich auch widersprüchlich, wenn er einerseits freiwillig und eigenverantwortlich personenbezogene Daten auf Facebook mitteilt, um an dem sozialen Netzwerk, das auf das Finden von „Freunden“ und einen Austausch sowie Kommunikation ausgerichtet ist, teilnehmen zu können, sich andererseits aber auf das Fehlen hinreichender Sicherheitsmaßnahmen hinsichtlich frei abrufbarer Daten beruft, vgl. auch LG Kiel, Urteil vom 12.01.2023, ZD 2023, 282; AG Strausberg, Urteil vom 13.10.2022 – 25 C 95/21, BeckRS 2022, 27811.

24
Dem Senat ist bewusst, dass das OLG Hamm in seinem Urteil vom 15.08.2023 – 7 U 19/23, GRUR 2023, 1791, dazu eine andere Ansicht vertritt, letztlich wurde aber auch dort ein Schadensersatzanspruch verneint. Zwar mag es schon damals anstelle der Kontakt-Import-Funktion die heute verwendete gleichwertige Funktion „people you may know“ gegeben haben, allerdings sind vorliegend keine Anhaltspunkte ersichtlich, dass der Beklagten bereits ab Beginn der Scraping-Vorfälle die Kontakt-Import-Funktion als „Schwachstelle“ bekannt gewesen ist, was zu einer unverzüglichen Einschränkung dieser Funktion hätte führen müssen.

25
1.2.3. Der Senat sieht vorliegend nach vorläufiger Bewertung der Sach- und Rechtslage auch keinen Datenschutzverstoß durch Technikdesign infolge der gewählten Voreinstellung, Art. 25 DSGVO. Diese Vorschrift bedeutet im Grundsatz, dass ein Produkt oder Dienst für den Nutzer bereits ohne weiteres Zutun beim ersten Einschalten bzw. Aufruf die datenschutzfreundlichsten Einstellungen und Komponenten aufweisen soll, vgl. Kühling/ Buchner/Hartung, 4. Auflage 2024, DS-GVO Art. 25 Rn. 24. Der Verantwortliche wird verpflichtet durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass durch eine Voreinstellung im technischen Verfahren nur die personenbezogenen Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind. Die hier von der Beklagten getroffene Voreinstellung im Rahmen der Suchbarkeit durch

die Telefonnummer auf „alle“ dürfte indessen keinen Verstoß gegen Art. 25 DSGVO darstellen, weil insoweit der Gesamtkontext des sozialen Netzwerkes sowie das Geschäftsmodell der Beklagten, das insbesondere in dem Finden von „Freunden“ liegt, zu berücksichtigen ist. Der von der Beklagten bereit gestellte Facebook-Dienst hat weltweit ca. 2,8 Milliarden Nutzer, so dass die Suchbarkeit allein anhand des Namens in der Regel nicht ausreicht, um einen anderen Nutzer zu finden. Insofern weist die Angabe der Telefonnummer eine höhere Trefferwahrscheinlichkeit auf, so auch LG Kiel, Urteil vom 12.01.2023 – 6 O 154/22, GRUR-RS 2023, 328. Es entspricht dem charakteristischen Wesen eines sozialen Netzwerkes, dass personenbezogene Daten erhoben und durch die Nutzer nach den selbst konfigurierten Privatsphäre-Einstellungen öffentlich zugänglich gemacht werden. Zudem erlegt Art. 25 Abs. 2 DSGVO dem Verantwortlichen nicht die Pflicht auf, stets die datenschutzfreudlichste, sondern (nur) die im Rahmen der Erforderlichkeit des Verarbeitungszwecks datenschutzfreundlichste Voreinstellung zu treffen, BeckOK/DatenschutzR/Paulus, 46. Ed. 1.11.202, DS-GVO Art. 25 Rn. 8. Es müssen also lediglich geeignete, technische und organisatorische Maßnahmen getroffen werden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dies ist bei einer Kontaktplattform auch dadurch möglich, dass dem Nutzer durch Anleitungen und Hilfen die Möglichkeit gegeben wird, die Einstellungen enger zu fassen und einen „privacy check“ durchzuführen, so auch OLG München, Hinweisverfügung vom 14.09.2023, Az. 14 U 3190/23 e, GRUR-RS 2023, 24733. Auch müssen Nutzer eines sozialen Netzwerkes damit rechnen, dass frei bzw. öffentlich zugänglich gemachte oder suchbare personenbezogene Daten ggf. kopiert und anderweitig veröffentlicht werden, vgl. LG Essen, Urteil vom 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818, Rn. 18.

26
Wie oben bereits ausgeführt, lässt der Senat jedoch die Frage, ob eine Verletzungshandlung durch die Beklagte vorliegt, ausdrücklich dahinstehen. Im Hinblick darauf, dass der Senat keinen immateriellen Schaden beim Kläger sieht, kommt es hierauf nicht entscheidungserheblich an.

27
1.3. Für das Vorliegen eines Schadens reicht die bloße Verletzung von Vorschriften der DSGVO nicht aus, vielmehr muss im Einzelfall ein konkreter Schaden vorliegen, wobei ein gewisser Grad an Erheblichkeit nicht erforderlich ist, EuGH, Urteil vom 14.12.2023 – C-340/21, Rn. 78 und Urteil vom 04.05.2023 – C-300/21, Rn. 51.

28
Zwar hat der EuGH zuletzt in den Rechtssachen C-340/21 und C-678/21 den auch vom Kläger geltend gemachten Verlust über die Kontrolle der eigenen Daten infolge eines Verstoßes gegen die DSGVO und weiter auch die Befürchtung einer Person, dass ihre personenbezogenen Daten durch Dritte missbräuchlich verwendet werden könnten, grundsätzlich als möglichen immateriellen Schaden ausreichen lassen. In den genannten Entscheidungen wurde aber jeweils betont, dass das angerufene nationale Gericht prüfen muss, ob der behauptete Kontrollverlust und die Befürchtung missbräuchlicher Verwendung von personenbezogenen Daten unter den gegebenen besonderen Umständen und im Hinblick auf die betroffene Person als begründet angesehen werden kann, was letztlich Tatfragen des Einzelfalls sind.

29
Im Einklang mit dem Landgericht kann der Senat aufgrund der Angaben des Klägers bei seiner persönlichen Anhörung vor dem Landgericht nicht erkennen, dass der Kläger tatsächlich einen solchen Schaden erlitten hat, wofür er den Nachweis erbringen muss (EuGH, Urteil vom 14.12.2023 – C-340/21, Rn. 84). Der Senat schließt sich hier vollumfänglich der Würdigung der Aussage des Klägers durch das Landgericht an. Mit den im Urteil diesbezüglich angestellten Erwägungen setzt sich die Berufung nicht auseinander, sondern wiederholt nur ihren bereits erstinstanzlich gebrachten Vortrag, der in dieser Weise auch in anderen von den Klägervertretern betriebenen Verfahren formelhaft gebracht wird.

30
Anders als im schriftsätzlichen Vorbringen hat der Kläger bei seiner Anhörung schon keine Befürchtung einer missbräuchlichen Verwendung seiner Telefonnummer geäußert, sondern lediglich erklärt, dass er gerne „Herr seiner Daten“ sein und bleiben wolle. Er wolle verhindern, dass so etwas nochmals vorkomme und er wolle Ersatz für seinen zeitlichen Aufwand. Dieser bestehe darin, dass er Anrufe erhalte, deren Beantwortung ihn wahnsinnig viel Zeit kosten würden. Auch habe er bei verschiedenen SMS die Angst, dass seine Kinder mit seinem Handy irgendwelche Bestätigungen durchführten, die dann zu

Verpflichtungen führten. Trotz dieser vom Kläger beschriebenen Umstände hat er aber sein Verhalten in keiner Weise geändert, insbesondere auch nicht die Einstellung der Telefonnummer im Rahmen der Suchbarkeit auf dem Portal der Beklagten, das nach wie vor auf „alle“ lautet, geändert, was aber zu erwarten wäre. Gerade die Voreinstellung auf „alle“ bei der Suchbarkeit greift der Kläger mit seiner Klage an und führt aus, dass er auf die Änderungsmöglichkeiten nicht transparent genug hingewiesen worden sei und dass genau diese Funktion dazu geführt habe, dass im Darknet nun seine Telefonnummer, verknüpft mit dem Namen zu finden sei. Inzwischen ist der Kläger jedenfalls über seine Prozessbevollmächtigten vollumfänglich darüber informiert, wie sich diese Einstellung ändern lässt. Gleichwohl sieht der Kläger offensichtlich bis jetzt keine Veranlassung hieran etwas zu ändern. Dass inzwischen eine andere Einstellungsoption gewählt worden wäre, was der Kläger bei seiner Anhörung vor dem Landgericht angekündigt hatte, wird mit der Berufung jedenfalls nicht vorgetragen. Insoweit teilt der Senat vollumfänglich den vom Landgericht beschriebenen Eindruck, dass der Kläger einen äußerst sorglosen Umgang mit seinen Daten vermittelt, obwohl er doch selbst angibt, er wolle „Herr der Daten“ sein. Gerade als Software-Entwickler sollte es für den Kläger ein leichtes sein, die entsprechende Einstellung der Suchbarkeit zu ändern. Soweit der Kläger seine Besorgnis darauf stützt, dass seine Kinder möglicherweise auf unbekannte SMS derart reagieren könnten, dass ihm möglicherweise nicht gewollte Verpflichtungen entstünden, obliegt es dem Kläger selbst, sein Handy vor dem Zugriff seiner Kinder zu schützen, z.B. durch sichere Verwahrung, Verwendung eines Passwortes oder einer FaceID.

31
Die vom Kläger geschilderten Umstände könnten nur dann einen ersatzpflichtigen Schaden begründen, wenn der Geschädigte diese persönlich erlebt und sie ihn seelisch belastet, mithin psychisch beeinträchtigt hätten, so auch Schlussanträge des Generalanwalts Giovanni Pitruzella vom 27.04.2022 – C-340/21, Rn. 83. Derartiges ist der Aussage des Klägers aber nicht zu entnehmen, so dass der Eintritt eines immateriellen Schadens nicht überwiegend wahrscheinlich im Sinne von § 287 Abs. 1 ZPO ist.

32
Der vom Kläger nur schriftsätzlich geltend gemachte Kontrollverlust ist für den Senat schon nicht nachvollziehbar, weil die nach dem klägerischen Vortrag den Gegenstand der Verletzung von Vorschriften der DSGVO bildenden Daten aus dem öffentlich zugänglichen Profil des Klägers stammen, die damit nicht mehr unter der ausschließlichen klägerischen Kontrolle waren, so auch LG Bielefeld, Urteil vom 19.12.2022 – 8 O 182/22, Rn. 39, juris.

33
1.4. Letztlich fehlt es aber auch an der dritten Voraussetzung für einen Schadensersatzanspruch, der Kausalität zwischen einer tatbestandsmäßigen Verletzungshandlung und dem Schaden. Die Beweislast für diese Voraussetzung obliegt dem Anspruchsberechtigten, was den allgemeinen deliktischen Voraussetzungen entspricht. Eine Beweislastumkehr ist Art. 82 DSGVO nur bezüglich des Gesichtspunkts des Verschuldens zu entnehmen, vgl. BeckOK DatenschutzR/Quaas, 46. Ed. 1.11.2023, DS-GVO Art. 82 Rn. 16-27. Den Nachweis der erforderlichen Kausalität hat der Kläger jedoch nicht geführt, denn gerichtsbekannt erhalten auch Personen „dubiose“ Telefonanrufe oder SMS von unbekannten Nummern, die keine Nutzer von Facebook sind.

34
1.5. Vor diesem Hintergrund kann die weitere Frage dahinstehen, wie die Höhe eines Schadensersatzanspruchs zu ermitteln ist.

2. Feststellungsantrag:

35
Die mit dem Antrag zu 2 verfolgte Feststellungsklage ist bereits unzulässig, weil es am notwendigen Feststellungsinteresse nach § 256 Abs. 1 ZPO fehlt. Die Möglichkeit eines Schadenseintritts (vgl. BGH, Urteil vom 29.06.2021 – VI ZR 52/18) materieller oder immaterieller Art ist durch den Kläger weder hinreichend dargelegt noch ersichtlich. Gerade im Hinblick auf die vergangene Zeit ist auch nicht damit zu rechnen, dass zukünftige Schäden noch eintreten werden. Jedenfalls wäre der Feststellungsantrag aber unbegründet, weil der Eintritt künftiger Schäden mangels eines bereits eingetretenen Schadens nicht hinreichend wahrscheinlich ist.

3. Unterlassungsklage

36
3.1. Bei der mit Antrag zu 3a verfolgten Unterlassungsklage handelt es sich tatsächlich um eine verdeckte Leistungsklage, die unabhängig davon, ob sie ausreichend bestimmt ist (§ 253 Abs. 2 Nr. 2 ZPO) ebenfalls bereits unzulässig ist. Ob eine Handlungspflicht auferlegt oder Unterlassung gefordert wird, ist im Wege der Auslegung mit Blick auf den Schwerpunkt der jeweils in Rede stehenden Verpflichtung zu beurteilen. Vorliegend fordert der Kläger mit Antrag zu 3a aber im Schwerpunkt ein aktives Tun, das nicht nach § 890 ZPO, sondern als vertretbare Handlung nach § 887 ZPO zu vollstrecken ist, nämlich zukünftig Kontakt-Import-Funktionen nur im Einklang mit den einzuhaltenden Sicherheitsvorkehrungen freizuschalten, um Zugriffe unbefugter Dritter nach Möglichkeit von vornherein zu verhindern, so wie es die DSGVO verlangt. Der Kläger will gar kein Unterlassen der Nutzung der Kontakt-Import-Funktion, was er auch durch eine schlichte Umstellung der Suchbarkeitseinstellungen hätte erreichen können, sondern er will, dass irgendeine andere Kontakt-Import-Funktion unter Wahrung der Sicherheitsanforderungen genutzt werden kann. Der Antrag ist damit auf ein zukünftiges aktives Tun gerichtet, das an § 259 ZPO zu messen ist. Da die Kontakt-Import-Funktion spätestens seit September 2019 nicht mehr existiert, besteht keine Besorgnis nicht rechtzeitiger Leistung. Es ist auch nicht ersichtlich, dass die Beklagte künftig die gesetzlichen Vorgaben der DSGVO nicht umsetzen wird, zumal sie ein hohes Eigeninteresse daran hat, dass es zu keinen weiteren Scraping-Vorfällen mit einhergehenden Klagen und Bußgeldverfahren kommt. Zudem fehlt dem Antrag das erforderliche Rechtschutzbedürfnis mit Blick auf die öffentlichen Nutzerdaten. In dem gestellten Antrag werden auch weitere Daten wie Bundesland, Land, Stadt und Beziehungsstatus genannt, die der Kläger nach den Ausführungen in der Klage gegenüber der Beklagten gar nicht angegeben hat. Der Antrag erweckt damit den Anschein, dass der Kläger allein die Allgemeinheit vor der Beklagten schützen will.

37
3.2. Auch die mit Antrag 3b verfolgte Unterlassungsklage ist unzulässig.

38
Soweit der Antrag tatsächlich als Unterlassungsantrag dahingehend zu verstehen wäre, dass die Beklagte die fortgesetzte Verarbeitung ohne informierte Einwilligung zu unterlassen hat, ist die Klage wegen fehlenden Rechtsschutzbedürfnisses unzulässig. Der Kläger wurde spätestens durch seine Prozessbevollmächtigten über die Sichtbarkeit- und Suchbarkeitsfunktion informiert und hatte Gelegenheit, diese Einstellungen umzustellen. Soweit der Antrag auf zukünftige Leistung gerichtet ist, weil eine Wiederholung befürchtet wird, liegt nach dem Schwerpunkt des Rechtsschutzbegehrens in der Sache erneut kein Unterlassen vor, das nach § 890 Abs. 2 ZPO vollstreckt werden könnte, sondern eine Leistungsklage, gerichtet auf ein aktives Tun. Die Klage ist darauf gerichtet, dass zukünftig die Mobilfunktelefonnummer nur nach Maßgabe einer in Folge ausreichender Information wirksam erteilten Einwilligung im Rahmen einer Suchfunktion zu verarbeiten ist. Diese verdeckte Leistungsklage wahrt nicht die Grenzen des § 259 ZPO. Wegen der endgültigen Abschaffung der Kontakt-Import-Funktion besteht keine Besorgnis einer Leistungsverweigerung.

39
Der Senat schließt sich hier vollumfänglich den Ausführungen des OLG Hamm in dessen Urteil vom 15.08.2023 – 7 U 19/23, GRUR 2023, 1791, an.

40
Auf die vom BGH im Beschluss vom 26.09.2023 – VI ZR 97/22 aufgeworfenen Fragen zum Unterlassungsanspruch kommt es insoweit nicht an, so dass ein Abwarten der Entscheidung des EuGH nicht geboten ist.

41
4. Die mit dem Antrag nur 4 verfolgte Auskunftsklage ist unbegründet, weil die Beklagte die entsprechende Auskunft mit Schreiben vom 17.11.2021, Anlage K 2, erfüllt hat, § 362 Abs. 1 BGB. Im Übrigen geht das Auskunftsbegehren zu weit, Art. 12 Abs. 5, S. 2 Buchst. b DSGVO. Der konkrete Zeitpunkt, wann das Scraping stattgefunden hat, ist für den Kläger ohne weitere Relevanz, zumal der Zeitpunkt für die Veröffentlichung des Leak-Datensatzes feststeht. Etwas anderes ergibt sich auch nicht aus der Entscheidung des EuGH, Urteil vom 12.01.2023, C-154/21. Darin wird zwar ausgeführt, dass der Verantwortliche verpflichtet ist, einer betroffenen Person gem. Art. 15 DSGV die konkrete Identität der Empfänger von Daten mitzuteilen. Voraussetzung ist aber, dass der Verantwortliche diese Daten gegenüber

Empfängern offengelegt hat. Eine derartige Offenlegung ist aber im Fall des Scrapings zu verneinen. Der Anspruch ist im Übrigen nach dem Urteil auch ausgeschlossen, wenn es dem Verantwortlichen nicht möglich ist, die Empfänger zu identifizieren oder wenn der Auskunftsanspruch offenkundig unbegründet oder exzessiv ist. Diese Voraussetzungen liegen hier vor. Insoweit wird auf die obigen Ausführungen verwiesen. Welche Zwecke der Kläger mit den weiteren Informationen verfolgt, wird auch nicht dargelegt.

42
5. Da die Klage insgesamt keinen Erfolg hat, schuldet die Beklagte auch keinen Ersatz von vorgerichtlichen Rechtsanwaltskosten.

III.

43
Im Hinblick auf die obigen Ausführungen wird der Klagepartei die Rücknahme ihrer offensichtlich aussichtslosen Berufung empfohlen. Auf die in Betracht kommende Ermäßigung der Gerichtsgebühren von 4,0 auf 2,0 (vgl. KV Nr. 1220, 1222) wird hingewiesen. gez.