Beglaubigte Abschrift

Landgericht Hamburg

Az.: 325 O 65/23

Verkündet am 14.06.2024

JAng
Urkundsbeamtin der Geschäftsstelle

Urteil

IM NAMEN DES VOLKES

In der Sache

- Kläger -

Prozessbevollmächtigte:
Rechtsanwälte **WBS LEGAL Rechtsanwaltsgesellschaft mbH**, Eupener Straße 67, 50933 Köln, Gz.:

gegen

Meta Platforms Ireland Limited (zuvor: Facebook Ireland Ltd.), vertreten durch die Mitglieder des Board of Directors, Merrion Road D04 X2K5, Dublin 2, Irland

- Beklagte -

Prozessbevollmächtigte:
Rechtsanwälte **Freshfields Bruckhaus Deringer Rechtsanwälte Steuerberater PartG mbB**, Josephsplatz 1, 90403 Nürnberg, Gz.:

erkennt das Landgericht Hamburg - Zivilkammer 25 - durch den Vorsitzenden Richter am Landgericht als Einzelrichter auf Grund der mündlichen Verhandlung vom 12.12.2023 für Recht:

I. Die Beklagte wird verurteilt, an den Kläger immateriellen Schadensersatz in Höhe von € 500,00 nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz p.a. seit dem 03.06.2023 zu zahlen.

II. Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger diejenigen künftigen Schäden zu ersetzen, die auf den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten im Jahr 2019 zurückzuführen sind.

III. Die Beklagte wird verurteilt, es bei Vermeidung eines vom Gericht für jeden Fall der Zuwiderhandlung festzusetzenden Ordnungsgeldes – und für den Fall, dass

dieses nicht beigetrieben werden kann, einer an ihrem Director zu vollstreckenden Ordnungshaft – oder einer an ihrem Director zu vollstreckenden Ordnungshaft bis zu sechs Monate (Ordnungsgeld im Einzelfall höchstens € 250.000,00, Ordnungshaft insgesamt höchstens zwei Jahre)

zu unterlassen,

die Telefonnummer des Klägers über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die dem Stand der Technik entsprechenden für eine angemessene Datensicherheit erforderlichen Maßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als die Kontaktaufnahme zu verhindern.

IV. Die Beklagte wird verurteilt, an den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von € 453,87 nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz p.a. seit dem 27.04.2022 zu zahlen.

V. Die weitergehende Klage wird abgewiesen.

VI. Die Kosten des Rechtsstreits werden gegeneinander aufgehoben.

VII. Das Urteil ist hinsichtlich der Entscheidungen zu I., III., IV. und VI. vorläufig vollstreckbar, für den Kläger jedoch nur gegen Sicherheitsleistung, und zwar hinsichtlich der Entscheidung zu III. gegen Sicherheitsleistung in Höhe von € 2.000 und im Übrigen gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrages.

Dem Kläger bleibt nachgelassen, die vorläufige Kostenvollstreckung der Beklagten durch Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils für die Beklagte vollstreckbaren Kostenbetrages abzuwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 110 % des jeweils zu vollstreckenden Betrages leistet;

und beschließt:

Der Streitwert wird auf insgesamt € 7.000,00 festgesetzt.

Tatbestand

Der Kläger nimmt die Beklagte u.a. auf immateriellen Schadensersatz, Auskunft und Unterlas-

sung in Anspruch.

Die Beklagte betreibt die Social Media Platform Facebook.

Der Kläger nutzt dieses Netzwerk, um mit anderen Nutzern zu kommunizieren, private Fotos zu teilen und mit anderen Nutzern zu diskutieren.

Die Nutzer des sozialen Netzwerks geben bei der Registrierung Informationen über sich an. Ein Teil dieser Angaben (Name, Geschlecht, Nutzer-ID) ist zwingend öffentlich einsehbar, für andere Informationen (Telefonnummer, E-Mail-Adresse, Wohnort, Geburtsdatum, Stadt und Beziehungsstatus) kann der Nutzer festlegen, ob diese für jedermann oder nur für einen engeren Nutzerkreis („Freunde“) einsehbar sind. Unter dem Auswahlpunkt „Finden mit E-Mail-Adresse oder Telefonnummer“ findet man bei der Einrichtung eines Accounts den voreingestellten Wert „ja“, den der Nutzer abändern kann. Zum Zeitpunkt der Einrichtung des Accounts durch den Kläger war es möglich, die Telefonnummer so zu hinterlegen, dass sie auf dem Profil nur für den Nutzer selbst einsehbar war. Die Beklagte gab an, dass sich ein Nutzer auf diese Weise eine Möglichkeit verschaffen könne, sein Passwort ggf. zurückzusetzen. Sie bot damals mit dem Kontaktimportprogramm eine Funktion an, mit der ein Nutzer ihm bekannte Telefonkontakte darauf überprüfen konnte, ob die Telefonnummern einer Facebook-Seite zugeordnet waren, um auf diese Weise andere ihm bekannte Nutzer bei Facebook aufzufinden.

Im Jahr 2019 lasen unbekannte Dritte Daten von 533 Millionen Facebook-Nutzern automatisiert aus und veröffentlichten diese im sogenannten Darknet, darunter auch Daten des Klägers. Hierüber wurde im April 2021 in den Medien berichtet. Den Vorgang des Auslesens bezeichnet man als „Scraping“. Die Täter waren dabei auch an Telefonnummern gelangt, die nicht öffentlich einsehbar waren, indem sie die Kontaktimportfunktion verwendeten. Scraping war im Jahr 2019 bereits ein bekanntes Vorgehen, um persönliche Daten Dritter zu erwerben; es war nach den Nutzungsbedingungen von Facebook nicht zulässig. Die Beklagte informierte weder den Kläger noch die für sie zuständige irische Datenschutzbehörde über den Datenzugriff.

Mit vorgerichtlichem anwaltlichem Schreiben forderte der Kläger die Beklagte erfolglos zu einer Schadensersatzzahlung, der Unterlassung einer künftigen Zugänglichmachung seiner Daten und zur Auskunft darüber auf, welche Daten von ihm abgegriffen worden seien. Die Beklagte wies das Schadensersatz- und Unterlassungsbegehren zurück und teilte mit, dass sich unter den von Dritten abgegriffenen und veröffentlichten Daten auch solche des Klägers befunden hätten. Sie gab weiter an, dass es im Jahr 2019 möglich gewesen sei, das Facebook-Konto des Klägers über die Telefonnummer zu finden, und dass die Nutzer-ID, Vorname, Nachname und Geschlecht des Klägers zu den durch Scraping abgerufenen Daten gehörten und zusammen mit dem Land und der Telefonnummer veröffentlicht worden seien (Anlage B16).

Die irische Datenschutzbehörde DPC hat am 28.11.2022 wegen des oben genannten Vorfalls, von dem auch die Daten des Klägers betroffen waren, eine Geldbuße von € 265 Mio. gegen die Beklagte verhängt. Die Beklagte bietet ihren Nutzern aktuell die Löschung der Telefonnummer aus ihrer Adressbuch-Datenbank an.

Der Kläger macht geltend, bei Erstellung eines Accounts werde ein Facebook-Nutzer mit einer Informationsflut aus Nutzungsbedingungen, Aussagen zur Verwendung von Cookies und Datenschutzrichtlinien konfrontiert. Auch unter dem Link „Privatsphäre auf einem Blick“ fänden sich eine Reihe von unübersichtlichen Unterseiten mit schwerverständlichen Informationen. Die Messenger-App von Facebook habe zudem weitere unübersichtliche Datenschutzeinstellungen. Er habe nicht gewollt, dass seine Daten standardmäßig unter Angabe seiner Telefonnummer einsehbar seien. Mit seiner Telefonnummer sei er immer vorsichtig umgegangen und habe diese nicht im Internet veröffentlicht. Die Täter, die die Daten bei Facebook entwendet hätten, hätten systematisch die in Deutschland existierenden elfstelligen Mobilfunknummern als ihre angeblichen Kontakte in das Kontaktimportprogramm eingestellt und bei einem Treffer die bei der Beklagten gespeicherten Daten abgegriffen. Sie hätten dabei Daten wie die Telefonnummer, die Facebook-ID, den Namen, Vornamen, das Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus u.a. ermittelt. Die Beklagte habe keine Maßnahmen ergriffen, um die Plausibilität derartiger Anfragen zu überprüfen. Sie habe sich nicht an etablierten Standards wie etwa dem IT-Grundschutzkompendium des Bundesamtes für Sicherheit in der Informationstechnik oder den geltenden ISO-Normen orientiert. Mittels IP-Logs sei der massenhafte Zugriff auf Profile erkennbar und blockierbar gewesen. Ferner hätte sie einen „Layered Defense“-Ansatz verwenden müssen. Ihm sei nicht bekannt, welche seiner Daten abgegriffen worden seien. Aufgrund der Veröffentlichung seiner Telefonnummer werde er mit unerwünschten SMS belästigt. Ihm drohe, Opfer eines auf diesem Weg ausgeführten Betrugsversuchs oder so übermittelter Viren zu werden. Er fühlte sich zudem wegen des Verlustes der Kontrolle über seine Daten unwohl und habe ein erhöhtes Misstrauen gegenüber E-Mails oder Anrufen mit unbekannter Nummer entwickelt. Durch Einblick in ihre Log-Dateien könne die Beklagte erkennen, welche Daten von ihm abgerufen worden seien.

Er habe die Suchbarkeitseinstellung während des Prozesses dahingehend verändert, dass eine Suche für alle Nutzer nach seiner Telefonnummer ausgeschlossen sei. Diese Einstellung sei auf „alle“ zurückgesetzt worden. Als er dies bemerkt habe, habe er die Einstellung erneut geändert (Anlage K6).

Des weiteren macht der Kläger geltend, die Beklagte habe in vielfacher Weise gegen Vorgaben der Datenschutzgrundverordnung verstoßen. Sie habe das Gebot nutzerfreundlicher Voreinstellungen gemäß Art. 25 Abs. 2 DSGVO nicht befolgt. Gerade aufgrund der Vielzahl an Einstellungs-

möglichkeiten habe sie damit rechnen müssen, dass die meisten Nutzer aus Bequemlichkeit die Voreinstellungen beibehalten würden. Es sei keinesfalls offensichtlich, dass die Nutzer der Beklagte ermöglichen wollten, dass ihre Daten bekannt würden. Gerade die bei der Beklagten geltende Klarnamenpflicht zwinge zu einem vorsichtigen Umgang hinsichtlich der Veröffentlichung von Nutzerdaten. Die Beklagte habe bei der Verarbeitung der Daten die Vorgaben nach § 5 Abs. 1 a), b) und c) DSGVO nicht beachtet. Auch sei seine Einwilligung in die Datenverarbeitung nicht wirksam, weil die Beklagte nicht hinreichend nach Artt. 13, 14 DSGVO über den Zweck der Verwendung der Daten, die Rechtsgrundlage und die berechtigten Interessen informiert habe. Sie habe die Vorgaben der Artt. 5 Abs. 1 f), 32 DSGVO über die Sicherheit der Datenverarbeitung nicht eingehalten. Insofern trage sie zumindest eine sekundäre Darlegungslast hinsichtlich der von ihr ergriffenen Maßnahmen, der Risikobewertung, der Datenschutzfolgeabschätzung und der Evaluierung. Ferner sei sie ihrer Pflicht nach Artt. 33, 34 DSGVO zur Dokumentation und Benachrichtigung der Nutzer und der Datenschutzbehörde von einer Verletzung des Schutzes personenbezogener Daten nicht nachgekommen. Außerdem habe sie ihm nicht die nach Art. 15 DSGVO geschuldete Auskunft erteilt. Es fehle die Angabe, welche Daten mittels Scraping abgefangen worden seien und wie viele Beteiligte diese Funktion ausgenutzt hätten. Sämtliche Verstöße gegen die Datenschutzgrundverordnung begründeten einen Schadensersatzanspruch nach Art. 82 DSGVO. Eine Verletzung subjektiver Rechte sei hierfür nicht erforderlich. Der Schadensbegriff sei weit zu verstehen. Er umfasse auch immaterielle Schäden und setze keine Erheblichkeit voraus. Nur dies entspreche der Funktion des Art. 82 DSGVO, eine abschreckende Wirkung zu erzielen.

Auch der Klagantrag zu 2. sei zulässig. Ihm stehe ein Feststellungsinteresse für künftige Schäden zu, die durch die Formulierung des Klagantrags umfassend erfasst würden. Ein Unterlassungsanspruch bestehe nach §§ 1004 Abs. 1 Satz 2, 823 Abs. 1 BGB sowie nach Art. 17 DSGVO. Der Antrag zu 3a) sei ausreichend bestimmt. Eine nähere Konkretisierung der zu unterlassenden Handlung sei nur dann zu fordern, wenn der Anspruchsinhaber diese ohne weiteres konkreter fassen könne. Dies sei bei den dem Stand der Technik entsprechenden künftigen Maßnahmen nicht der Fall. Von ihm als Verbraucher sei nicht zu erwarten, dass er einem Großkonzern wie der Beklagten die dem Stand der Technik entsprechenden Maßnahmen aufzeigt. Auch der Antrag zu 3b) sei ausreichend bestimmt. Er könne verlangen, dass die Beklagte die Nutzung derjenigen Daten unterlasse, in deren Verarbeitung er aufgrund der unübersichtlichen Nutzungsbedingungen nicht wirksam eingewilligt hat. Sein mit dem Antrag zu 4. verfolgtes Auskunftsverlagen sei nicht erfüllt, da die Beklagte keinen konkreten Empfänger benannt habe. Sie müsse die Identität der Scraper kennen, wenn sie gegen diese mit einer Unterlassungsverfügung vorgehe.

Der Kläger stellt folgende Anträge:

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

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger alle künftigen Schäden zu ersetzen, die ihm durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte, entstanden sind, und/oder noch entstehen werden,

3. Die Beklagte wird verurteilt, es bei Meidung einer für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu € 250.000,00, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckenden Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,

a) personenbezogene Daten des Klägers, namentlich Telefonnummer, FacebookID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als die Kontaktaufnahme zu verhindern,

b) die Telefonnummer des Klägers auf Grund der 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 Kontaktimportportals verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger-App, hier ebenfalls explizit die Berechtigung verweigert wird,

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

5. Die Beklagte wird verurteilt, an den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe

von € 887,02 zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte macht geltend, sie habe bereits bei Anmeldung des Klägers leicht zugängliche Privatsphäre-Einstellungen zur Verfügung gestellt. Dazu gehöre die Darlegung, welche Daten öffentlich sichtbar seien, und die Suchbarkeitseinstellungen. Zudem ermögliche sie mit einem Privatsphäre-Check und einem „Wer-kann-nach-mir-Suchen“-Bereich zu kontrollieren, welche Daten von Dritten gefunden werden könnten. Die Datenschutzeinstellungen würden automatisch auf die Messenger-App übertragen.

Die Kontaktimportfunktion sei von ihren Nutzern überwiegend bestimmungsgemäß verwendet worden. Es sei nicht möglich gewesen, mit ihr sämtliche Daten eines Nutzers abzufragen. Für einige der angeblich ermittelten Daten existiere gar kein Profilfeld. Richtig sei, dass ausschließlich öffentlich einsehbare Daten ausgelesen worden seien. Ihr seien nicht sämtliche im Darknet auf der Seite raidforums.com eingestellten Daten bekannt. Sie habe schon vor dem Vorfall Maßnahmen ergriffen, um Nutzer über die Möglichkeit des Scrapings zu informieren. Zur Vermeidung eines solchen Vorgehens habe sie Übertragungsbegrenzungen und Bot-Erkennungen verwendet. Es habe diesbezüglich keinen Branchenstandard gegeben. Sie beschäftige ein Team von Softwareingenieuren, die Scraping-Vorgänge erkennen und unterbinden sollten. Gegen ihr bekannte Scraper gehe sie auch mit Kontosperren und gerichtlich vor. Sie verwende auch Captchas. Scraping lasse sich aber nicht vollständig verhindern, vielmehr sei in diesem Zusammenhang eine Balance zwischen der Gewährleistung der Nutzbarkeit der Funktionen für legitime Nutzer und der Eindämmung des Scraping-Risikos zu finden. Zudem habe sie ihr System so angepasst, dass eine Suche der Telefonnummer über die Facebook-Suchfunktion nicht mehr möglich sei. Im Nachgang habe sie den Kontakt-Importer dahingehend eingeschränkt, dass ein Treffer nur nach Durchführung eines Social-Connection Check erfolge. Schließlich habe sie die Anzeige direkter Kontaktübereinstimmungen durch eine Liste mit Kontaktvorschlägen ersetzt, für die neben der Telefonnummer auch andere Anhaltspunkte genutzt würden. Die öffentlich verbreiteten Daten des Klägers seien bereits zuvor von ihm öffentlich zugänglich gemacht worden. Diese Daten seien für Kriminelle von geringem Nutzen. Auch der Zugriff auf die Telefondaten erhöhe nicht das Risiko, dass eine Person Opfer von Internetverbrechern werde.

Der Kläger habe seine Suchbarkeitseinstellung nicht nachträglich verändert. Sie ermögliche seit dem 25.3.2017 eine Suche durch jeden (Anlage B21).

Des weiteren macht die Beklagte geltend, der Klagantrag zu 1. sei unzulässig, da er auf zwei zeitlich auseinanderliegende Vorgänge gestützt werde, ohne das Verhältnis klarzustellen. Damit sei der Umfang der Rechtskraft einer Entscheidung unklar, außerdem werde durch die alternative Verbindung von Streitgegenständen das Kostenrisiko unzulässig auf sie abgewälzt. Der Kläger trage die Darlegungs- und Beweislast für einen Verstoß von ihr gegen die Datenschutzgrundverordnung bei der Verarbeitung von Daten. Dazu gehörten weder die Informationspflichten noch ein Verstoß gegen den Grundsatz der “Privacy by Default“. Sie habe sämtliche in Artt. 13 und 14 DS-GVO vorgesehenen Informationen zur Datenschutzvereinbarung zur Verfügung gestellt. Mehrstufen-Datenschutzerklärungen, wie sie sie verwendet habe, entsprächen einer Empfehlung der europäischen Datenschutzbehörde. Über hypothetische Verarbeitungsmöglichkeiten Dritter habe sie nicht informieren müssen. Sie habe Maßnahmen gegen das Scraping getroffen, wobei ihr ein Ermessensspielraum zustehe. Der Kläger habe nicht dargelegt, dass diese bei der gebotenen Gesamtbewertung aus ex-ante-Sicht unzureichend gewesen seien. Für öffentlich einsehbare Daten gelte der in Art. 32 DSGVO genannte Grundsatz der Vertraulichkeit von Daten schon nicht. Auch ein Verstoß gegen Art. 25 DSGVO liege nicht vor. Zweck von Facebook sei es, Menschen zu ermöglichen, sich mit Freunden, Familien und Gemeinschaften zu verbinden. Aus diesem Grund habe sie die Funktionen so einrichten können, dass dies möglich sei. Dem entspreche eine Standard-Sucheinstellung, die im Ausgangspunkt auf „alle“ gesetzt sei. Die Scraping-Vorgänge hätten keine Benachrichtigungspflicht ausgelöst, weil sie dabei den Schutz personenbezogener Daten nicht verletzt habe. Von Art. 82 DSGVO seien nur Handlungen im Zusammenhang mit der Verarbeitung von Daten erfasst. Schaden im Sinn des Art. 82 DSGVO könne nur eine spürbare tatsächliche Beeinträchtigung von einigem Gewicht sei, denn ein Schaden als Anspruchsvoraussetzung wäre überflüssig, wenn schon bei jedem Verstoß gegen die Datenschutzgrundverordnung eine Zahlung veranlasst sei. Ein etwaiger Kontrollverlust sei ihr nicht zuzurechnen, da der Kläger selbst seine Daten öffentlich gemacht habe. Es fehle auch an Kausalität und Verschulden.

Des weiteren macht die Beklagte geltend, der Klagantrag zu 2. sei zu unbestimmt und in seinem Wortlaut widersprüchlich. Es fehle ein Feststellungsinteresse mangels Wahrscheinlichkeit eines Schadenseintritts. Die Klaganträge zu 3) seien schon nicht auf eine Unterlassung, sondern auf ein aktives Handeln gerichtet. Auch der Antrag zu 3a) sei zu unbestimmt, da die Bestimmung der nach dem Stand der Technik möglichen Sicherheitsmaßnahmen ins Vollstreckungsverfahren verlagert würde. Zudem könne sie nicht dazu verpflichtet werden, es zu unterlassen, die zwingend

öffentlichen Nutzerdaten anderen zugänglich zu machen. Es fehle außerdem an einer Anspruchsgrundlage, da ihr mangels Gewährung eines unbefugten Zugriffs auf die Nutzerdaten keine Erstbegehung vorzuwerfen sei. Die Regelungen der Datenschutzgrundverordnung seien abschließend und sähen keine Unterlassungsansprüche vor. Zudem müssten nach Art. 32 DSGVO eine Abwägung vorgenommen werden, welche Maßnahmen nach den dort genannten Kriterien zu ergreifen seien. Für die Nutzung der Telefonnummer habe sie alle benötigten Informationen zur Verfügung gestellt. Die geschuldete Auskunft habe sie erteilt. Die vorgerichtlichen Anwaltskosten seien mangels Schuldnerverzugs nicht von ihr zu erstatten.

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die von den Parteien zur Akte gereichten Schriftsätze nebst Anlagen Bezug genommen.

Entscheidungsgründe

Die Zuständigkeit des Gerichts für die Klage ist gegeben (I.) und die Klage hat in dem aus dem Tenor ersichtlichen Umfang Erfolg. Mit den weitergehenden Anträgen vermag der Kläger hingegen nicht durchzudringen.

I. Das Gericht ist nach Art. 18 Abs. 1 2. Alternative, Art. 17 EuGVVO international zuständig. Die Beklagte hat ihr Angebot unter anderem auf Deutschland ausgerichtet.

II. Dem Kläger steht nach Art. 82 DSGVO ein Schadensersatzanspruch in der tenorierten Höhe zu.

1. Der Antrag ist zulässig. Entgegen der Auffassung der Beklagten macht der Kläger die verschiedenen von ihm behaupteten Verstöße nicht alternativ zum Gegenstand seiner Klage, ohne einen logischen Vorrang zu benennen. Richtig ist zwar, dass der Kläger vier verschiedene zeitlich zum Teil weit auseinanderliegende Handlungen als Verstoß gegen die Vorgaben der Datenschutzgrundverordnung wertet, indem er der Beklagten vorwirft, sie hätte 2017 bei Einrichtung seines Accounts andere Standardeinstellungen und Informationen vorhalten müssen, sie hätte vor 2019 geeignetere Maßnahmen zum Schutz vor Scraping und einem Missbrauch des

Kontaktimportprogramms einführen müssen, sie hätte nach dem Vorfall im April 2019 unverzüglich die Datenschutzbehörden und ihn selbst informieren müssen und schließlich auf sein Auskunftsverlangen 2021 eine andere Auskunft erteilen müssen. Der Kläger kann jedoch seinen Anspruch auf mehrere Ereignisse stützen. Denn er macht einen unbezifferten Schaden geltend, für den er nur einen Mindestbetrag vorgibt. Das Gericht muss also etwaige Schäden, die sich aus den unterschiedlichen Pflichtverletzungen ergeben, wenn sie nebeneinander bestehen sollten, kumulieren. Selbst wenn der geltend gemachte Mindestschaden bereits durch eine Pflichtverletzung begründet wäre, müsste es dementsprechend prüfen, ob die übrigen behaupteten Pflichtverletzungen zu einem weitergehenden Schaden geführt haben. Auch eine Klagabweisung käme bei einem solchen Antrag nur dann in Betracht, wenn keine der behaupteten Pflichtverletzungen als solche einzuordnen wäre und einen Schaden verursacht hätte.

2. Der Schadensersatzanspruch ist teilweise begründet.

a) Die Beklagte hat gegen Pflichten der Datenschutzgrundverordnung verstoßen.

aa) Einstellungen der Beklagten bezüglich der ihr gegenüber angegebenen Telefonnnummern verstießen gegen das in Art. 25 Abs. 2 DSGVO vorgesehene Prinzip der „Privacy by Default“. Nach dieser Bestimmung hat der Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Nach Art. 25 Abs. 2 Satz 3 DSGVO müssen solche Maßnahmen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Nach diesen Vorgaben hätte die Beklagte für die Kontaktimportfunktion nicht die Einstellung vorsehen dürfen, dass alle Nutzer den Kläger über seine Telefonnummer suchen können. Eine solche Suchfunktion ist für ein soziales Netzwerk wie Facebook nicht zwingend erforderlich. Das zeigt schon der Umstand, dass die Beklagte nunmehr nach eigenen Angaben die Kontaktimportfunktion vollständig deaktiviert hat und die einem neuen Nutzer bekannten Telefonnummern nur noch als Anhaltspunkt für Kontaktvorschläge gemacht hat. Gegen eine Erforderlichkeit spricht auch, dass die Beklagte ihren Nutzern ermöglicht hat, die Suchbarkeit über die Telefonnummer einzuschränken oder auszuschließen. Ob möglicherweise eine Mehrzahl der Nutzer von Facebook die Kontaktimportfunktion als hilfreich erachtete, kann dahinstehen. Denn allein dies würde keine „opt-out“-Regelung, wie sie die Beklagte verwendet hat, rechtfertigen. Dass eine Standardeinstellung, die dem mutmaßlichen Willen der Mehrheit der

Nutzer widerspricht, nicht mit Art. 25 DSGVO vereinbar ist, ist selbstverständlich. Die Regelung des § 25 Abs. 2 Satz 3 DSGVO geht aber darüber hinaus und verbietet generell, dass personenbezogene Daten durch Voreinstellungen ohne Eingreifen der betroffenen Personen einer unbestimmten Zahl von Nutzern zugänglich gemacht werden. Das gilt also selbst dann, wenn die Mehrheit der Nutzer mutmaßlich mit einer solchen Veröffentlichung einverstanden wäre

bb) Zudem hat die Beklagte gegen die Schutzpflichten aus Art. 5f) und Art. 32 DSGVO verstoßen. Nach Art. 32 Abs. 1 DSGVO hat unter anderem der Verantwortliche unter Berücksichtigung des Standes der Technik und weiterer Gesichtspunkte die geeigneten technischen und organisatorischen Maßnahmen zu gewährleisten, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken durch unbefugte Offenlegung beziehungsweise unbefugten Zugang zu personenbezogenen Daten zu berücksichtigen. Die Bestimmung steht damit im Kontext zu dem in Art. 5f) DSGVO genannten Grundsatz der Datenverarbeitung, wonach diese so zu erfolgen hat, dass eine angemessene Sicherheit einschließlich eines Schutzes vor unbefugter Verarbeitung erfolgt (Sydow/Marsch DS-GVO/BDSG/Reimer, 3. Aufl. 2022, DS GVO Art. 5 Rn. 48).

Die Beklagte hat diese Vorgaben nicht eingehalten, indem sie zugelassen hat, dass Dritte in großem Umfang Telefonnummern mittels des Kontaktimportprogramms auf ihre Zuordnung zu vorhandenen Facebookprofilen überprüfen konnten. Der Beklagten oblag es darzulegen, dass sie die angemessenen Maßnahmen zum Schutz der Daten gegenüber einem solchen Vorgehen ergriffen hat. Zwar ist umstritten, ob die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO mit einer Übertragung der Beweislast auf den für die Verarbeitung der Daten Verantwortlichen einhergeht (so BeckOK DatenschutzR/Schantz, 44. Ed. 1.11.2021, DS-GVO Art. 5 Rn. 39 m.w.N.; entgegengesetzt Sydow/Marsch DS-GVO/BDSG/Reimer, 3. Aufl. 2022, DS GVO Art. 5 Rn. 56). Ungeachtet dessen ergibt sich aus Art. 5 Abs. 2 DSGVO jedenfalls eine auch prozessrechtlich relevante Vortragslast. Denn wenn diese Bestimmung die Beklagte verpflichtet, die Einhaltung der Grundsätze der personenbezogenen Datenverarbeitung des Art. 5 Abs. 1 DSGVO nachweisen zu können, so zwingt sie dies im Prozess zu einem Vortrag, der geeignet ist, als Nachweis für die Einhaltung der Vorgaben der Verordnung zu dienen. Eine zumindest sekundäre Darlegungslast folgt zudem aus dem Gesichtspunkt, dass die irische Datenschutzbehörde aufgrund des gleichen Vorfalls wegen Verstößen gegen Verpflichtungen der Datenschutzgrundverordnung ein Bußgeld gegen die Beklagte verhängt hat. Denn nach der zum Abgasskandal entwickelten Rechtsprechung des Bundesgerichtshofs stellt es in einem zivilrechtlichen Rechtsstreit ein Indiz für den vom Kläger vorgetragenen Pflichtverstoß dar, wenn die zuständige Fachbehörde (in jenen Fällen das Kraftfahrtbundesamt) den gleichen Sachverhalt

bereits als Pflichtverstoß beurteilt hat (BGH, Beschluss v. 4.5.2022 – VII ZR 733/21, Rn. 24 nach juris). Dem Autohersteller obliegt in einem solchen Fall eine sekundäre Darlegungslast zu den Hintergründen des Rückrufs und zur Rechtmäßigkeit seines Vorgehens. Er ist zwar auch in einem solchen Fall nicht zu einem Vorbringen gezwungen, insbesondere wenn er dies zum Schutz von Geschäftsgeheimnissen nicht für angezeigt hält, muss dann aber damit rechnen, den Prozess zu verlieren. Diese Erwägungen lassen sich auf den von der Datenschutzbehörde beanstandeten Verstoß übertragen.

Die Beklagte hat den von ihr geforderten Nachweis nicht erbracht. Ihrem Vorbringen lässt sich nicht entnehmen, dass und ggf. wie sie der Gefahr eines Missbrauchs des Kontaktimportprogramms durch Dritte begegnet ist. Es handelt sich dabei um eine durchaus naheliegende Gefahr, weil schon vor 2019 bekannt war, dass aktive E-Mailadressen und Telefonnummern im Internet illegal gehandelt werden. Die Beklagte hat zu ihrem Vorgehen vor dem Vorfall nur vorgetragen, dass sie die Übertragungsbeschränkungen innerhalb dieser Funktion gesenkt habe. Diesem Vorbringen lässt sich ein Nachweis, dass die Beklagte die angemessenen Maßnahmen zum Schutz der personenbezogenen Daten ergriffen hat, nicht entnehmen. Es ist nicht klar, wie hoch die Übertragungsbeschränkung lag, womit vermutlich ausgedrückt wird, welche Zahl an Datensätzen innerhalb einer bestimmten Zeit mittels des Kontaktimportprogramms überprüft werden konnte. Damit ist auch kein Rückschluss möglich, inwiefern die Maßnahme sich ex-ante betrachtet als angemessene Schutzmaßnahme darstellte. Die übrigen Maßnahmen, die die Beklagte im Hinblick auf einen Missbrauch des Kontaktimportprogramms ergriffen hat, erfolgten – so versteht das Gericht den Vortrag der Beklagten – erst nach dem streitgegenständlichen Vorfall. Ob die Beklagte darüber hinaus weitere Maßnahmen ergriffen hatte, die sich allgemein gegen Scraping, also das automatisierte Absuchen von Facebookprofilen, richteten, kann dahinstehen. Denn diese Maßnahmen waren jedenfalls nicht geeignet, die Verknüpfung nicht öffentlich einsehbarer Telefonnummern oder E-Mailadressen mit den öffentlich einsehbaren Profildaten über die Kontaktimportfunktion zu vermeiden.

cc) Ob die weiteren vom Kläger beanstandeten Vorgänge ebenfalls Pflichtverstöße der Beklagten darstellen, kann dahinstehen. Denn sie führen jedenfalls nicht zu einem weitergehenden Schaden als demjenigen, der bereits aufgrund der Veröffentlichung der Daten des Klägers im Darknet entstanden war. Weder eine frühere Information über den Vorfall nach dessen Feststellung noch eine weitergehende Auskunft zu den ausgelesenen Daten und den Tätern wäre geeignet gewesen, an diesem Umstand etwas zu ändern. Ein sonstiger Schaden durch diese behaupteten Pflichtverletzungen ist nicht ersichtlich.

b) Die genannten Pflichtverstöße begründen einen Schadensersatzanspruch nach Art. 82 DSGVO.

aa) Nach Art. 82 Abs. 1 DSGVO führt jeder Verstoß gegen die Verordnung der zu einem materiellen oder immateriellen Schaden geführt hat, zu einem Anspruch auf Schadensersatz gegen den Verantwortlichen. Zwar wird mit Rücksicht auf Art. 82 Abs. 2 DSGVO argumentiert, dass nur Schäden, die im Rahmen einer Verarbeitung entstanden seien, Gegenstand einer Ersatzpflicht nach Art. 82 DSGVO sein könnten (Sydow/Marsch DS-GVO/BDSG/Kreße, 3. Aufl. 2022, DS GVO Art. 82 Rn. 7; Gola/Heckmann/Gola/Piltz, 3. Aufl. 2022, DS-GVO Art. 82 Rn. 1; dagegen BeckOK DatenschutzR/Quaas, 44. Ed. 1.5.2023, DS-GVO Art. 82 Rn. 14). Dies überzeugt schon systematisch nicht, denn auch bei einem umfassenderen Verständnis der Haftungsgrundlage des Absatzes 1 hätte der Verordnungsgeber in Absatz 2 festlegen können, wie im Fall einer Verarbeitung die Haftung zwischen dem Verantwortlichen und dem Auftragsverarbeiter aufzuteilen ist. Die Streitfrage kann aber dahinstehen. Denn nach der Legaldefinition in Art. 4 Nr. 2 DSGVO ist der Begriff der Verarbeitung denkbar weit und umfasst alle beim Umgang mit Daten anfallenden Schritte wie unter anderem das Erheben, Erfassen und die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung. Damit sind die beanstandeten Vorgänge, nämlich die fehlerhafte Standardeinstellung beim Erfassen der Daten und die unzureichende Kontrolle bei deren Abfrage, Bestandteil der Verarbeitung.

bb) Der Umstand, dass die Telefonnummer des Klägers ohne dessen Willen im Darknet veröffentlicht wurde, stellt einen Schaden im Sinn des Art. 82 DSGVO dar. Die Bestimmung betrifft auch immaterielle Schäden, wobei sich dem Erwägungsgrund 85 der Datenschutzgrundverordnung entnehmen lässt, dass der Verordnungsgeber ausdrücklich den Kontrollverlust des Betroffenen hinsichtlich seiner persönlichen Daten als möglichen immateriellen Schaden ansah. Ob Art. 82 DSGVO eine Beschränkung auf erhebliche Schäden enthält, kann dahinstehen. Ein Ausschluss als Bagatellfall mag gerechtfertigt sein, wenn persönliche Daten an einzelne namentlich bekannte Personen gelangt sind. Die Veröffentlichung der Daten im Darknet, wo sie einer unbeschränkten Zahl an Personen für eine unbefugte Nutzung zur Verfügung stehen, stellt einen erheblichen Kontrollverlust dar, der eine etwaige Bagatellschwelle überschreitet.

cc) Die Verstöße der Beklagten gegen die Verordnung sind für den Schadenseintritt kausal geworden. Das gilt offenkundig für die Möglichkeit eines Missbrauchs des Kontaktimportprogramms. Denn ohne diese Möglichkeit hätten die Dritten die öffentlich nicht einsehbare Telefonnummer des Klägers nicht auslesen können. Es gilt aber auch für den

Verstoß gegen Art. 25 Abs. 2 Satz 3 DSGVO. Der Kläger hat glaubhaft vorgetragen, dass er sich nicht für eine Suchbarkeit über die Telefonnummer entschieden hätte, wenn ihm bewusst gewesen wäre, dass er insofern eine Wahlmöglichkeit besitzt, und wenn er hierfür hätte optieren müssen. Dies wird durch die (streitige) Behauptung der Beklagten, der Kläger habe durchgehend die Standardeinstellung für die Suche nach der Telefonnummer auf „alle“ beibehalten, selbst dann nicht entgegen, wenn sie zutreffen sollte. Denn nach der Veröffentlichung seiner Telefonnummer im Darknet bestand für den Kläger kein Grund mehr, zukünftig weiterhin eine Verknüpfung seiner Telefonnummer mit seinem Namen zu vermeiden.

dd) Nach Art. 82 Abs. 3 DSGVO obliegt es der Beklagten als Verantwortlicher für die Datenverarbeitung, sich von der Haftung zu befreien, indem sie nachweist, dass sie in keiner Weise für den eingetretenen Schaden verantwortlich ist. Ein solcher Nachweis ist ihr nicht gelungen. Insbesondere trifft den Kläger nicht unter dem Gesichtspunkt ein Mitverschulden, dass er bei umfassender Befassung mit den Datenschutzmöglichkeiten der Beklagten hätte erkennen können, dass er die Suchbarkeit über die Telefonnummer „durch alle“ abwählen konnte. Denn die Regelung des Art. 25 Abs. 2 Satz 3 DSGVO beruht gerade auf dem Gesichtspunkt, dass viele Nutzer nicht bereit sind, sich umfassend mit den Datenschutzeinstellungen zu befassen und deshalb die Standardeinstellungen beibehalten. Würde man hieraus ein Mitverschulden des Betroffenen herleiten, dann liefe die Regelung des Art. 25 Abs. 2 Satz 3 DSGVO auf der Sanktionsebene weitgehend leer.

ee) Die Höhe des Schadens bemisst das Gericht mit € 500,00. Dabei ist zu berücksichtigen, dass der Schaden allein darin besteht, dass die Telefonnummer des Klägers mit den bereits über sein Facebookprofil öffentlich bekannt gegebenen Daten verknüpft wurde. Dafür dass die Scraper neben der Telefonnummer an sonstige nicht öffentlich einsehbare Daten des Klägers gelangt sind, besteht kein Anhaltspunkt. Insbesondere sind die vom Kläger mitgeteilten im Intranet gespeicherten Daten außer der Telefonnummer im Profil öffentlich einsehbar gewesen. Bei der Bemessung des Schadens berücksichtigt das Gericht, dass der Kläger den eingetretenen Schaden dadurch aus der Welt schaffen kann, dass er sich eine neue SIM-Karte mit einer neuen Telefonnummer zulegt. Der damit verbundene Aufwand, der vor allem darin besteht, dass man einer Reihe von Bekannten die neue Telefonnummer mitteilen muss, begrenzt den Schaden nach oben. Da der Kläger die Telefonnummer nicht gewechselt hat, gewichtet er den durch die Veröffentlichung seiner Telefonnummer mit seinem Namen eingetretenen Schaden offenbar als geringer.

lll. Der auf Feststellung gerichtete Klagantrag zu 2. hat weitgehend Erfolg.

1. Der Antrag ist in dem tenorierten Umfang zulässig. Richtig ist zwar, dass der Antrag einen sprachlichen Widerspruch enthält, soweit er sich auf künftige Schäden bezieht, die bereits entstanden sind. Hinsichtlich der noch entstehenden, durch den im Klagantrag bezeichneten Vorfall verursachten Schäden ist der Klagantrag jedoch nicht widersprüchlich. Dem Kläger steht auch ein Feststellungsinteresse zu. Das Feststellungsinteresse nach § 256 Abs. 1 ZPO liegt bei einer Verletzung eines absoluten Rechts oder eines vergleichbaren Rechtsguts bereits dann vor, wenn künftige Schadensfolgen möglich sind, auch wenn der Eintritt eines Schadens noch ungewiss ist. Dies wäre nur dann nicht der Fall, wenn aus Sicht des Klägers bei verständiger Würdigung kein Grund bestünde, mit dem Eintritt eines Schadens wenigstens zu rechnen (BGH, Beschluss v. 9.1.2007 – VI ZR 13/06, MDR 2007, 792, Rn. 5 nach juris; Urteil v. 29.6.2021 – VI ZR 52/18, NJW 2021, 3130, Rn.30). Dies gilt insbesondere für Schäden, die auf einer Verletzung des allgemeinen Persönlichkeitsrechts beruhen (BGH, Urt. v. 29.6.2021, a.a.O.). Ein künftiger materieller Schaden ist möglich, etwa auf der Grundlage der vom Kläger angesprochenen betrügerischen Verwendung der veröffentlichten Daten oder einer Übertragung eines Virus auf sein Mobiltelefon über die im Internet veröffentlichte Nummer. Auch ein späterer, derzeit noch nicht absehbarer immaterieller Schaden ist denkbar, sofern beispielsweise die Belästigung durch Spam-Nachrichten künftig weit über das aktuell bekannte Maß hinausgeht. Dass der Kläger den Kausalzusammenhang zwischen einem späteren Schaden und dem im Jahr 2019 erfolgten Abgreifen seiner Daten nur schwer wird nachweisen können, ist für die Bejahung des Feststellungsinteresses nicht maßgeblich.

2. In dem gemäß vorstehender Ziff. III. 1. zulässigen Umfang ist der Feststellungsantrag auch begründet, da die Beklagte aus den oben genannten Gründen auch für etwaige künftige Schäden einstehen muss, die aus der Veröffentlichung der Telefonnummer des Klägers zusammen mit den von seinem Facebookprofil ausgelesenen Daten entstehen.

IV. Soweit es die mit dem Klagantrag zu 3. geltend gemachten Unterlassungsansprüche anbelangt, hat nur der mit dem Antrag zu 3a) verfolgten Unterlassungsanspruch Erfolg.

1. Der Klagantrag zu 3a) ist zulässig und in dem aus dem Tenor ersichtlichen Umfang begründet.

a) Der Antrag ist als Unterlassungsantrag statthaft. Soweit die Beklagte dem entgegenhält, dass der Antrag auf ein Handeln, nämlich auf die Einführung datenschutzrechtlicher Schutzmaßnahmen gerichtet ist, trifft dies nicht zu. Denn der Kläger beantragt nicht, die Beklagte

zu verpflichten, ein Kontaktimportprogramm mit den erforderlichen datenschutzrechtlichen Schutzmaßnahmen zu betreiben. Vielmehr steht es der Beklagten entsprechend dem Antrag zu 3.a) offen, ob sie ein solches Programm künftig einsetzt. Der Kläger möchte sie nur dazu verpflichten, ein solches Programm nicht einzusetzen, sofern sie nicht die technisch möglichen Schutzmaßnahmen verwendet.

Der Antrag ist auch hinreichend bestimmt. Nach der Rechtsprechung des Bundesgerichtshofs ist eine auslegungsbedürftige Antragsformulierung hinzunehmen, wenn dies zur Gewährleistung effektiven Rechtsschutzes erforderlich ist (BGH, Urt. v. 21.5.2015 – I ZR 183/13, GRUR 2015, 1237 Rn 13 m.w.N.; Urt. v. 26.1.2017 – I ZR 207/14, MDR 2017, 315, Rn. 18 nach juris). Das ist hier der Fall. Dem Kläger ist nicht zuzumuten, die nach dem Stand der Technik zu erbringenden Sicherheitsmaßnahmen zu konkretisieren. Dies ist ihm schon für die Gegenwart nicht möglich, weil er als Privatperson die dem Stand der Technik entsprechenden Sicherheitsmaßnahmen nicht kennt. Vor allem richtet sich aber das Unterlassungsbegehren gegen künftige Verstöße, für die weder der Kläger noch jemand anderes vorhersehen kann, welche technischen Maßnahmen dann geboten sein werden.

b) Der geltend gemachte Unterlassungsanspruch ergibt sich nicht unmittelbar aus Art. 17 DSGVO. Zwar kann sich aus dieser Bestimmung ein Unterlassungsanspruch ergeben (BGH, Urt. v. 27.7.2020 – VI ZR 405/18, BGHZ 226, 285, Rn. 17 nach juris). Dabei handelt es sich aber um einen Anspruch im Zusammenhang mit einer Löschung der Daten, die Art. 17 DSGVO eigentlich regelt. Eine solche wird vom Kläger jedoch nicht begehrt.

Rechtsgrundlage des Unterlassungsanspruchs ist jedoch §§ 823 Abs. 1, 1004 BGB analog. Danach kann bei Verletzung eines absoluten Rechts – wie es hier das Allgemeine Persönlichkeitsrecht darstellt, dem das Recht zur Kontrolle über die eigenen persönlichen Daten zuzuordnen ist – der Verletzte für die Zukunft eine Unterlassung der beanstandeten Handlung beanspruchen. Der Anspruch ist nicht durch die Bestimmungen der Datenschutzgrundverordnung gesperrt. Denn die Verordnung regelt die einer betroffenen Person zustehenden Rechtsbehelfe nicht abschließend. Vielmehr verpflichtet Art. 79 DSGVO, den Betroffenen wirksame gerichtliche Rechtsbehelfe zur Verfügung zu stellen.

Der Unterlassungsanspruch gilt aber nicht unbeschränkt. Der Kläger kann für die Zukunft nicht verlangen, dass die Beklagte, wie er es in seinem Klagantrag fordert, die nach dem Stand der Technik möglichen Maßnahmen vornimmt. Die mit der Sicherheit der Daten befassten Bestimmungen in Art. 5 f) DSGVO und Art. 32 DSGVO fordern nämlich jeweils nur, dass die

angemessenen Maßnahmen getroffen werden. Der Begriff der Angemessenheit erfordert, wie Art. 32 DSGVO zeigt, eine umfassende Abwägung, die nicht allein auf den Stand der Technik abstellt, sondern auch Gesichtspunkte wie die Schwere und Eintrittswahrscheinlichkeit des Risikos, aber auch die Umstände und Zwecke der Verarbeitung umfasst. Dementsprechend wird bei der Prüfung, ob eine Sicherheitsmaßnahme angemessen ist, auch zu berücksichtigen sein, inwiefern die jeweilige Maßnahme übliche Nutzungen des sozialen Netzwerks Facebook beeinträchtigt.

2. Dem Antrag zu 3.b) fehlt schon das Rechtsschutzbedürfnis. Der Kläger hat selbst vorgetragen, dass die Beklagte ihren Nutzern anbietet, die in der Vergangenheit übermittelten Telefonnummern aus ihrer Datenbank zu löschen. Ungeachtet der Frage, ob die Beklagte rechtmäßig die Telefonnummer des Klägers gespeichert hat, hätte er deshalb eine einfachere Möglichkeit gehabt, die künftige Nutzung seiner Telefonnummer zu unterbinden. Sofern der Kläger hingegen nunmehr in Kenntnis der von ihm behaupteten Mängel seiner ursprünglichen Einwilligung mit der Nutzung seiner Telefonnummer durch Facebook einverstanden ist, fehlt ihm ebenfalls ein Rechtsschutzbedürfnis für den Klagantrag zu 3b).

V. Der Auskunftsanspruch ist zwar teilweise zulässig, aber unbegründet. Soweit der Kläger mit dem Anspruch sämtliche seiner von der Beklagten verarbeiteten persönlichen Daten erfahren möchte, fehlt ihm das Rechtsschutzbedürfnis, weil er in seinem Profil nachsehen kann, welche Daten die Beklagte gespeichert hat und für wen diese sichtbar sind.

Im Übrigen ist der Auskunftsanspruch bereits erfüllt. Die Beklagte hat die verlangte Auskunft erteilt, indem sie mitgeteilt hat, dass unbekannte Täter Daten des Klägers ausgelesen haben und um welche Datengruppen es dabei geht. Ob die Beklagte den genauen Inhalt der ausgelesenen Datenfelder mitteilen müsste, kann dahinstehen, weil dieser dem Kläger nach seinem eigenen Vorbringen ohnehin bekannt ist.

Der Kläger macht mit der Klage sinngemäß geltend, dass die erteilte Auskunft insofern falsch sei, als die Täter der Beklagten bekannt sein müssten, weil sie angibt, gegen Scraper mit Unterlassungsaufforderungen vorzugehen. Dies überzeugt schon inhaltlich nicht, denn die Beklagte hat nicht erklärt, dass sie gegen jeden Scraper vorgehe. Ihr Vorbringen ist durchaus damit vereinbar, dass ihr einige Scraper bekannt werden, andere aber nicht. Im Übrigen ist dies für das Fortbestehen des Auskunftsanspruchs auch irrelevant, weil ein Auskunftsanspruch auch durch eine falsche Auskunft erfüllt wird. Zweifel an der inhaltlichen Richtigkeit der Auskunft begründen keinen Anspruch auf deren Ergänzung oder erneute Erteilung, sondern allenfalls einen Anspruch auf eidesstattliche Versicherung der erteilten Auskunft. Denn der Schuldner einer

Auskunftsverpflichtung soll nicht mit staatlichen Zwangsmitteln dazu gezwungen werden, die vom Gericht für richtig erachteten Angaben erklären zu müssen (BVerfG, Beschluss v. 28.10.2010 – 2 BvR 535/10, BVerfGK 18, 144).

Dementsprechend geht auch das Auskunftsverlangen, wie viele Täter die persönlichen Daten des Klägers abgerufen haben, ins Leere. Denn mit der Auskunft, dass die Daten durch unbekannte Täter erlangt wurden, hat die Beklagte bereits mitgeteilt, dass ihr die Anzahl der Täter nicht bekannt sei.

VI. Der zuerkannte Anspruch auf Zinsen auf den dem Kläger zugesprochenen immateriellen Schadensersatz-Betrag folgt aus §§ 291, 288 Abs. 1 BGB.

VII. Der geltend gemachte Anspruch auf Erstattung der vorgerichtlichen Kosten steht dem Kläger unter dem Gesichtspunkt des Schadensersatzes nach Art. 82 DSGVO dem Grunde nach zu; der Höhe nach ist der Anspruch nur teilweise begründet. Ersetzt verlangen kann der die vorgerichtlichen anwaltlichen Kosten nur in Höhe einer 1,3-Gebühr nebst Kommunikationspauschale und Umsatzsteuer nach demjenigen Gegenstandswert, der anzusetzen wäre, wenn der Kläger allein die – gemäß den obigen Ausführungen – berechtigten Ansprüche geltend gemacht hätte. Denn nur hinsichtlich der berechtigten Ansprüche ist die Erforderlichkeit der vorgerichtlichen anwaltlichen Anspruchsverfolgung zu bejahen. Die darüber hinausgehende Anspruchsverfolgung war hingegen nicht erforderlich.

Der bezüglich des zugesprochenen Erstattungsanspruchs zuerkannte Zinsanspruch folgt aus §§ 291, 288 Abs. 1 BGB.

VIII. Die Kostenentscheidung beruht auf § 92 Abs. 1 ZPO. Die Entscheidung über die vorläufige Vollstreckbarkeit folgt aus §§ 708 Nr. 11, 709, 711 ZPO.
Die Streitwertentscheidung ergeht nach § 63 Abs. 2 GKG i.V.m. § 48 GKG, 3 ZPO.

Vorsitzender Richter am Landgericht

Für die Richtigkeit der Abschrift
Hamburg, 17.06.2024

JAng
Urkundsbeamtin der Geschäftsstelle