

Landgericht Bayreuth

Az.: 31 O 40/23



IM NAMEN DES VOLKES

In dem Rechtsstreit



- Kläger -

Prozessbevollmächtigte:

Rechtsanwälte **Wilde Beuger Solmecke**, Rechtsanwälte Partnerschaft mbB, Kaiser-Wilhelm-Ring 27-29, 50672 Köln, Gz.: 7093/22 maz


gegen

Meta Platforms Ireland Limited, vertreten durch den Geschäftsführer (Director) Gareth Lambe, ebenda, (zuvor Facebook Ireland Ltd.), 4 Grand Canal Square, Dublin 2, Irland, Irland
- Beklagte -

Prozessbevollmächtigte:

Rechtsanwälte **Freshfields Bruckhaus Deringer**, Rechtsanwälte Steuerberater PartG mbB, Bockenheimer Anlage 44, 60322 Frankfurt, Gz.: 169638-0036 MCM/AMO/jma

wegen Persönlichkeitsrechtsverletzung

erlässt das Landgericht Bayreuth - 3. Zivilkammer - durch den Vorsitzenden Richter am Landgericht  als Einzelrichter aufgrund der mündlichen Verhandlung vom 27.03.2023 folgendes

Endurteil

1. Die Beklagte wird verurteilt, an den Kläger 100,00 € nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit 14.02.2023 sowie weitere 83,54 € nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit 14.02.2023 zu zahlen.

Im Übrigen wird die Klage abgewiesen.

2. Der Kläger hat die Kosten des Rechtsstreits zu tragen.

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

Beschluss

Der Streitwert wird auf 5.500,00 € festgesetzt.

Tatbestand

Gegenstand des Rechtsstreits sind DSGVO-Ansprüche aus dem sogenannten „Facebook-Scraping“ im Jahr 2018.

Die Beklagte ist die für europäische Nutzer zuständige Betreiberin der social-media-Plattform Facebook. Der Kläger unterhielt ein Benutzerkonto.

Für jeden Nutzer sind dort persönliche Daten für Mitglieder der Plattform abrufbar gespeichert, insbesondere der Vor- und Nachname, Alter, Geschlecht, Land und eine Nutzer-ID; welche weiteren Daten (etwa Beziehungsstatus, Religionszugehörigkeit oder „Schuhgröße des Mathematiklehrers“) enthalten sind, ist weitgehend dem Nutzer überlassen, der sein Profil für seine sozialen Kontakte ausgestaltet.

Es ist technisch möglich, automatisiert aus der Anzeige des Nutzerprofils die enthaltenen persönlichen Daten auszulesen und zu einem Datensatz zusammenzuführen (scraping). Nach den Nutzungsbedingungen der Beklagten ist dies allerdings untersagt.

Eine Mobiltelefonnummer und/oder eine E-Mail-Adresse hingegen wird von der Beklagten unabhängig davon abgefragt und insbesondere für die Identifikation des berechtigten Nutzers verwendet. Es ist dem Nutzer jedoch möglich, diese auch in das öffentliche Profil einzustellen.

Es ist auch möglich, von einem anderen Benutzerkonto aus den Nutzer (dessen Profil) zu finden, wenn diese Daten, insbesondere die Mobiltelefonnummer bekannt sind (Contact Importer Tool). Dies ermöglicht insbesondere dem Nutzer eines Mobiltelefons, schnell andere Facebook-Nutzer unter den im Telefon gespeicherten Kontakten zu finden. Diese Funktion konnte zwar deaktiviert werden, war aber voreingestellt aktiviert.

Im Jahr 2019 war es unter Ausnutzung dieser Funktion außerdem möglich, durch einen bru-

te-force-Angriff die Telefonnummer eines Nutzers zu ermitteln, auch wenn der Nutzer diese nicht ins Profil eingestellt hatte, bzw. für eine beliebige Telefonnummer ein etwa zugeordnetes Nutzerkonto zu finden (dessen für Mitglieder des Dienstes der Beklagten einsehbare Daten dann gescraped und mit der Telefonnummer zusammengeführt wurden). Dies geschah automatisiert millionenfach, die so zusammengeführten Daten wurden von Dritten zum Kauf angeboten.

Die Beklagte änderte danach die Funktion. Die Nutzer informierte sie erst April 2021 (B12).

Die irische Datenschutzbehörde hat wegen des Handlings der Telefonnummern beim Importieren von Kontakten ein Bußgeld gegen die Beklagte verhängt und ihr aufgegeben, geeignete Maßnahmen zur künftigen Vermeidung zu treffen. Die Entscheidung wird von der Beklagten gerichtlich angefochten.

Der Kläger behauptet, bei der Beklagten ein Nutzerkonto unterhalten zu haben (K6). Dem entsprechend sei er auch bei den gescrapten Datensätzen zu finden.

Zum Schadensersatz- und Unterlassungsanspruch stützt sich der Kläger einerseits auf insgesamt nicht transparente Informationen der Beklagten darüber, welche Daten gegenüber welchen anderen Nutzern des Dienstes bzw. „öffentlich“ bereitgehalten werden und mit welchen Optionen dies hätte beeinflusst werden können; zum anderen darauf, dass die Beklagte keine nach damaligem Stand der Technik zumutbare Maßnahmen gegen „scraping“ und die Ermittlung der verknüpften Telefonnummer getroffen habe.

Er erhalte seit April 2021 auch deutlich mehr beunruhigende Phishing E-Mails und SMS.

Der Kläger beantragt:

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 künftigen Schäden zu ersetzen, die der Klägerseite durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte,

entstanden sind und/oder noch entstehen werden.

3. Die Beklagte 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 Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird.

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

Die Beklagte beantragt, die Klage abzuweisen.

Die Beklagte meint, ihre Informationen zur Konfiguration und Verwendung der Daten seien verständlich und übersichtlich, soweit Daten außerhalb der Telefonnummer gescraped worden seien, sei dem Kläger kein ersichtlicher Schaden entstanden, nachdem er alle diese Daten selbst veröffentlicht habe.

Sie habe auch Maßnahmen gegen Scraping und gegen die Ermittlung der Telefonnummer getroffen, diese Maßnahmen seien aber nicht vorhersehbar umgangen worden. Insbesondere handele es sich nicht um eine Sicherheitslücke, da von vornherein vorgesehen war, dass mit einer Telefonnummer auf ein Benutzerprofil lesend zugegriffen werden (das Benutzerprofil gefunden werden) kann.

Das Gericht hat keinen Beweis erhoben. Auf den Akteninhalt wird Bezug genommen.

Entscheidungsgründe

Die zulässige Klage ist nur zum geringen Teil begründet. Dem Kläger ist durch das Handeln der Beklagten immaterieller Schaden entstanden, zu dessen Ersatz das Gericht einen Betrag von 100 € als angemessenen Ausgleich schätzt. Die weiter in der Hauptsache geltend gemachten Ansprüche sind nicht gegeben.

1. Der Kläger ist aktiv legitimiert. Als Nachweis dafür, dass er ein Konto bei der Beklagten unterhalten hat, hat der Kläger einen Abzug der von ihm bei der Beklagten gespeicherten Daten vorgelegt. Diese enthalten für Facebook-Profilen typische Angaben über persönliche Vorlieben etc., so dass das Gericht vom Klägervortrag überzeugt ist. Die Beklagte hat auch die ergänzenden Angaben des Klägers zu seiner Benutzererkennung nicht mehr substantiiert bestritten.

2. Ein Schadensersatzanspruch oder Unterlassungsanspruch für vom Profil ausgelesene Daten ist nicht gegeben, weil der Beklagten hinsichtlich der gescrapten Daten kein Verstoß gegen die DSGVO zur Last gelegt werden kann. Welche Daten auf dem Profil eines Benutzers auslesbar sind, bestimmt zum einen der Benutzer selbst, zum andern und wesentlich kann er dies bei der Betrachtung seines Profils selbst überprüfen und Daten wieder herausnehmen, die er nicht veröffentlicht sehen will.

Dabei ist insbesondere zu berücksichtigen, dass es gerade die Funktion des Dienstes der Beklagten ist, die vom Kläger selbst zur Verfügung gestellten Daten im Mitgliederkreis der Plattform zu verbreiten. Dass die Beklagte hier eine nicht für jeden übersichtliche Vielzahl von Funktionen und Konfigurationseinstellungen anbietet, um der Vielfalt sozialer Beziehungen ihrer Benutzer gerecht zu werden, ist für ein soziales Netzwerk immanent und kann der Beklagten nicht zur Last gelegt werden. Bereits an dieser Stelle muss auch festgehalten werden, dass ein materieller oder immaterieller Schaden für einen Benutzer, der weiterhin sein Konto bei der Beklagten unterhält und die auf seinem Profil einsehbaren Daten weiterhin an Dritte übermitteln lässt, kaum vorliegen kann.

3. Eine Verletzung der DSGVO und damit ein Anspruch kann von vornherein nur vorliegen, soweit eine Verknüpfung der – nicht auf dem Profil veröffentlichten – Mobiltelefonnummer mit den restlichen Profildaten stattfand. (so auch die von Klägerseite vorgelegte Entscheidung des irischen Datenschutzbeauftragten).

a) Allerdings ist auch hier zu berücksichtigen, dass die Mobiltelefonnummer vom Kläger selbst eingetragen worden sein muss, insbesondere auch zu dem Zweck, dass Dritte sein Profil über diese Mobiltelefonnummer ermitteln. Soweit die Klage das in Abrede stellt, zitiert sie selbst (auf Seite 15 oben) einen Text der Beklagten, in dem explizit benannt wird, dass die Mobilnummer auch verwendet werden kann, damit andere „auf Facebook nach dir suchen“ können.

Die Einwilligung des Betroffenen ist allerdings naturgemäß auf diejenigen Personen beschränkt, die die Mobiltelefonnummer bereits kennen, nicht auf solche Personen, die Nummern oder Nummernkreise gezielt durchprobieren, um erst zu ermitteln, ob und gegebenenfalls welche natürliche Person Anschlussinhaber einer solchen Nummer ist.

b) Ob die Beklagte wirksame Vorkehrungen hiergegen zu treffen hatte und ob solche wirksamen Vorkehrungen überhaupt möglich sind, kann dahinstehen. Jedenfalls aber hatte sie eine informierte Entscheidung ihrer Nutzer über die Möglichkeit einer solchen Rückwärtssuche zu ermöglichen.

Freilich ist hier die Beklagte dazu berufen, es einen potentiellen Angreifer nicht so leicht zu machen. Es ist der Beklagten aber andererseits nicht zuzumuten, den Zugriff der Benutzer auf ihre gerade dem Austausch von Informationen dienende Plattform erheblich zu erschweren. Das setzt von vornherein enge Grenzen für Sicherheitsmaßnahmen gegen die unbefugte Ausnutzung von Funktionen, die Benutzern gerade zur Verfügung stehen sollen (wie hier der Telefonnum-

mernsuche). Captcha z.B. können von KI-Anwendungen gelöst werden, obwohl sie insbesondere sehbehinderten Benutzern große Schwierigkeiten bereiten.

Die Beklagte hat aber vorgetragen, in den verwendeten Algorithmus sowohl zeitliche Beschränkungen für die Anzahl der Zugriffe mit verschiedenen Nummern als auch Captcha eingebaut zu haben. Die Klage stützt sich hier im wesentlichen auf eine ex post - Betrachtung ohne auszuformulieren, welchen Grad an Sicherheitsmaßnahmen sie für 2019 für nötig – und zumutbar – gehalten hätte.

Gleichwohl vermisst der Vortrag der Beklagten eine einlassungsfähige Schilderung des Stands der Technik 2019 und insbesondere eine Schilderung der Maßnahmen, die sie zur Vermeidung eines Brute-force-Angriffs getroffen hatte. Dabei ist zu berücksichtigen, dass der zuständige Datenschutzbeauftragte festgestellt hat, dass die Beklagte nicht alle ihr möglichen Sicherungsmaßnahmen unternommen hat. Letztendlich kann das dahinstehen.

c) Ohne weiteres überzeugend ist nämlich die zweite Feststellung des zuständigen Datenschutzbeauftragten dahingehend, dass die Beklagte Art. 25 Abs. 2 DSGVO verletzt hat, indem sie die Rückwärtssuche über die Telefonnummer als Voreinstellung vorgab, was gegen den Grundsatz verstößt, die Voreinstellungen datenschutzfreundlich zu gestalten. Die Beklagte musste daher dem Benutzer für die Möglichkeit der Telefonnummernsuche ein Opt-In, nicht aber ein Opt-Out anbieten. Dem kann sich das Gericht in eigener Prüfungskompetenz zur vollen Überzeugung anschließen. Auf die Rechtskraft der Entscheidung kommt es deshalb nicht an.

d) Zu dem ihm entstandenen Schaden hat der Kläger nachvollziehbar vorgetragen, dass sich bei ihm im Anschluss an den April 2021 Phishing E-Mails und – SMS häuften und er dadurch belästigt wurde. Die Beklagte ist dem auch nicht ausdrücklich entgegengetreten, sondern hat sich nur darauf zurückgezogen, dass dies auch andere Ursachen haben kann. Sicher ist es so, dass Phishing E-Mails etc. mehr oder weniger jeden erreichen; der Beweis des ersten Anscheins spricht jedoch dafür, dass sie zunehmen, wenn – wie hier – entsprechende Datensätze veröffentlicht werden. Sicher ist es unmöglich, zu rekonstruieren, welcher Anteil an zunehmenden Phishing E-Mails beim Kläger auf den Verstoß der Beklagten zurückzuführen sind, dass es ein gewisser Anteil ist, kann jedoch nach dem gewöhnlichen Lauf der Dinge als sicher angenommen werden.

e) Zur Schadenshöhe ist allerdings zu berücksichtigen, dass es die Geschädigten ohne weiteres in der Hand hatten, immateriellen Schaden dadurch abzuwenden, dass sie eine andere Mobiltelefonnummer beantragten. Dies ist nach Schätzung des Gerichts – einschließlich der Zeit die benö-

tigt wird, um die neue Telefonnummer dem im vorliegenden Fall kleinen Kreis der Kontakte bekanntzumachen – mit ca. 100 € Kosten verbunden gewesen. Der Kläger macht nämlich gerade nicht geltend, dass seine Mobiltelefonnummer geschäftlich genutzt und einem großen Kreis Dritter bekannt gemacht werden muss, ein solcher Vortrag wäre andererseits mit der Annahme eines Schadens des Klägers durch das Bekanntwerden der Nummer unvereinbar. Der vom Kläger erlittene zusätzliche Belästigungsschaden kann nur auftreten, wenn eine Mobiltelefonnummer öffentlich wird, die vorher nicht „außerhalb eines kleinen Kreises von Freunden“ bekannt war.

Auf diesen Betrag von 100 Euro ist aufgrund der Obliegenheit des Klägers zur Schadensminimierung auch die Höhe eines immateriellen Schadens zu begrenzen. Aufgrund der potenziell hohen Anzahl der Anspruchsteller handelt es sich auch um eine für die Beklagte durchaus fühlbare Sanktion.

4. Darüber hinaus sind zukünftige Schäden nicht ersichtlich.

5. Unterlassungsansprüche (§ 1004 BGB analog) können nicht mit Erfolg geltend gemacht werden, weil eine Wiederholungsgefahr für einen im Kern gleichen Verstoß fehlt. Grundsätzlich kann aus einem Verstoß zwar auf die Gefahr der Wiederholung geschlossen werden, die Vermutung entfällt jedoch, wenn die Störung auf einer einmaligen Sondersituation beruht hat oder sich die Umstände, auf die sie fußt, grundlegend ändern (BeckOGK/Spohnheimer BGB § 1004 Rn. 269.7 m.w.N)

So liegt der Fall hier. Der zum Bekanntwerden der klägerischen Telefonnummer führende Vorfall hat sich 2018 ereignet. Die Vorkehrungen der Beklagten haben sich seitdem vielfach verändert, ebenso das Vorgehen eventueller Angreifer. Aufgrund der Schnelllebigkeit im IT-Sicherheitsbereich ist der Angriffsvektor längst überholt und ein kerngleicher Verstoß nicht mehr zu besorgen.

Es kann daher dahinstehen, ob der Kläger nicht rechtsmissbräuchlich einen Unterlassungsanspruch geltend macht, wenn er das zu unterlassende Verhalten selbst durch eine einfache Konfigurationsänderung abstellen kann, jedenfalls nachdem ihm diese spätestens im Lauf des Prozesses bekannt geworden ist.

Dahinstehen kann auch, ob eine Anordnung der irischen Datenschutzbehörde – analog zu den Gepflogenheiten im Wettbewerbsrecht – Unterlassungsansprüche Dritter ausschließt. Nachdem die Beklagte derzeit Rechtsmittel führt, wäre das ohnehin nicht der Fall.

6. Einen Auskunftsanspruch kann der Kläger nur geltend machen für Daten, die die Beklagte kennt und verarbeitet.

Die Beklagte hat vorgetragen, dass sie dem Kläger bereits Auskunft über die vorhandenen Daten erteilt hat, darauf hat der Kläger nicht mehr substantiiert erwidert. Gerichtsbekannt hält die Beklagte Funktionen bereit, die es den Nutzern ihre Plattform ermöglichen, die von ihr verarbeiteten Daten einzusehen und zu überprüfen. Das indessen ist gerade nicht der Streitgegenstand.

Darüber, welche Daten ihr ohne ihr Zutun abhandengekommen sind, kann die Beklagte – über den dem Kläger bekannten Eintrag in der gescannten Datei hinaus – typischerweise keine Angaben machen. Zugriffslogs aus dem Jahr 2018 sollten schon aus Rechtsgründen nicht mehr gespeichert sein. Ultra posse nemo obligatur.

6. Außergerichtliche Kosten sind bei einem Streitwert von unter 300 € gerechtfertigt in Höhe von Euro 83,54.

8. Nebenentscheidungen: §§ 286, 288 BGB, §§ 3, 91, 92 II, 709 ZPO.

Rechtsbehelfsbelehrung:

Gegen die Entscheidung, mit der der Streitwert festgesetzt worden ist, kann Beschwerde eingelegt werden, wenn der Wert des Beschwerdegegenstands 200 Euro übersteigt oder das Gericht die Beschwerde zugelassen hat.

Die Beschwerde ist binnen **sechs Monaten** bei dem

Landgericht Bayreuth
Wittelsbacherring 22
95444 Bayreuth

einzulegen.

Die Frist beginnt mit Eintreten der Rechtskraft der Entscheidung in der Hauptsache oder der anderweitigen Erledigung des Verfahrens. Ist der Streitwert später als einen Monat vor Ablauf der sechsmonatigen Frist festgesetzt worden, kann die Beschwerde noch innerhalb eines Monats nach Zustellung oder formloser Mit-

teilung des Festsetzungsbeschlusses eingelegt werden. Im Fall der formlosen Mitteilung gilt der Beschluss mit dem dritten Tage nach Aufgabe zur Post als bekannt gemacht.

Die Beschwerde ist schriftlich einzulegen oder durch Erklärung zu Protokoll der Geschäftsstelle des genannten Gerichts. Sie kann auch vor der Geschäftsstelle jedes Amtsgerichts zu Protokoll erklärt werden; die Frist ist jedoch nur gewahrt, wenn das Protokoll rechtzeitig bei dem oben genannten Gericht eingeht. Eine anwaltliche Mitwirkung ist nicht vorgeschrieben.

Rechtsbehelfe können auch als **elektronisches Dokument** eingereicht werden. Eine einfache E-Mail genügt den gesetzlichen Anforderungen nicht.

Rechtsbehelfe, die durch eine Rechtsanwältin, einen Rechtsanwalt, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht werden, sind **als elektronisches Dokument** einzureichen, es sei denn, dass dies aus technischen Gründen vorübergehend nicht möglich ist. In diesem Fall bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig, wobei die vorübergehende Unmöglichkeit bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen ist. Auf Anforderung ist das elektronische Dokument nachzureichen.

Elektronische Dokumente müssen

- mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein oder
- von der verantwortenden Person signiert und auf einem sicheren Übermittlungsweg eingereicht werden.

Ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen ist, darf wie folgt übermittelt werden:

- auf einem sicheren Übermittlungsweg oder
- an das für den Empfang elektronischer Dokumente eingerichtete Elektronische Gerichts- und Verwaltungspostfach (EGVP) des Gerichts.

Wegen der sicheren Übermittlungswege wird auf § 130a Absatz 4 der Zivilprozessordnung verwiesen. Hinsichtlich der weiteren Voraussetzungen zur elektronischen Kommunikation mit den Gerichten wird auf die Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (Elektronischer-Rechtsverkehr-Verordnung - ERVV) in der jeweils geltenden Fassung sowie auf die Internetseite www.justiz.de verwiesen.

gez.

■

Vorsitzender Richter am Landgericht

Verkündet am 22.06.2023

gez.

■, JHSekr

Urkundsbeamter der Geschäftsstelle



Für die Richtigkeit der Abschrift
Bayreuth, 26.06.2023

■■■■■, JHSekr
Urkundsbeamter der Geschäftsstelle