FS–PP Berlin
Part mbB

Dr. iur. Rainer Frank
Rechtsanwalt · Fachanwalt für Strafrecht
Compliance Officer (Steinbeis)
Compliance Auditor (TÜV)

Dr. iur. Niklas Auffermann
Rechtsanwalt · Fachanwalt für Strafrecht
Mediator

Dr. iur. Sebastian T. Vogel
Rechtsanwalt · Fachanwalt für Strafrecht
Healthcare Compliance Officer (HCO)

Dr. iur. David Albrecht
Rechtsanwalt · Fachanwalt für Strafrecht

Dr. iur. Leonie Lo Re
Rechtsanwältin · Fachanwältin für Strafrecht
Compliance Officer (Steinbeis)
Compliance Auditor (TÜV)

Dr. iur. Michael Liedke
Rechtsanwalt

Fabian Breuer
Rechtsanwalt
Compliance Officer (Steinbeis)

Dr. iur. Viktor Volkmann, LL.M. (TCD)
Rechtsanwalt
Compliance Officer (Steinbeis)

Dr. iur. Laura Seifert
Rechtsanwältin

Sophia Hoffmeister
Rechtsanwältin

Lisa Engelbrecht
Rechtsanwältin

Potsdamer Platz 8 · 10117 Berlin

Telefon 030/31 86 85-3
Telefax 030/31 86 85-55
E-Mail mail@fs-pp.de

www.fs-pp.de

AG Chlbg. – PR 994 B

20.07.2023
50.23

per beA
Amtsgericht Passau
94032 Passau

In dem Rechtsstreit

[redacted]

– Kläger –

Prozessbevollmächtigte: FS-PP Berlin Part mbB, Potsdamer Platz 8, 10117 Berlin

gegen

[redacted]

– Beklagte –

wegen: Unterlassung der „Chatkontrolle“

vorläufiger Streitwert: EUR 5.000,00

erheben wir namens und in Vollmacht des Klägers

Klage

und beantragen:

1. **Die Beklagte wird dazu verurteilt, es zu unterlassen, den Inhalt und die näheren Umstände von mittels „Facebook-Messenger“ von und an den Kläger versandten Nachrichten zur Suche nach möglicherweise rechtswidrigen Inhalten oder Kontaktaufnahmen automatisiert zu analysieren, zu kontrollieren und an Dritte weiterzugeben.**

2. **Für jeden Fall der Zuwiderhandlung gegen den Antrag zu 1. wird der Beklagten ein Ordnungsgeld bis zu 250.000 Euro, ersatzweise Ordnungshaft bis zu sechs Monaten, zu vollstrecken an ihren jeweiligen Vorständen, angedroht.**

Begründung:

Den weiteren Ausführungen wird folgende Gliederung vorangestellt.

A. Sachverhalt

Die Beklagte ist eine in Irland ansässige Tochtergesellschaft des US-amerikanischen Technologieunternehmens Meta Platforms, Inc., dem unter anderem die sozialen Netzwerke „Facebook“ und „Instagram“ sowie die Nachrichtenübermittlungsapps „WhatsApp“ und „Messenger“ gehören.

Ausweislich des Impressums der deutschen Facebook-Seite (www.facebook.de) werden

> „[d]*ie Websites unter www.facebook.com und die Dienste auf diesen Seiten* […] *angeboten von: Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Irland“.* (Impressum und Nutzungsbedingungen deutscher Facebook-Seite als **Anlage K1**)

Die Beklagte ist daher Vertragspartnerin der Nutzer von Facebook in Deutschland sowie in der gesamten europäischen Region und datenschutzrechtlich verantwortlich für die Verarbeitung personenbezogener Daten dieser Nutzer.

Der Kläger ist Nutzer der von der Beklagten bereitgestellten Internet-Plattform Facebook und unterhält dort eine Profil-Seite. Neben der Möglichkeit, ein Profil zu erstellen und Inhalte auf der dazugehörigen Pinnwand öffentlich zu teilen, wird den Nutzern die Möglichkeit eingeräumt, mit einer anderen Person oder ausgewählten Personengruppe über die „Facebook-Messenger“-Dienste unter Ausschluss Dritter privat zu kommunizieren. Beim Messenger handelt es sich um eine in Facebook integrierte Chatfunktion, die aber auch über eine separate App zugänglich ist.

Die Beklagte selbst bewirbt ihren Messenger-Dienst mit den Worten:

> *„privat, sicher und vertraulich“* (Datenschutz- und Sicherheitsrubrik der Messenger-Seite als **Anlage K2**)

Der Kläger nutzt den angebotenen Messenger-Dienst, sowohl über die Facebook-Website als auch über die Messenger-App, und kommuniziert so über diesen ausschließlich im privaten Kontext. Aufgrund der eigenen Missbrauchserfahrungen des Klägers ist die Vertraulichkeit seiner Kommunikation für ihn von herausgehobener Bedeutung.

Die Beklagte führt automatisierte Kontrollen der Chatverläufe über ihre Messenger-Dienste durch. In Nr. 1 Unterabschnitt 5 der Nutzungsbedingungen heißt es dazu u.a.:

> *„Wir beschäftigen weltweit spezielle Teams, arbeiten mit externen Dienstleistern, Partnern und anderen relevanten Unternehmen zusammen und entwickeln fortschrittliche technische Systeme, um potenziellen Missbrauch unserer Produkte, schädliches Verhalten gegenüber anderen und Situationen aufzudecken, in denen wir möglicherweise dazu beitragen können, unsere Gemeinschaft zu unterstützen und zu schützen, u. a. indem wir auf Nutzermeldungen von potenziell unzulässigen Inhalten reagieren."* (Impressum und Nutzungsbedingungen, **Anlage K1**)

Sie untersucht die private Kommunikation unabhängig von einem vorher bestehenden Verdacht auf „Muster", die nach Einschätzung der Beklagten darauf hindeuten, dass Kommunikation im Zusammenhang mit Kinderpornografie oder der Anbahnung sexueller Kontakte zu Minderjährigen stehen könnte („Chatkontrolle"). Die Untersuchung zielt dabei vor allem auf die Entdeckung von CSA-Material und Grooming ab. CSA-Material umfasst alle Inhalte, die sexuellen Kindesmissbrauch darstellen (englischer Originalausdruck „Child sexual abuse material"). „Grooming" (deutsch sinngemäß „Anbahnung") bezeichnet die gezielte Kontaktaufnahme zu Minderjährigen durch Erwachsene, um sexuellen Kontakt anzubahnen. Werden solche „Muster" festgestellt, leitet die Beklagte die Daten intern und an private Organisationen oder Strafverfolgungsbehörden weiter:

> *„Wir teilen Daten mit anderen Meta-Unternehmen, wenn wir Missbrauch oder schädliches Verhalten durch eine Person feststellen, die eines unserer Produkte nutzt, oder um die Meta-Produkte, Nutzer und die Community zu schützen. Wir geben beispielsweise Informationen an Meta-Unternehmen weiter, die finanzielle Produkte und Dienstleistungen anbieten, um ihnen dabei zu helfen, Schutz, Sicherheit und Integrität zu fördern und geltendes Recht einzuhalten. Meta kann auf jegliche Informationen, die es über dich erfasst, zugreifen, sie aufbewahren, verwenden und teilen, wenn es in gutem Glauben der Ansicht ist, dass dies gesetzlich vorgeschrieben oder zulässig ist. Weitere Informationen erhältst du in unserer Datenrichtlinie."* (Nr. 1 Unterabschnitt 5 der Nutzungsbedingungen, **Anlage K1**)

Auf der deutschen Internetseite des Messenger-Dienstes unter dem Reiter „Datenschutz und Sicherheit" ist zudem ausgeführt:

> *„Wenn wir von potenziellem Missbrauch in unseren Diensten erfahren, werden wir aktiv. Wir setzen dazu unsere Gemeinschaftsstandards durch und teilen Informationen mit dem NCMEC* [National Center for Missing and Exploited Children] *und den entsprechenden Strafverfolgungsbehörden.* […] *Wir verwenden außerdem maschinelles Lernen, um Konten zu erkennen und zu deaktivieren, die auf unangemessene Weise mit Kindern interagieren."* (Datenschutz- und Sicherheitsrubrik der Messenger-Seite, **Anlage K2**)

Weitere Details, wie die genaue Funktionsweise der Kontrollen der Beklagten, legt diese nicht offen.

Generell bekannt ist jedoch der Umstand, dass die technischen Systeme zur Erkennung der „Muster" fehleranfällig sind. Die Europäische Kommission selbst geht in einem Bericht zur geplanten verpflichtenden „Chatkontrolle" (aktuelles Vorhaben, siehe COM/2022/209 final) von einer Fehlerquote von 10 % aus (auf

www.netzpolitik.org veröffentlichter Bericht der Kommission, S. 13 als **Anlage K3**).

Zudem spricht eine von „netzpolitik.org“ veröffentlichte Studie des Europäischen Parlamentarischen Forschungsdienstes (EPRS) von April 2023 zu der geplanten Einführung einer verpflichtenden „Chatkontrolle“ den aktuellen Technologien zur Durchführung einer „Chatkontrolle“ die Fähigkeit ab, neues CSA-Material und Grooming zuverlässig zu erkennen. So führt sie aus:

> Originalfassung:
>
> *„At this point in time, detecting new* [CSA] *material and grooming results in substantial amounts of false positives and false negatives and, in particular, the accuracy levels of the tools used to detect grooming can be considered insufficiently accurate to be deployed on a large scale. The detection would, moreover, require cultural and context-sensitive technologies to identify grooming accurately, which are currently not sufficiently developed. Technologically, the detection of CSAM in E2EE* [End-to-end encryption] *communications is possible but the solutions available are not sufficiently transparent and secure, and known detection mechanisms undermine the end-to-end protection offered by the encryption.* […] *It is unlikely that technologies to detect CSAM in E2EE communications develop rapidly to reach high accuracy levels in the upcoming 2 to 5 years, without undermining the secure nature of E2EE communications and the security at the end devices. The same conclusion can be drawn with regard to the technologies that could identify new CSAM or grooming in E2EE communications.“* (Studie des EPRS, Punkt 3, S. 1 als **Anlage K4**)
>
> Deutsche Übersetzung der Unterzeichner:

> *„Zum gegenwärtigen Zeitpunkt führt die Erkennung von neuem* [CSA] *Material und Grooming zu einer beträchtlichen Anzahl von falsch-positiven und falsch-negativen Ergebnissen, und insbesondere der Genauigkeitsgrad der zur Erkennung von Grooming verwendeten Instrumente kann als nicht genau genug angesehen werden, um in großem Maßstab eingesetzt zu werden. Die Erkennung würde außerdem kulturelle und kontextabhängige Technologien zur genauen Identifizierung von Grooming erfordern, die derzeit nicht ausreichend entwickelt sind. Technologisch ist die Erkennung von CSAM in der E2EE* [Ende-zu-Ende-Verschlüsselung] *- Kommunikation möglich, aber die verfügbaren Lösungen sind nicht transparent und sicher genug, und die bekannten Erkennungsmechanismen untergraben den durch die Verschlüsselung gebotenen Ende-zu-Ende-Schutz.* […] *Es ist unwahrscheinlich, dass sich Technologien zur Erkennung von CSAM in der E2EE-Kommunikation so schnell entwickeln, dass sie in den nächsten 2 bis 5 Jahren ein hohes Maß an Genauigkeit erreichen, ohne die Sicherheit der E2EE-Kommunikation und die Sicherheit der Endgeräte zu untergraben. Die gleiche Schlussfolgerung kann in Bezug auf die Technologien gezogen werden, die neue CSAM oder Grooming in der E2EE-Kommunikation identifizieren könnten.“*

Eine menschliche Überprüfung vorausgewählter Inhalte bleibt deshalb weiterhin notwendig. Aufgrund der Fehlerrate ist davon auszugehen, dass die Beklagte automatisiert herausgefilterte Inhalte vor der Weiterleitung an Dritte (vor allem Strafverfolgungsbehörden und das NCMEC) durch Menschen überprüft und diese dabei Kenntnis von dem Inhalt der privaten Nachrichten nehmen.

B. Rechtliche Würdigung

Die Klage ist zulässig und begründet.

I. Zulässigkeit der Klage

Die Klage ist zulässig. Insbesondere ist das Amtsgericht sachlich gemäß § 25 Nr. 1 GVG i.V.m. §§ 2, 3, 5 ZPO zuständig. Der Streitwert liegt für alle Klageanträge zusammen jedenfalls nicht über 5.000 Euro. Nach § 3 ZPO erfolgt die Streitwertfestsetzung durch das Gericht nach freiem Ermessen (Prütting/Gehrlein/*Beumers*, ZPO, 14. Aufl. 2022, § 3 Rn. 1).

Bezüglich des Unterlassungsantrags zu 1. als nichtvermögensrechtlichem Streitgegenstand sind in Anlehnung an die Regelung in § 48 Abs. 2 S. 1 GKG zum Gebührenstreitwert alle Umstände des Einzelfalls hinsichtlich der Bedeutung der Sache für den Kläger zu berücksichtigen (OLG Frankfurt, Urt. v. 14.04.2022 – 3 U 21/20, Rn. 71, zit. nach juris; OLG Stuttgart, Beschl. v. 03.01.2023 – 4 AR 4/22, Rn. 26, zit. nach juris). In dieser Sache ist vor allem der Umstand zu würdigen, dass lediglich die rein private Kommunikation des Klägers im Zweipersonenverhältnis eines kostenlosen Messenger-Dienstes betroffen ist.

II. Begründetheit der Klage

Dem Kläger steht gegen die Beklagte ein Anspruch auf Unterlassung der Durchführung einer automatisierten Analyse, Kontrolle und Weitergabe an Dritte des Inhalts und der näheren Umstände von mittels „Facebook-Messenger“ (sowohl über den Browser als auch über die App) versandten Nachrichten von und an den Kläger zur Suche nach möglicherweise rechtswidrigen Inhalten oder Kontaktaufnahmen zu.

1. Anspruch auf Unterlassung der „Chatkontrolle“

Dem Kläger steht gegen die Beklagte ein Anspruch auf Unterlassung der Durchführung einer automatisierten Analyse, Kontrolle und Weitergabe an Dritte des Inhalts und der näheren Umstände von mittels „Facebook-Messenger“ versandten Nachrichten von und an den Kläger zur Suche nach möglicherweise rechtswidrigen Inhalten oder Kontaktaufnahmen gemäß dem Klageantrag zu 1. zu.

a. Anspruch auf Unterlassung nach § 1004 Abs. 1 S. 2 BGB analog i.V.m. § 823 Abs. 1 BGB

Der Anspruch des Klägers auf Unterlassung gemäß dem Klageantrag zu 1. folgt zunächst aus § 1004 Abs. 1 S. 2 BGB analog i.V.m. § 823 Abs. 1 BGB. Die „Chatkontrollen“ der Beklagten beeinträchtigen das allgemeine Persönlichkeitsrecht des Klägers in rechtswidriger Weise.

aa. Beeinträchtigung des allgemeinen Persönlichkeitsrechts, Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG

Die Durchführung von anlasslosen „Chatkontrollen“ in privaten Nachrichtenaustauschen über den Messenger-Dienst durch die Beklagte beeinträchtigt das allgemeine Persönlichkeitsrecht des Klägers aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG.

(1) Abstrakt-generelle Erwägungen

Das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG kennt verschiedene Ausprägungen seiner Schutzrichtung, unter anderem das Recht auf informationelle Selbstbestimmung. Dieses Recht garantiert dem Einzelnen, selbstständig über die Preisgabe oder Verwendung seiner personenbezogenen Daten zu entscheiden. Insbesondere schützt es vor intransparenter Verarbeitung und Nutzung der Daten durch Dritte (BGH, Urt. v. 29.06.2021 – VI ZR 52/18, Rn. 21, zit. nach juris; BGH, Urt. v.

14.12.2021 – VI ZR 403/19, Rn. 12, zit. nach juris). Das umfasst den Schutz davor, dass Dritte Daten in nicht nachvollziehbarer Weise als Instrument nutzen, um die Betroffenen auf Eigenschaften, Typen und Profile festzulegen, auf die sie keinen Einfluss haben, die aber für eine freie Entfaltung der Persönlichkeit von erheblicher Bedeutung sind (BGH, Urt. v. 29.06.2021 – VI ZR 52/18, Rn. 21, zit. nach juris; BGH, Urt. v. 14.12.2021 – VI ZR 403/19, Rn. 12, zit. nach juris).

Die Intensität von Eingriffen in das allgemeine Persönlichkeitsrecht und mithin auch in das Recht auf informationelle Selbstbestimmung differenziert sich nach den betroffenen Schutzsphären. Am schwersten wiegt ein Eingriff in die absolut geschützte Intimsphäre, danach folgt die Privatsphäre und letztlich die Sozialsphäre. Die Intimsphäre bildet den Raum persönlichster Wünsche, Gedanken und Kommunikation des unantastbaren Kernbereichs privater Lebensgestaltung ab, die dem Zugriff oder der Kenntnis Dritter absolut entzogen sein sollen. Dieser Eingriff kann nicht gerechtfertigt werden (zum Ganzen BGH, Urt. v. 25.10.2011 – VI ZR 332/09, Rn. 11, zit. nach juris). Die Privatsphäre meint einen Bereich autonomer Lebensführung, in dem der Einzelne seine Individualität unter Ausschluss anderer entwickeln und wahrnehmen kann, was das Recht umfasst, für sich zu sein und den Einblick durch andere auszuschließen. (BGH, Urt. v. 25.10.2011 – VI ZR 332/09, Rn. 15, zit. nach juris; BGH, Urt. v. 14.12.2021 – VI ZR 403/19, Rn. 14, zit. nach juris). Der Schutz umfasst Angelegenheiten, die wegen ihres Informationsgehalts typischerweise als „privat“ eingestuft werden (BGH, Urt. v. 14.12.2021 – VI ZR 403/19, Rn. 14, zit. nach juris).

(2) Subsumtion in concreto

Gemessen an diesen Maßstäben ist die anlasslose „Chatkontrolle“ der Beklagten in ihrem Messenger-Dienst als Beeinträchtigung des allgemeinen Persönlichkeitsrechts einzuordnen.

Die Kommunikation via Messenger erfolgt in einem festgelegten Personenkreis. Die Kommunikationspartner haben sich explizit dazu entschieden, die Inhalte nicht öffentlich auf ihrer Facebook-

Seite mit einem größeren, je nach Privatsphäre-Einstellung gar unbestimmten Personenkreis zu teilen, sondern zum Gegenstand einer privaten Konversation über den Messenger-Dienst gemacht. Dies entspricht gerade auch der Kernfunktion des Messengers, die ausweislich der Werbung der Beklagten in der privaten und vertraulichen Kommunikation liegt. Die Inhalte dieser Kommunikation sind deshalb zumindest der Privatsphäre zuzuordnen.

Je nach Inhalt der Konversation ist aber auch die Betroffenheit der Intimsphäre denkbar. Dabei ist zu berücksichtigen, dass sich Kommunikationspartner mittlerweile in zunehmendem Maße Messenger-Diensten für intime Gespräche bedienen (z.B. sogenanntes „Sexting“) und diese nicht mehr ausschließlich im Rahmen gleichzeitiger körperlicher Anwesenheit erfolgen. Insofern ist die Durchführung einer „Chatkontrolle“ mit dem Öffnen und vorsorglichen Scannen von persönlichen oder intimen Briefen vergleichbar. Dass beispielsweise Liebesbriefe mit intimen Inhalten dem unantastbaren Kernbereich privater Lebensgestaltung, also der Intimsphäre zuzuordnen sind, hat die Rechtsprechung bereits entschieden (LG Frankfurt, Teilurt. v. 21.12.2017 – 2-03 O 130/17, Rn. 92 ff., zit. nach juris). Im Zeitalter digitaler Medien, in dem Messenger-Nachrichten Briefe − wie allgemein bekannt − überwiegend abgelöst haben, kann nichts Anderes gelten, ohne dass man das Schutzniveau empfindlich absenkte.

Durch die anlasslose „Chatkontrolle“ der Beklagten wird eine vertrauliche Kommunikation unmöglich. Unabhängig von einer konkreten Verdachtslage wird die Kommunikation durch die Beklagte analysiert. Vermeintliche Treffer werden an Dritte (Unternehmen von Meta oder NCMEC) übermittelt, weshalb es zur Weitergabe personenbezogener Daten kommt. Dies ist kritisch zu sehen, da die Wahrung des europäischen Datenschutzniveaus bei der Übermittlung in die USA höchst fraglich erscheint. So hat der EuGH in seinem Schrems II-Urteil den Durchführungsbeschluss zum Privacy Shield, der ein angemessenes Schutzniveau personenbezogener Daten in den USA feststellte (DSS-Beschluss), für unwirksam erklärt:

> *„Daher hat die Kommission bei ihrer Feststellung in Art. 1 Abs. 1 des DSS-Beschlusses, dass die Vereinigten Staaten für personenbezogene Daten, die im Rahmen des EU-US-Datenschutzschilds aus der Union an Organisationen in diesem Drittland übermittelt würden, ein angemessenes Schutzniveau gewährleisteten, die Anforderungen verkannt, die sich aus Art. 45 Abs. 1 der DSGVO im Licht der Art. 7, 8 und 47 der Charta ergeben. Daraus folgt, dass Art. 1 des DSS-Beschlusses mit Art. 45 Abs. 1 der DSGVO, ausgelegt im Licht der Art. 7, 8 und 47 der Charta, unvereinbar und somit ungültig ist.“* (EuGH, Urt. v. 16.07.2020 − C-311/18, Rn. 198 f., zit. nach juris)

Erschwerend tritt hinzu, dass diese Weitergabe keineswegs nur bei eindeutig strafbaren Inhalten erfolgt. Die eingesetzten Systeme weisen eine hohe Fehleranfälligkeit auf, sodass fälschlicherweise als strafbar klassifizierte Inhalte und damit anlasslos rein private Kommunikation an Dritte weitergeleitet wird. Dieser Umstand wiegt besonders schwer, da insbesondere der Intimsphäre zugehörige, absolut geschützte Nachrichten (vor allem Sexting) aufgrund der verwendeten Worte und/oder versandten Dateien von der fälschlichen Herausfilterung durch den Algorithmus der „Chatkontrolle“ betroffen sein dürften.

Letztlich hat der Bundesgerichtshof − wie oben dargelegt − klargestellt, dass das Recht auf informationelle Selbstbestimmung auch die Transparenz des Umgangs und der Verwendung personenbezogener Daten schützt. Im Widerspruch hierzu legt die Beklagte die genaue Funktionsweise ihrer „Chatkontrolle“ nicht offen. Für die Nutzer des Messengers, somit auch für den Kläger, ist vollkommen unklar, nach welchen Logiken ihre eigentlich privaten und teilweise intimen Nachrichten gescannt, an Dritte weitergegeben sowie durch Menschen manuell gesichtet werden.

bb. Rechtswidrigkeit der „Chatkontrolle“

Die Durchführung der „Chatkontrolle“ als Beeinträchtigung des allgemeinen Persönlichkeitsrechts ist rechtswidrig. Die Beeinträchtigung entbehrt eines Rechtfertigungsgrundes. Weder die Verordnung (EU) 2021/1232 (im Folgenden: „Übergangs-VO“) gewährt eine Rechtsgrundlage für die von der Beklagten ausgeübte „Chatkontrolle“ (dazu (1)), noch ist sie nach Art. 6 Abs. 1 DS-GVO als rechtmäßig einzuordnen (dazu (2)). Überdies steht die mit der „Chatkontrolle“ verbundene Rechtsverletzung in einem unangemessenen Verhältnis zu ihrem Zweck (dazu (3)).

(1) Übergangs-VO keine Rechtsgrundlage

Die Übergangs-VO ist wegen ihrer unverhältnismäßigen Einschränkung der Grundrechte ungültig und soll überdies keine Rechtsgrundlage für die Kontrolle und Analyse privater Nachrichten wie die „Chatkontrolle“ der Beklagten darstellen.

(a) Ungültigkeit der Übergangs-VO

Die Übergangs-VO ist ungültig. Sie greift in unverhältnismäßiger Weise in die Grundrechte der EU-Grundrechtecharta ein.

(aa) Eingriff in Art. 7 und 8 GRCh

Die Übergangs-VO erkennt in ihrem 8. Erwägungsgrund ausdrücklich an, dass die „Chatkontrolle“ in das Grundrecht auf Achtung des Privat- und Familienlebens und der Vertraulichkeit der Kommunikation (Art. 7 GRCh) sowie das Grundrecht auf Schutz personenbezogener Daten (Art. 8 GRCh) eingreift.

(bb) Eingriff in Art. 11 GRCh

Darüber hinaus begründet die „Chatkontrolle“ einen Eingriff in Art. 11 GRCh, der die Freiheit, Informationen ohne behördliche Eingriffe zu empfangen und weiterzugeben, schützt. Argumentativ können in diesem Zusammenhang EuGH-Urteile aus der Urheberrechtsprechung zur ähnlichen Diskussion um Upload-Filter herangezogen werden. Im Rahmen der Problematik des sogenannten „Overblockings“, das heißt der Herausfilterung auch zulässiger Inhalte, hat der EuGH ausgeführt:

> *„Zum anderen könnte die fragliche Anordnung* [, ein Filtersystem einzurichten,] *die Informationsfreiheit beeinträchtigen, weil die Gefahr bestünde, dass das System nicht hinreichend zwischen einem unzulässigen und einem zulässigen Inhalt unterscheiden kann, so dass sein Einsatz zur Sperrung von Kommunikationen mit zulässigem Inhalt führen könnte.“* (EuGH, Urt. v. 16.02.2012 – C-360/10, Rn. 50, zit. nach juris)

Diesen Grundsatz hat der EuGH in einem späteren Urteil nochmals klargestellt:

> *„In diesem Zusammenhang ist darauf hinzuweisen, dass der Gerichtshof bereits festgestellt hat, dass ein* ***Filtersystem, bei dem die Gefahr bestünde, dass es nicht hinreichend zwischen einem unzulässigen Inhalt und einem zulässigen Inhalt unterscheidet****, so dass sein Einsatz zur Sperrung von Kommunikationen mit zulässigem Inhalt führen könnte,* ***mit dem in Art. 11 der Charta verbürgten Recht auf freie Meinungsäußerung und Informationsfreiheit unvereinbar*** *wäre und das angemessene Gleichgewicht zwischen ihm und dem Recht des geistigen Eigentums nicht beachten würde.“* (EuGH, Urteil vom 26.04.2022 − C-401/19, Rn. 86, zit. nach juris, Hervorh. nicht im Original)

Dieses Herausfiltern zulässiger Inhalte ist übertragbar auf die fälschliche Erkennung von CSAM oder Grooming durch die „Chatkontrolle“. Nun hat der EuGH in diesen Urteilen unmissverständlich klargestellt, dass Filtersysteme, die falsch-positive Treffer herausfiltern, mit Art. 11 GRCh unvereinbar sind. Nach den obigen Erläuterungen existieren für den Bereich der „Chatkontrollen“ zur Erkennung von CSAM und Grooming aber noch keine technischen Systeme, die fehlerfrei funktionieren. Um keinen nicht zu rechtfertigenden Verstoß gegen Art. 11 GRCh durch die „Chatkontrolle“ zu verursachen, müsste mithin zur Sicherstellung der Herausfilterung und Weiterleitung an Dritte eine menschliche Kontrolle erfolgen. Sollte sich die Beklagte also mit dem Hinweis verteidigen – der freilich nachzuweisen wäre –, dass keine menschliche Überprüfung bei der „Chatkontrolle“ stattfinde, so räumte sie implizit aufgrund der derzeitigen Schwäche technischer Systeme einen Verstoß gegen Art. 11 GRCh ein.

(cc) Eingriff in das Berufsgeheimnis

Letztlich greift die Übergangs-VO in das Berufsgeheimnis ein, da die Kommunikation über elektronische Dienste nicht mehr vertraulich ist. Das Berufsgeheimnis ist in einem Rechtsstaat unabdingbar und dient speziell bezogen auf Anwälte der Verwirklichung des Anspruchs auf ein faires Verfahren inklusive einer Verteidigung (Art. 6 EMRK), des Rechts auf einen wirksamen Rechtsbehelf inklusive der Beratung, Verteidigung und Vertretung (Art. 47 GRCh), der Umsetzung des Rechtsstaatsgebotes, der Verwirklichung des Anspruchs auf rechtliches Gehör, dem Schutz des allgemeinen Persönlichkeitsrechts des Mandanten und des Rechts auf Achtung des Privatlebens (Art. 8 EMRK und Art. 7 GRCh). All diese Gewährleistungen des Berufsgeheimnisses werden durch die „Chatkontrolle“ mithin ebenfalls beeinträchtigt.

Insbesondere das Berufsgeheimnis, unter anderem von Anwälten und Journalisten, ist durch die Übergangs-VO bedroht. Der Erwägungsgrund Nr. 27 führt zwar aus, dass die Verordnung nationale Vorschriften zum Berufsgeheimnis unberührt lässt und erkennt die

zentrale Bedeutung der Vertraulichkeit der Kommunikation zwischen Anwälten und Mandanten oder Journalisten und ihren Quellen an. Im Verordnungstext selbst findet sich aber keine Regelung, die derartige Kommunikation wiederum von der Suspendierung ausnimmt.

Vor allem drei Fallkonstellationen sind im Hinblick auf die „Chatkontrolle“ problematisch: Die anwaltliche Vertretung von Opfern von Kindermissbrauch; die abstrakte anwaltliche Beratung zum Schutz vor Kindermissbrauch und die anwaltliche Verteidigung von Beschuldigten in diesem Bereich. In allen drei genannten Konstellationen ist ein Bruch der Vertraulichkeit denkbar. Die Kommunikation in Mandatsverhältnissen erfolgt heutzutage auf vielfältigen Wegen. Mandanten nutzen für die Korrespondenz mit ihren Anwälten E-Mail-Dienste wie Gmail, Messenger-Dienste wie WhatsApp, Videokonferenzdienste wie Microsoft Teams und eine Vielzahl weiterer digitaler Kanäle. Da die Übergangs-VO keine Ausnahme für verschlüsselte Kommunikationsinhalte vorsieht, ist selbst die Nutzung von „Krypto-Messengern“ kein geeignetes Mittel, um den Schutz des Mandatsgeheimnisses zu bewahren.

Das Berufsgeheimnis muss dabei schon auf der Ebene der Datenerhebung in Gestalt der Auswertung der Kommunikationsinhalte einen wirksamen Schutz erfahren. Denn bereits die inhaltliche Analyse der Kommunikationsdaten stellt einen Eingriff dar, der durch eine Übermittlung an Behörden und sonstige Dritte intensiviert, aber nicht erst begründet wird. Die Notwendigkeit ausreichender Schutzmechanismen entfällt auch nicht dadurch, dass die Datenanalyse nicht von staatlichen Stellen, sondern von Unternehmen der Privatwirtschaft durchgeführt wird. Die Übergangs-VO soll es Telekommunikationsanbietern ermöglichen, eigene Maßnahmen zur Verhütung und Verfolgung von Straftaten im Internet umzusetzen und identifizierte „Treffer“ an Behörden zu übermitteln. Darin liegt eine weitere Form der „Auslagerung“ staatlicher Aufgaben im Bereich der Verbrechensbekämpfung auf Privatunternehmen, die dem Trend der Zeit entspricht, die es aber erforderlich macht, ausreichende Schutzvorkehrungen bereits auf der Ebene der zweckgerichteten Datenerhebung durch die betreffenden privaten Stellen zu implementieren.

Dem kann auch nicht entgegengehalten werden, dass Kommunikationsinhalte, die dem Berufsgeheimnis unterliegen, aus technischen Gründen nicht zuverlässig identifiziert werden können. Ist es, wovon die Übergangs-VO ausgeht, technisch möglich, bestimmte inkriminierte Inhalte durch den Einsatz von künstlicher Intelligenz zu ermitteln, ist es nicht einsichtig, warum entsprechendes nicht auch in Bezug auf rechtlich privilegierte Inhalte möglich sein soll. Sollte die jeweils verwendete Analysesoftware tatsächlich nicht in der Lage sein, zu schützende Kommunikationsinhalte zuverlässig auszusondern, stellt dies nicht die Notwendigkeit des Berufsgeheimnisschutzes infrage, sondern offenbart nur die Ungeeignetheit der Software, eine rechtlich beanstandungsfreie Auswertung sicherzustellen.

(dd) Verletzung Verhältnismäßigkeitsgrundsatz

Die Übergangs-VO ist insgesamt als unverhältnismäßig zu werten. Sie ist nicht geeignet ihren Zweck zu erfüllen und zudem stehen die hervorgerufenen Grundrechtsbeeinträchtigungen außer Verhältnis zu ihrem angestrebten Zweck.

Gemäß Art. 15 Abs. 1 der RL 2002/58/EG („ePrivacy-Richtlinie“) können Mitgliedsstaaten Rechtsvorschriften zur Beschränkung der Rechte und Pflichten aus Art. 5 (Vertraulichkeit der Kommunikation) und Art. 6 (Pflichten im Umgang mit Verkehrsdaten) ePrivacy-Richtlinie erlassen, wenn dies für die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten notwendig sowie angemessen und verhältnismäßig ist. Im 11. Erwägungsgrund der ePrivacy-Richtlinie wird klargestellt, dass eine derartige Maßnahme in einem „strikt“ angemessenen Verhältnis zum intendierten Zweck stehen muss. Überdies gilt der allgemeine Verhältnismäßigkeitsgrundsatz für Unionshandlungen gemäß Art. 5 Abs. 4 EUV.

Die Übergangs-VO ist schon nicht zur Erreichung ihres Ziels geeignet. Art. 1 Abs. 1 Übergangs-VO benennt als ihr Ziel die Aufdeckung, Meldung und Entfernung von Online-Material sexuellen Missbrauchs von Kindern bei Anbietern nummernunabhängiger interpersoneller Kommunikationsdienste. Dieses Ziel ist ein zentrales

Anliegen der Gesellschaft und stets ein legitimer Zweck. Aber legitime Zwecke können nur durch geeignete Maßnahmen erreicht werden. Die freiwillige „Chatkontrolle“ trägt nicht zum effektiven Kinderschutz bei – im Gegenteil: Sie kann ihn gar behindern.

Zunächst dämmt die „Chatkontrolle“ die Verbreitung kinderpornographischen Materials nicht ein. Das liegt maßgeblich zum einen daran, dass Missbrauchstäter sowie Konsumenten Material oft nicht über kommerzielle E-Mail- oder Messenger-Dienste verbreiten, austauschen bzw. beziehen, sondern über selbst betriebene geheime Foren (vgl. hierzu *Woerlein,* ZD-Aktuell 2022, 01251). Selbst wenn über kommerzielle Dienste Links zu entsprechenden Foren oder Mediendateien versendet werden, erkennen die Algorithmen der Beklagten diese nicht. Zum anderen erkennen die Algorithmen neues CSAM nur schwer (dazu A.).

Hinzu tritt, dass die automatisierte „Chatkontrolle“ zu einer Masse von Meldungen wegen des Verdachts auf CSAM führt und dies zumindest teilweise an die Strafverfolgungsbehörden weitergeleitet wird. Eine große, von den Behörden im Moment nicht bewältigbare Menge an Meldungen entsteht, die die Ermittlungen in den relevanten Fällen behindern können. Die Studie des EPRS führt hierzu aus:

> *„An increase in the quantity of reported content may not necessarily result in an equivalent increase in investigations and prosecutions, and, thus, better protection of children. As long as the capacity of LEAs* [Law enforcement agencies] *is limited to its current size, an increase in reporting will make effective investigation of CSAM more difficult.“* (Studie des EPRS, Punkt 3, S. 2, **Anlage K4**
>
> Deutsche Übersetzung der Unterzeichner:
>
> *„Eine Zunahme der gemeldeten Inhalte führt nicht unbedingt zu einer entsprechenden Zunahme der Ermittlungen und der Strafverfolgung und damit zu einem besseren Schutz der Kinder. Solange die Kapazität der Strafverfolgungsbehörden auf ihren derzeitigen Umfang*

beschränkt ist, wird eine Zunahme der Meldungen eine effektive Untersuchung von CSAM erschweren."

Ein Großteil der herausgefilterten Inhalte betrifft Nachrichten von Minderjährigen untereinander, die einvernehmlich intime Bilder austauschen (sogenanntes Sexting), die die Algorithmen als CSAM erkennen. So ergab eine Sonderauswertung des Bundeskriminalamtes aus der Polizeilichen Kriminalstatistik (PKS) von 2022, dass von den Tatverdächtigen wegen der Verbreitung, des Erwerbs, Besitzes und der Herstellung kinderpornografischer Inhalte nach § 184b StGB über das Tatmittel Internet 42 Prozent unter 18 Jahre alt waren (Sonderauswertung PKS 2022 als **Anlage K5**). Diese Fälle betreffen mehrheitlich also keinen Kindesmissbrauch, sondern einvernehmliches Verhalten. Bedenklicherweise führt die Herausfilterung dieser Inhalte zu der Kenntnisnahme durch Mitarbeiter der Beklagten, des NCMEC oder der Ermittlungsbehörden, obwohl diese intimen Bilder nur für den Kommunikationspartner bestimmt waren.

Als Veranschaulichung der nicht zu bewältigenden Menge der Hinweise an Strafverfolgungsbehörden seien exemplarisch Daten von 2019 dargestellt. 2019 meldete das NCMEC an deutsche Ermittlungsbehörden circa 62.000 Hinweise auf Kinderpornografie, aus denen sich 21.600 Fälle ergaben, die das Bundeskriminalamt (BKA) mit dem Ziel bearbeitete, Ermittlungsverfahren einzuleiten (Pressekonferenz BKA, Vorstellung der Zahlen kindlicher Gewaltopfer – Auswertung der PKS 2019 vom 11.05.2020, S. 2, als **Anlage K6**). Laut der PKS 2019 (Auszug aus dem PKS Jahrbuch 2019 als **Anlage K7**) wurden dann aber insgesamt von den Ermittlungsbehörden lediglich 12.262 Fälle von Kinderpornografie nach § 184b StGB erfasst, d.h. die von NCMEC und alle auf anderen Wegen gemeldete oder bekannt gewordene Fälle zusammen. Auch im Vorjahr 2018 meldete das NCMEC an das BKA 70.000 Hinweise (**Anlage K6**, S. 2). Bei dieser anhaltend großen Zahl von Hinweisen im Vergleich zu den Ermittlungskapazitäten der Ermittlungsbehörden können Ermittlungen bezüglich aller Verdachtsfälle nicht gewährleistet werden. Dabei entscheidet gerade die Aufdeckungs- und Verurteilungswahrscheinlichkeit über die Existenz eines Abschreckungseffekts der Strafandrohung wegen des Verbreitens, Erwerbs und Besitzes von Kinderpornographie nach § 184b StGB (vgl. nur *Kreuzer*,

KriPoZ 2020, 263, 265). Die hohe Anzahl an Hinweisen dürfte diese Wahrscheinlichkeit gerade nicht erhöhen und damit auch das Schutzniveau nicht.

Einen wertvollen, nachweisbaren Beitrag zur Zielerreichung des Kinderschutzes kann die „Chatkontrolle“ folglich nicht leisten.

Überdies und besonders schwer wiegt, dass die „Chatkontrolle“ in keinem angemessenen Verhältnis zur Schwere der durch sie hervorgerufenen Grundrechtsbeeinträchtigungen steht. Der EuGH hat der anlasslosen Speicherung von Verkehrs- und Standortdaten durch Telekommunikationsanbieter enge Grenzen gesetzt. Anlässlich der Vorratsdatenspeicherung hat er den allgemeinen Grundsatz aufgestellt, dass eine allgemeine und unterschiedslose Speicherung von Verkehrs- und Standortdaten durch Telekommunikationsanbieter im Grundsatz unzulässig und nur ausnahmsweise unter spezifischen Voraussetzungen und unter Gewährleistung ausreichender prozessualer Sicherungen erlaubt ist. Entsprechende Rechtsvorschriften müssen durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen (EuGH, Urt. v. 6.10.2020 – C-511/18, C-512/18, C-520/18, Rn. 138, zit. nach juris; EuGH, Urt. v. 20.09.2022 – C-793/19, Rn. 69, zit. nach juris).

Eine automatisierte Analyse von Verkehrs- und Standortdaten ist aufgrund ihrer besonderen Eingriffsintensität nach der Rechtsprechung des EuGH nur dann gerechtfertigt, wenn sie auf Situationen „einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit“ beschränkt ist oder ein konkreter Verdacht terroristischer Aktivitäten der Betroffenen besteht. In beiden Fällen ist eine hinreichend wirksame gerichtliche oder behördliche Kontrolle zu gewährleisten (EuGH, Urt. v. 6.10.2020 – C-511/18, C-512/18, C-520/18, Rn. 137, zit. nach juris; EuGH, Urt. v. 20.09.2022 – C-793/19, Rn. 72, zit. nach juris).

Diese Grundsätze sind auch auf Fälle freiwilliger Datenverarbeitung durch Private übertragbar, da es aus Sicht der Kommunikationsteilnehmer keinen Unterschied macht, ob eine Datenverarbeitung durch einen Diensteanbieter aufgrund einer rechtlichen Verpflichtung erfolgt oder nicht. Die Intensität der mit der Verarbeitung verbundenen Grundrechtseingriffe und damit das Schutzbedürfnis der Nutzer ändert sich dadurch nicht. Sofern der Staat also sein Strafverfolgungsmonopol lockert und Private mit der Aufdeckung strafbaren Verhaltens im Internet betraut, muss er ausreichende Kontroll- und Schutzmechanismen installieren, um das Schutzniveau nicht abzusenken oder den Grundrechtsschutz für bestimmte Bereiche gänzlich zu suspendieren.

Die Übergangs-VO sieht die vom EuGH angemahnten Sicherungsgarantien nicht vor und bleibt daher weit hinter den Vorgaben des EuGH zur Vorratsdatenspeicherung zurück. Die in der Verordnung vorgesehene anlasslose und massenhafte Auswertung auch von Kommunikationsinhalten und deren Meldung an Behörden stellen besonders schwere Eingriffe in die Vertraulichkeit von Kommunikation dar, die erheblich über die bisher diskutierten Maßnahmen der Vorratsdatenspeicherung hinausgehen. Die anlasslose und umfassende Analyse von Inhaltsdaten und deren Übermittlung an staatliche Stellen im Fall echter oder vermeintlicher „Treffer“ führt letztlich zu einer vollständigen Aufhebung der Vertraulichkeit elektronischer Kommunikation. Bereits die inhaltliche Auswertung von Kommunikationsdaten stellt unabhängig von einer späteren Übermittlung an Dritte einen erheblichen Eingriff in Grundrechte dar, der einer Rechtfertigung bedarf.

Intensiviert werden die Grundrechtseingriffe noch dadurch, dass den Diensteanbietern eine Datenanalyse mittels künstlicher Intelligenz erlaubt ist. Diese Art der Auswertung birgt spezielle Risiken für die Betroffenen, weil die Richtigkeit der Auswertungsergebnisse von der Ausgestaltung der Analysesoftware, insbesondere der Bezeichnung der Indikatoren abhängt. Insoweit bestehen aber erhebliche Zweifel daran, dass Art. 3 der Verordnung sicherstellt, dass die Diensteanbieter ausreichend zuverlässige Software zum Einsatz bringen. Die Vorgaben bleiben hier denkbar vage („bewährte Tech-

nik“, „hinreichend zuverlässig“, „geeigneter Indikatoren wie Schlüsselwörter und objektiv ermittelte Risikofaktoren“). Darüber hinaus enthält die Vorschrift unzureichende und unklare Regelungen hinsichtlich der Datenverwendung. So sollen Diensteanbieter beispielsweise berechtigt sein, identifizierte Inhalte an „Strafverfolgungsbehörden und andere einschlägige Behörden“ zu übermitteln. Welche Stellen unter die letztgenannte Kategorie fallen, ist völlig unklar.

(ee) Zwischenfazit: Ungültigkeit der Verordnung

Die Übergangs-VO ist zusammenfassend als ungültig zu werten und ist von vorneherein nicht geeignet, der „Chatkontrolle“ der Beklagten eine Rechtsgrundlage zu bieten.

(ff) Anregung: Vorlage an EUGH

Der Kläger regt aufgrund der dargelegten Ungültigkeit der Übergangs-VO eine Vorlage an den EuGH zu der Entscheidung über die Ungültigkeit gemäß Art. 267 Abs. 1 lit. b AEUV an (vgl. dazu EuGH, Urt. v. 22.10.1987 − C-314/85 – „Foto-Frost“).

Der Kläger schlägt vor, die Vorlagefrage wie folgt zu formulieren:

> „Verstößt Artikel 3 der Verordnung (EU) 2021/1232 vom 14. Juli 2021, der für bestimmte Fälle die Geltung von Artikel 5 Absatz 1 und Artikel 6 Absatz 1 der Richtlinie 2002/58/EG vom 12. Juli 2002 suspendiert, gegen höherrangiges Unionsrecht, insbesondere Art. 7, Art. 8, Art. 11 und Art. 47 GRCh sowie Art. 5 Abs. 4 EUV und ist aus diesem Grund ungültig?“

(b) Hilfsweise: Keine Aufgabenübertragung durch Übergangs-VO

Hilfsweise sei angemerkt, dass der Beklagten die Durchführung von „Chatkontrollen“ weder durch nationales Recht noch durch EU-

Recht übertragen wurde. Sofern man die Übergangs-VO nicht als ungültig wertete, bildet sie jedenfalls keine derartige Rechtsgrundlage. Sie erlaubt den Anbietern elektronischer Kommunikationsdienste nicht die Kontrolle und Analyse privater Nachrichten bzw. überträgt diese nicht explizit auf diese. Entsprechend stellt ihr Erwägungsgrund 10 klar:

> *„Die vorliegende Verordnung bietet zwar **keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten** durch Anbieter zum alleinigen Zweck der Aufdeckung von sexuellem Missbrauch von Kindern im Internet in ihren Diensten und der Meldung desselben und der Entfernung von Online-Material über sexuellen Missbrauch von Kindern aus ihren Diensten, aber sie sieht eine Ausnahme von bestimmten Vorschriften der Richtlinie 2002/58/EG vor.“* (Hevorh. nicht im Original)

Wie im letzten Halbsatz angesprochen suspendiert die Verordnung in Art. 3 lediglich Pflichten der Mitgliedsstaaten vor allem zur Gewährleistung der Vertraulichkeit der Kommunikation aus Art. 5 und Art. 6 RL 2002/58/EG der ePrivacy-Richtlinie. Eine staatliche Ermächtigung oder Veranlassung zur Durchführung der „Chatkontrolle“ stellt sie mithin nicht dar.

(2) Rechtswidrigkeit gemäß Art. 6 DS-GVO

Der Eingriff in das allgemeine Persönlichkeitsrecht kann ferner nicht durch datenschutzrechtliche Bestimmungen gerechtfertigt werden, da die „Chatkontrolle“ gemessen an Art. 6 DS-GVO als rechtswidrig einzustufen ist. Art. 6 Abs. 1 DS-GVO nennt verschiedene Fälle, in denen die Verarbeitung personenbezogener Daten rechtmäßig ist. Die Rechtfertigungsgründe in Art. 6 Abs. 1 lit. b−f DS-GVO sind dabei eng auszulegen, da sie trotz fehlender Einwilligung der betroffenen Person zu einer Rechtmäßigkeit der Datenverarbeitung führen können (EuGH, Urt. v. 04.07.2023 − C-252/21, Rn. 93, zit. nach juris).

Keine der in Art. 6 Abs. 1 DS-GVO genannten Fallgruppen ist für die durch die Beklagte durchgeführte „Chatkontrolle“ einschlägig, weshalb die grundsätzliche Vermutung für die Unrechtmäßigkeit der Datenverarbeitung bestehen bleibt. Zu beachten ist in dem Zusammenhang, dass sowohl nach allgemeinen zivilprozessualen Regelungen als auch speziell nach Art. 5 Abs. 2 DS-GVO die Beklagte als Verantwortliche für die Datenverarbeitung die Beweislast für die Rechtmäßigkeit der Datenverarbeitung trägt (EuGH, Urt. v. 04.07.2023 − C-252/21, Rn. 95, zit. nach juris; OLG Schleswig, Urt. v. 02.07.2021 – 17 U 15/21, Rn. 51, zit. nach juris; OLG Stuttgart, Urt. v. 18.05.2021 – 12 U 296/20, Rn. 28, 30, zit. nach juris).

(a) Grundsätzliche Anwendbarkeit der DS-GVO

Zunächst ist festzuhalten, dass bei der von der Beklagten praktizierten „Chatkontrolle“ personenbezogene Daten im Sinne der DS-GVO verarbeitet werden. Art. 4 Nr. 1 DS-GVO definiert personenbezogene Daten als

> *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen“*.

Bei der Durchführung der „Chatkontrolle“ kommen zwar technische Systeme zum Einsatz, die die via Messenger ausgetauschten Inhalte grundsätzlich automatisiert analysieren können. Aber auch ein automatisierter Prozess kann eine inhaltliche Kenntnisnahme nicht vermeiden, da die Relevanz oder die Intimität eines Inhalts eingeordnet werden muss. Hierzu ist zumindest die vorübergehende Speicherung des Inhalts im Arbeitsspeicher notwendig (*Zurawski*, ZD-Aktuell 2022, 01240). Überdies bleibt es nicht bei einem rein maschinellen Hash-Abgleich. Nach Durchführung der technischen Prüfung ist letztlich eine menschliche Überprüfung zur Aussortierung falsch-positiver Inhalte erforderlich (*Zurawski*, ZD-Aktuell 2022, 01240). Ferner eignet sich der reine Abgleich aufgrund von Hash-Werten nicht bei neuem CSAM-Material, da dieses in der Hash-Datenbank nicht vorhanden ist. Algorithmen und künstliche

Intelligenz müssen eingesetzt werden, die aber keineswegs so genau sind, als dass sie eine menschliche Überprüfung komplett ersetzten und überflüssig machten (Studie des EPRS, Punkt 3, S. 3, **Anlage K4).**

(b) Keine Einwilligung, Art. 6 Abs. 1 lit. a DS-GVO

Klargestellt sei, dass eine Einwilligung gemäß Art. 6 Abs. 1 lit. a DS-GVO in die Verarbeitung personenbezogener Daten im Rahmen der „Chatkontrolle“ nicht vorliegt. Die Beklagte deutet auf ihrer Seite zwar an, dass sie rechtswidrige Inhalte nicht toleriert und an Dritte weiterleitet (siehe oben **Anlage K1**). Dass hierunter die anlasslose Überwachung jedes Chats zu verstehen ist und insbesondere die genaue Funktionsweise der „Chatkontrolle“ legt die Beklagte hingegen nicht offen. Eine wirksame Einwilligung im Sinne von Art. 6 Abs. 1 lit. a DS-GVO verlangt nach der Legaldefinition in Art. 4 Nr. 11 DS-GVO jedoch gerade eine

> *„freiwillig für den bestimmten Fall,* ***in informierter Weise*** *und unmissverständlich abgegebene Willensbekundung* […]*“*. (Hervorh. nicht im Original)

Zum Informationserfordernis gehört beispielsweise die Angabe der Datenempfänger inklusive Adresse im Falle einer Weiterleitung von Daten, bei Datenübermittlungen in Drittländer eine Aufklärung über die damit verbundenen Risiken sowie die Angabe der Art der verarbeiteten Daten (Taeger/Gabel/*Arning*/*Rothkegel*, DSGVO, 4. Aufl. 2022, Art. 4 Rn. 339). Die unspezifischen Angaben der Beklagten genügen diesen Anforderungen nicht.

(c) Kein Schutz lebenswichtiger Interessen, Art. 6 Abs. 1 lit. d DS-GVO

Die Verarbeitung der personenbezogenen Daten des Klägers ist nicht nach Art. 6 Abs. 1 lit. d DS-GVO zum Schutz lebenswichtiger Interessen notwendig. Die Variante erfasst Ausnahmekonstellationen wie humanitäre Notfälle, Katastrophen oder Epidemien, die die

körperliche Unversehrtheit oder das Leben betreffen (Kühling/Buchner/*Buchner*/*Petri*, DS-GVO, 3. Aufl. 2020, Art. 6 Rn. 106 f.). Die Suche nach CSAM über die „Chatkontrolle“ stellt keinen solchen Ausnahmefall, sondern einen auf Dauer angelegten, regelmäßigen Vorgang dar.

(d) Keine Aufgabe im öffentlichen Interesse, Art. 6 Abs. 1 lit. e DS-GVO

Die Verarbeitung von personenbezogenen Daten des Klägers im Rahmen der „Chatkontrolle“ ist auch nicht gemäß Art. 6 Abs. 1 lit. e DS-GVO als im öffentlichen Interesse liegende Aufgabe und Ausübung öffentlicher Gewalt rechtmäßig. Eine derartige Übertragung müsste gemäß Art. 6 Abs. 3 S. 1 DS-GVO in einer Rechtsgrundlage geregelt sein. Private müssten anstelle einer Behörde handeln, was einen staatlichen Übertragungsakt voraussetzt (BVerwG, Urt. v. 27.03.2019 – 6 C 2/18, Rn. 46, zit. nach juris). Ein derartiger expliziter Übertragungsakt fehlt. Insbesondere stellt die Übergangs-VO nach den obenstehenden Ausführungen keine Rechtsgrundlage dar (oben (1)).

(e) Keine Wahrung berechtigter Interessen Art. 6 Abs. 1 lit. f DS-GVO

Schließlich ist die Verarbeitung personenbezogener Daten auch nicht zur Wahrung berechtigter Interessen im Sinne von Art. 6 Abs. 1 lit. f DS-GVO rechtmäßig. Diese Alternative ist im Lichte der Grundrechtecharta der EU auszulegen und dient dem angemessenen Ausgleich der Grundrechte Privater (BVerfG, Beschl. v. 06.11.2019 – 1 BvR 276/17, Rn. 33, zit. nach juris; BGH, Urt. v. 22.02.2022 – VI ZR 14/21, Rn. 19, zit. nach juris: Kühling/Buchner/*Buchner*/*Petri*, DS-GVO, 3. Aufl. 2020, Art. 6 Rn. 141). In drei Schritten ist zu prüfen, ob überhaupt ein berechtigtes Interesse des Verantwortlichen oder eines Dritten, an den Daten übermittelt werden, an der Datenverarbeitung vorliegt, ob die Datenverarbeitung zur Erreichung dieses berechtigten Interesses erforderlich ist und

ob die Grundrechte sowie Grundfreiheiten der von der Datenverarbeitung betroffenen Person nicht das berechtigte Interesse überwiegen (EuGH, Urt. v. 04.07.2023 − C-252/21, Rn. 106, zit. nach juris; Kühling/Buchner/*Buchner*/*Petri*, DS-GVO, 3. Aufl. 2020, Art. 6 Rn. 146; Paal/Pauly/*Frenzel*, DS-GVO, 3. Aufl. 2021, Art. 6 Rn. 27).

Unter das berechtigte Interesse im Sinne von Art. 6 Abs. 1 lit. f DS-GVO fallen alle tatsächlichen, rechtlichen, wirtschaftlichen oder ideellen Interessen. Nicht davon umfasst sind in Abgrenzung zu Art. 6 Abs. 1 lit. e DS-GVO jedoch Allgemeininteressen (Kühling/Buchner/*Buchner*/*Petri*, DS-GVO, 3. Aufl. 2020, Art. 6 Rn. 146a; Simitis/Hornung/Spiecker gen. Döhmann/*Schantz*, DS-GVO, 2019, Art. 6 Rn. 99). Der Vorschlag im Gesetzgebungsverfahren auch „im Interesse der öffentlichen Sicherheit und des Wohlergehens oder der Gesundheit des Menschen im Einklang mit den Grundrechten und Grundfreiheiten notwendig[e]“ Datenverarbeitungen mit in die Norm aufzunehmen, ist gerade nicht umgesetzt worden (Kühling/Buchner/*Buchner*/*Petri*, DS-GVO, 3. Aufl. 2020, Art. 6 Rn. 146a).

Das öffentliche Anliegen Kinderschutz beziehungsweise die Strafverfolgung des Verbreitens oder Besitzes von Kinderpornografie und von Grooming unterfallen dem staatlichen Strafverfolgungsmonopol und können folglich nicht als berechtigtes Interesse speziell der Beklagten gelten. Die Beklagte leitet vermeintliche Treffer vornehmlich auch nicht direkt an Strafverfolgungsbehörden weiter, sondern vor allem an das NCMEC als US-amerikanische Nichtregierungsorganisation. Folglich kann die Beklagte als eigenes berechtigtes Interesse nur geltend machen, innerhalb der Vertragsbeziehung zu den Nutzern vertragswidriges Verhalten durch die Verbreitung rechtswidriger Inhalte zu unterbinden. Grundrechtlich gestützt kann dieses Interesse allenfalls von Art. 16 GRCh, dem Schutz der unternehmerischen Freiheit, sein.

Dieses Grundrecht kann aber keineswegs die gewichtige Grundrechtsbeeinträchtigung auf Seiten der von der „Chatkontrolle“ betroffenen Kommunikationsparteien vor allem in Art. 7, 8 und 11 GRCh (siehe soeben (1)) rechtfertigen. Die fehlende Geeignetheit

der „Chatkontrolle“ zur Aufdeckung rechtswidriger Inhalte wurde bereits erläutert. Ebenso wurde hinlänglich die hohe Fehleranfälligkeit der Systeme dargelegt. Die vertrauliche Kommunikation und damit die Grundrechte von einer äußerst hohen Nutzerzahl werden anhaltslos beeinträchtigt, um einem wenig erfolgsversprechenden Ziel nachzugehen. Entstehende bedeutende Nachteil für die Beklagte, wenn sie ihre „Chatkontrollen“ nicht mehr praktiziert, lassen sich nicht identifizieren. Hier überwiegen deshalb die Grundrechte der Kommunikationsparteien sehr deutlich, weshalb die Beklagte kein berechtigtes Interesse an der Datenverarbeitung im Rahmen der „Chatkontrollen“ im Sinne von Art. 6 Abs. 1 lit. f DS-GVO geltend machen kann.

(3) Abschließende Abwägung zugunsten des allgemeinen Persönlichkeitsrechts

Aufgrund der Einordnung des allgemeinen Persönlichkeitsrechts als Rahmenrecht ist im Zusammenhang der Beurteilung der Rechtswidrigkeit der Rechtsbeeinträchtigung stets und hier abschließend eine umfassende Abwägung der Interessen des Inhabers des verletzten Rechts sowie der Interessen der anderen Seite anzustellen (vgl. nur BGH, Urt. v. 17.05.2022 – VI ZR 141/21, Rn. 35, zit. nach juris; BGH, Urt. v. 14.03.2023 – VI ZR 338/21, Rn. 31, zit. nach juris). Eine Gesamtabwägung der Rechte des Klägers und der Beklagten ergibt im vorliegenden Fall ein deutliches Überwiegen der klägerischen Rechte und mithin eine Rechtswidrigkeit der Beeinträchtigung. Auf Seiten der Beklagten ist schon fraglich, welches Recht zur Durchführung der freiwilligen „Chatkontrollen“ für sie streiten sollte. Eine Beeinträchtigung der Berufsfreiheit oder ähnliches ist bei Nichtdurchführung der freiwilligen „Chatkontrollen“ nicht erkennbar. Das allgemeine Ziel des Kinderschutzes, für das grundrechtlich geschützte Positionen streiten, ist nach dem eben Gesagten durch freiwillige „Chatkontrollen“ nicht erreichbar bzw. wird durch sie nicht nachweisbar gefördert (oben (1)). Auf Seiten des Klägers hingegen wiegt der Eingriff in das grundrechtlich untermauerte, unter anderem aus der Menschenwürde abzuleitende allgemeine Persönlichkeitsrecht schwer. Im Einzelnen:

(a) Aushöhlung des absolut geschützten Kernbereichs privater Lebensführung

Zum unantastbaren Kern der Gewährleistung des allgemeinen Persönlichkeitsrechts gehört es, anderen Menschen intimste Gedanken, Gefühle und auch Bilder unter Ausschluss Dritter mitzuteilen. Im digitalen Zeitalter erfolgt dieser Austausch in schnell ansteigendem Maße über das Internet. Für Kommunikationsmittel über das Internet muss aber dasselbe Schutzniveau gelten, wie seit Jahrzehnten für die Kommunikation über Briefe anerkannt. Das gilt umso mehr, als die Kommunikation häufig auch über große Distanzen etwa über zwei Kontinente erfolgt und internetbasierte Kommunikationsmittel hierfür unabdingbar sind. Praktizierte die Beklagte ihre „Chatkontrolle“ mithin weiter, führte das zwangsläufig zu einer empfindlichen Absenkung des grundrechtlichen Schutzniveaus und der Erkenntnis, dass der bedeutende Grundsatz vom unantastbaren Kernbereich der Intimsphäre für die Kommunikation über das Internet, konkret für die Kommunikation über den Messenger-Dienst der Beklagten nicht gilt.

(b) Eingeschränkte Freiwilligkeit der Nutzung

Im Rahmen der Abwägung ist zudem zu berücksichtigen, dass die Nutzung der Dienste der Beklagten im Grundsatz zwar freiwillig erfolgt, angesichts ihres dominierenden Marktanteils oft aber unumgänglich zur Kommunikation über das Internet ist.

So geht das Bundeskartellamt von einem Marktanteil Facebooks unter den sozialen Netzwerken von über 90 Prozent aus (Bundeskartellamt, Hintergrundinformationen zum Facebook-Verfahren v. 07.02.2019, S. 4, **Anlage K8**). Diese kartellrechtlich marktbeherrschende Stellung Facebooks hat der BGH auch bestätigt:

> *„Es bestehen keine ernstlichen Zweifel daran, dass Facebook Normadressat des § 19 I GWB [verbotenes Verhalten von marktbeherrschenden Unternehmen] ist. Die*

> *Annahme des BKartA, dass Facebook auf dem relevanten nationalen Markt für soziale Netzwerke für private Nutzer über eine marktbeherrschende Stellung verfügt, ist auf Grundlage des hier geltenden eingeschränkten Prüfungsmaßstabs nicht zu beanstanden."* (BGH, Beschl. v. 23.06.2020 – KVR 69/19, Rn. 14, zit. nach juris)

Um mit möglichst vielen Kommunikationspartnern weltweit in Kontakt treten zu können, sind die Dienste der Beklagten unumgänglich. Deshalb trägt das mögliche Argument, den Anbieter zu wechseln, um der „Chatkontrolle" zu entgehen, im Ergebnis nicht.

(c) Fragliche „Freiwilligkeit" der „Chatkontrolle"

Überdies ist die „Chatkontrolle" zwar aktuell noch nicht verpflichtend vorgeschrieben. Aber auch schon die derzeitig praktizierte „freiwillige" „Chatkontrolle" verdient das Attribut der Freiwilligkeit genau genommen nicht. Rechtlich mag ihre Durchführung nicht verpflichtend sein. Allerdings existiert ein politischer Druck für Anbieter von Kommunikationsdiensten die Kontrollen durchzuführen, wenn auch andere Anbieter diese praktizieren. Es droht ein negativer Ruf, wenn ein Kommunikationsanbieter im Gegensatz zu Konkurrenten keine Kontrollen mehr durchführt.

Hinzu tritt, dass Länder außerhalb der EU eine entsprechende Verpflichtung zur Durchführung von „Chatkontrollen" konkret planen. So befindet sich beispielsweise in Großbritannien das sogenannte „Online Safety Bill" im fortgeschrittenen Gesetzgebungsverfahren (Gesetzesentwurf abrufbar unter: https://bills.parliament.uk/bills/3137). Nahe liegt die Vermutung, dass ein Kommunikationsanbieter, der in einem Land zur „Chatkontrolle" verpflichtet ist, diese aus technischen, organisatorischen und/oder finanziellen Gründen für seine Dienste generell durchführt, wenn er sie technisch aufgrund der Verpflichtung in einem Land ohnehin implementieren muss.

(4) Zwischenfazit: rechtswidrige Beeinträchtigung des allgemeinen Persönlichkeitsrechts durch die „Chatkontrolle“

Die von der Beklagten praktizierte „Chatkontrolle“ verletzt das allgemeine Persönlichkeitsrecht des Klägers insbesondere dessen Ausprägung als informationelles Selbstbestimmungsrecht.

cc. Wiederholungsgefahr

Die erforderliche Wiederholungsgefahr besteht. Sie wird schon durch die Erstbegehung indiziert (stRspr., vgl. nur LG Frankfurt, Urt. v. 13.09.2018 – 2-03 O 283/18, Rn. 42, zit. nach juris). Die Beklagte betreibt die „Chatkontrollen“ weiter und hat eine Aussetzung der „Chatkontrollen“ bislang nicht angekündigt.

dd. Fazit: Unterlassungsanspruch aus § 1004 Abs. 1 S. 2 BGB analog i.V.m. § 823 Abs. 1 BGB

Im Ergebnis steht dem Kläger gegen die Beklagte ein Anspruch auf Unterlassung der „Chatkontrolle“ gemäß dem Klageantrag zu 1. aus § 1004 Abs. 1 S. 2 BGB analog i.V.m. § 823 Abs. 1 BGB zu.

b. Unterlassungsanspruch gemäß § 1004 Abs. 1 S. 2 BGB analog i.V.m. § 823 Abs. 2 BGB i.V.m. Art. 6 DS-GVO

Ein Anspruch des Klägers auf Unterlassung gemäß dem Klageantrag zu 1. folgt überdies aus § 1004 Abs. 1 S. 2 BGB analog i.V.m. § 823 Abs. 2 BGB i.V.m. Art. 6 DS-GVO.

aa. Anwendbarkeit des Unterlassungsanspruchs § 1004 Abs. 1 S. 2 BGB analog i.V.m. § 823 BGB bei Verstößen gegen die DS-GVO

Zur Geltendmachung der Rechte aus der DS-GVO, hier Art. 6 DS-GVO, kann der Unterlassungsanspruch gemäß § 1004 Abs. 1 S. 2

BGB analog i.V.m. § 823 BGB des deutschen Rechts herangezogen werden (hM, vgl. OLG Dresden, Urt. v. 14.12.2021 – 4 U 1278/21, Rn. 46, zit. nach juris; OLG Köln, Urt. v. 14.11.2019 – 15 U 126/19, Rn. 30, zit. nach juris; OLG Frankfurt, Urt. v. 14.04.2022 – 3 U 21/20, Rn. 28 f., zit. nach juris; OLG München, Urt. v. 19.01.2021 – 18 U 7243/19 Pre, Rn. 53, 62, zit. nach juris; OLG Schleswig, Urt. v. 02.07.2021 – 17 U 15/21, R. 70, zit. nach juris; OLG Stuttgart, Urt. v. 18.05.2021 – 12 U 296/20, Rn. 4, zit. nach juris; VGH München, Urt. v. 30.05.2023 – 5 BV 20.2104; LAG Hamm, Urt. v. 14.12.2021 – 17 Sa 1185/20, Rn. 97, zit. nach juris; LG Darmstadt, Urt. v. 26.05.2020 – 13 O 244/19, Rn. 37 f., zit. nach juris; LG Frankfurt, Urt. v. 13.09.2018 – 2-03 O 283/18, Rn. 24, zit. nach juris; LG Frankfurt, Beschl. v. 15.10.2020 – 2-03 O 356/20, Rn. 2, zit. nach juris; LG Hamburg, Urt. v. 13.02.2020 – 312 O 372/18, Rn. 39, zit. nach juris; LG Karlsruhe, Urt. v. 24.01.2023 – 2 O 446/20, Rn. 63, zit. nach juris; LG München I, Urt. v. 20.01.2022 – 3 O 17493/20, Rn. 26, zit. nach juris; BeckOK-DatenschutzR/*Quaas*, DS-GVO, 43. Ed., Art. 82 Rn. 9; Gola/Heckmann/*Gola*/*Piltz*, DS-GVO, 3. Aufl. 2022, Art. 82 Rn. 38; *Halder,* MMR 2022, 314, 315; *Leibold*/*Laoutoumai*, ZD-Aktuell 2021, 05583 m.w.N.; MüKo-BGB/*Wagner*, BGB, 8. Aufl. 2020, § 823 Rn. 547; Paal/Pauly/*Frenzel*, DS-GVO, 3. Aufl. 2021, Art. 82 Rn. 20; Sydow/Marsch/*Kreße*, DS-GVO, 3. Aufl. 2022, Art. 82 Rn. 27; Taeger/Gabel/*Moos*/*Schefzig*, DS-GVO, 4. Aufl. 2022, Art. 82 Rn. 107).

Hierzu führt der dritte Senat des OLG Frankfurt explizit aus:

> *„Die Durchsetzung eines Anspruchs auf Unterlassung bei einer rechtswidrigen Verarbeitung personenbezogener Daten im Sinne der Datenschutzgrundverordnung ist nach ganz herrschender Meinung möglich (vgl. zum Meinungsstand* Leibold/Laoutoumai*: Unterlassungsanspruch unter der DS-GVO? ZD-Aktuell 2021, 05583). Im Ergebnis sieht die herrschende Meinung einen Unterlassungsanspruch jedenfalls gemäß §§ 823, 1004 BGB (zum Teil i. V. m. Art. 6 Abs. 1 DSGVO) als gegeben an, da dieser nicht durch Art. 79 Abs. 1 DSGVO gesperrt ist (OLG Köln Urt. v. 14.11.2019 - 15 U 126/19, BeckRS 2019, 28523;* Leibold/Laoutoumai *aaO; a. A.*

> *VG Regensburg, Gerichtsbescheid vom 6.8.2020 - RN 9 K 19.1061, BeckRS 2020, 19361).“* (OLG Frankfurt, Urt. v. 14.04.2022 – 3 U 21/20, Rn. 29, zit. nach juris)

Auch der VGH München hat sich in einer aktuellen Entscheidung der herrschenden Ansicht angeschlossen und die anderslautende Entscheidung des VG Regensburg (VG Regensburg, Gerichtsbescheid vom 06.08.2020 − RN 9 K 19.1061) aufgehoben:

> *„Art. 79 Abs. 1 DSGVO schließt entgegen der Ansicht des Verwaltungsgerichts eine Unterlassungsklage betroffener Personen nach § 1004 Abs. 1 Satz 2 BGB analog i.V.m. Art. 2 Abs. 1 und Art. 1 Abs. 1 GG bei Verletzung ihres Grundrechts auf informationelle Selbstbestimmung durch eine rechtswidrige Verarbeitung ihrer personenbezogenen Daten nicht aus.“* (VGH München, Urt. v. 30.05.2023 – 5 BV 20.2104, Rn. 27, zit. nach juris)

Auch die Wissenschaftlichen Dienste des Deutschen Bundestages schließen sich dieser Meinung an:

> *„Art. 79 DS-GVO statuiert insoweit eine Rechtsschutzgarantie. Dem Betroffen*[en] *muss daher bei rechtswidriger Verarbeitung seiner auf seine Person bezogenen Daten gerichtlicher Rechtsschutz unmittelbar gegen den Verantwortlichen oder Auftragsverarbeiter zustehen. Da die DS-GVO sowie das BDSG selbst keinen Unterlassungsanspruch bei rechtswidriger Datenerhebung, -verarbeitung oder -nutzung beinhaltet, richtet sich ein solcher Anspruch des Betroffenen weiterhin nach dem allgemeinen nationalen Unterlassungsanspruch in § 1004 Abs. 1 Satz 2 BGB i. V. m. § 823 Abs. 1 BGB in analoger Anwendung.“* (Deutscher Bundestag − Wissenschaftliche Dienste, Ausarbeitung: Abmahnungen im Datenschutzrecht v. 13.06.2018, S. 7, **Anlage K9**)

Sofern eine gegensätzliche Entscheidung des 16. Senats des OLG Frankfurt im Sinne der Mindermeinung den Unterlassungsanspruch verneint und dabei unter anderem auf Entscheidungen des BVerfG (BVerfG, Beschl. v. 06.11.2019 – 1 BvR 276/17) und des BGH (BGH, Urt. v. 27.07.2020 – VI ZR 405/18) zur parallelen Anwendbarkeit von §§ 1004, 823 BGB neben Art. 17 DS-GVO bezüglich eines Auslistungsanspruchs, mithin eines Löschungsrechts, rekurriert (OLG Frankfurt, Urt. v. 30.03.2023 − 16 U 22/22, Rn. 58, zit. nach juris), muss dem entschieden entgegengetreten werden. Anders als für Unterlassungsansprüche kennt die DS-GVO mit Art. 17 explizit einen eigenständigen Rechtsbehelf für Löschansprüche, der keines Rückgriffs auf das nationale Recht bedarf (BeckOK-DatenschutzR/*Quaas*, DS-GVO, 43. Ed., Art. 82 Rn. 9.2).

bb. Art. 6 DS-GVO als Schutzgesetz i.S.v. § 823 Abs. 2 BGB

Art. 6 DS-GVO ist als Schutzgesetz i.S.v. § 823 Abs. 2 BGB einzustufen (OLG Köln, Urt. v. 14.11.2019 – 15 U 126/19, Rn. 30, zit. nach juris; LAG Hamm, Urt. v. 14.12.2021 – 17 Sa 1185/20, Rn. 99, zit. nach juris; LG Hamburg, Urt. v. 13.02.2020 – 312 O 372/18, Rn. 40; zit. nach juris; BeckOK-DatenschutzR/*Albers*/*Veit*, DS-GVO, 43. Ed., Stand: 01.02.2023, Art. 6 Rn. 115; Gola/Heckmann/*Gola*/*Piltz*, DS-GVO, 3. Aufl. 2022, Art. 82 Rn. 39; MüKo-BGB/*Wagner*, BGB, 8. Aufl. 2020, § 823 Rn. 547, 563; *Wybitul/Haß/Albrecht*, NJW 2018, 113 Fn. 3). Schutzgesetze sind Normen, die dem Schutz von Individualinteressen zu dienen bestimmt sind (MüKo-BGB/*Wagner*, BGB, 8. Aufl. 2020, § 823 Rn. 562). Dabei reicht es aus, wenn Individualschutz nicht den ausschließlichen Normzweck darstellt, zumindest aber auch Individualinteressen geschützt werden sollen (vgl. nur BGH, Urt. v. 11.01.2005 – VI ZR 34/04, Rn. 6, zit. nach juris).

Die DS-GVO verdeutlicht ihren individualschützenden Charakter selbst in § 1 Abs. 2 DS-GVO:

> *„Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.“*

Infolge dieser ausdrücklichen Klarstellung stellt Art. 6 DS-GVO ein Individualinteressen dienendes Schutzgesetz i.S.v. § 823 Abs. 2 BGB dar. Auch die Vorgängernormen der DS-GVO ordneten Gerichte als Schutzgesetze ein:

> *„Diese datenschutzrechtlichen Vorschriften* [§§ 4, 29 Abs. 2 BDSG] *dienen dem Zweck, den Einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird, und sind deshalb Schutzgesetze im Sinne des § 823 Abs. 2 BGB (Bergmann/Möhrle/Herb, BDSG, § 29 Rdnr. 12.3; Ordemann/Schomerus, a. a. O., § 1 Anm. 2.3; OLG Hamm, MDR 1983, 667, betreffend § 24 BDSG a. F.).“* (OLG Hamm, Urt. v. 04.04.1995 – 9 U 42/95, Rn. 16, zit. nach juris zu § 4 BDSG, ebenso BGH, Urt. v. 20.02.2018 – VI ZR 30/17, Rn. 21, zit. nach juris)

cc. Verletzung von Art. 6 DS-GVO

Die obigen Feststellungen haben bereits aufgezeigt, dass die „Chatkontrolle“ eine unrechtmäßige Verarbeitung personenbezogener Daten im Sinne von Art. 6 Abs. 1 DS-GVO darstellt (B.II.1.a.bb.(2)) und damit eine Schutzgesetzverletzung vorliegt.

dd. Fazit: Unterlassungsanspruch gemäß § 1004 Abs. 1 S. 2 BGB analog i.V.m. § 823 Abs. 2 BGB i.V.m. Art. 6 DS-GVO

Im Ergebnis steht dem Kläger gegen die Beklagte ein Anspruch auf Unterlassung der „Chatkontrolle“ gemäß dem Klageantrag zu 1. aus § 1004 Abs. 1 S. 2 BGB analog i.V.m. § 823 Abs. 2 BGB i.V.m. Art. 6 DS-GVO zu.

c. Unterlassungsanspruch gemäß § 1004 Abs. 1 S. 2 BGB analog i.V.m. § 823 Abs. 2 BGB i.V.m. § 3 TTDSG

Ein Unterlassungsanspruch hinsichtlich der „Chatkontrollen“ der Beklagten ergibt sich ferner aus § 1004 Abs. 1 S. 2 BGB analog i.V.m. § 823 Abs. 2 BGB i.V.m. § 3 TTDSG.

aa. Schutzgesetzcharakter von § 3 TTDSG

§ 3 TTDSG schützt einfachgesetzlich das Fernmeldegeheimnis nach Art. 10 GG (Taeger/Gabel/*Munz*, TTDSG, 4. Aufl. 2022, § 3 Rn. 38). Das Fernmeldegeheimnis soll vor einem Verlust an Privatheit durch die Nutzung distanzüberwindender Kommunikationsmedien schützen (*Assion*, TTDSG, 2022, § 3 Rn. 1). Aufgrund dieses individualschützenden Charakters ist § 3 TTDSG Schutzgesetz nach § 823 Abs. 2 BGB (Taeger/Gabel/*Munz*, TTDSG, 4. Aufl. 2022, § 3 Rn. 38).

bb. Verstoß gegen § 3 TTDSG

Das Fernmeldegeheimnis schützt nach § 3 Abs. 1 S. 1 TTDSG den Inhalt und die näheren Umstände von Telekommunikation. Unter den Begriff der Telekommunikation fallen gemäß § 3 Nr. 40 i.V.m. Nr. 61 lit. b TKG auch die nummernunabhängigen interpersonellen Messenger-Dienste (*Assion*, TTDSG, 2022, § 3 Rn. 8). Was unter den Inhalt der Telekommunikation fällt, muss im Lichte von Art. 5 Abs. 1 ePrivacy-Richtlinie ausgelegt werden (*Assion*, TTDSG, 2022, § 3 Rn. 43). Im Ergebnis sind Informationen geschützt, die Auskunft über die Kommunikation zwischen den Personen geben (*Assion*, TTDSG, 2022, § 3 Rn. 45). Das betrifft die bei der Kommunikation anfallenden Verkehrsdaten sowie alle Daten, die die Kommunikation individualisierbar machen (Taeger/Gabel/*Munz*, TTDSG, 4. Aufl. 2022, § 3 Rn. 10). Telekommunikationsanbietern ist nach § 3 Abs. 3 S. 1 TTDSG jede Kenntnisnahme des Inhalts oder der näheren Umstände der Telekommunikation im Sinne von § 3 Abs. 1 S. 1 TTDSG verboten, soweit es nicht zur Erbringung des

Telekommunikationsdienstes oder zum Schutz technischer Systeme erforderlich ist.

Die von der Beklagten durchgeführte „Chatkontrolle“ verstößt gegen diese gesetzlichen Regelungen. Die „Chatkontrolle“ arbeitet mit den betroffenen, die Kommunikation individualisierenden Daten. Spätestens zum Endabgleich des maschinell erkannten CSAM muss der Inhalt der Nachricht direkt zur Kenntnis genommen werden. Dies ist weder zum Anbieten des Messenger-Dienstes noch zum Schutz dessen technischer Systeme an sich erforderlich. Auch existiert keine § 3 Abs. 3 S. 3 TTDSG entsprechende gesetzliche Verwendung der Daten, da wie oben erörtert die Übergangs-VO eine solche gerade nicht darstellt (B.II.1.a.bb.(1)).

cc. Fazit: Unterlassungsanspruch gemäß § 1004 Abs. 1 S. 2 BGB analog i.V.m. § 823 Abs. 2 BGB i.V.m. § 3 TTDSG

Ein Unterlassungsanspruch hinsichtlich der „Chatkontrolle“ der Beklagten gemäß dem Klageantrag zu 1. ergibt sich aus § 1004 Abs. 1 S. 2 BGB analog i.V.m. § 823 Abs. 2 BGB i.V.m. § 3 TTDSG.

d. Unterlassungsanspruch aus Art. 17 Abs. 1 DS-GVO

Letztlich kann der Kläger seinen Unterlassungsanspruch gemäß dem Klageantrag zu 1. bezüglich der festgestellt rechtswidrigen Datenverarbeitung durch die Beklagte auch auf Art. 17 Abs. 1 lit. d DS-GVO i.V.m. Art. 6 Abs. 1 DS-GVO stützen. Der BGH erkennt über den Wortlaut dieses Löschanspruchs hinaus einen Unterlassungsanspruch bei rechtswidriger Datenverarbeitung nach der DS-GVO aus Art. 17 Abs. 1 DS-GVO an (BGH, Urt. v. 12.10.2021 – VI ZR 489/19, Rn. 10, zit. nach juris; BGH, Urt. v. 13.12.2022 – VI ZR 54/21, Rn. 40, zit. nach juris). Dass die Verarbeitung der personenbezogenen Daten des Klägers durch die Beklagte gemessen an Art. 6 Abs. 1 DS-GVO rechtswidrig ist, wurde oben bereits dargelegt (B.II.1.a.bb.(2)).

2. Ordnungsgeld

Die Androhung eines Ordnungsgeldes, ersatzweise Ordnungshaft, gemäß dem Klageantrag zu 2. folgt aus § 890 Abs. 1, Abs. 2 ZPO.

Wir bitten nach alldem um antragsgemäße Entscheidung.

Dr. David Albrecht
Rechtsanwalt

Lisa Engelbrecht
Rechtsanwältin