STEINMEIER

STEINMEIER | Palaisplatz 3 | 01097 Dresden

per beA
Amtsgericht Kiel
Deliusstraße 22

24114 Kiel

Geschäftszeichen: 108 C 46/22

In dem Rechtsstreit

Dr. Breyer

gegen

Meta Platforms Ireland Limited

nehmen wir Stellung zum Schriftsatz der Beklagten vom 28.09.2022.

Die Klage ist zulässig und begründet.

I. Zulässigkeit

1. Internationale und örtliche Zuständigkeit

a) Zuständigkeit nach Art. 17 Abs. 1, c), 18 Abs. 1 EuGVVO

STEINMEIER Rechtsanwälte Partnerschaft mbB

Heike Steinmeier [B]
Achim A. Poppe [B 2)]
Prof. Dr. Ralph Wagner LL.M. [D 1) 3) 4)]
Ute Salamon [B 2)]
Dr. Erik Hinrichs [D 3) 4)]
Markus Hilbert [D]
Dr. Daniel Sturm MBA [D 1)]
Carolin Rubel [D]
Alexander Weidenhammer [D]

B Berlin
D Dresden

1) Fachanwalt für Arbeitsrecht
2) Fachanwalt für Familienrecht
3) Fachanwalt für Handels- und Gesellschaftsrecht
4) Fachanwalt für Steuerrecht

Dresden, den 04.11.2022

Aktenzeichen 2-33/22-4

Ihr Zeichen 108 C 46/22

Schreibzeichen A-7125_1

Sekretariat 0351 / 448 333 - 45

Dresden
Palaisplatz 3
01097 Dresden
Telefon +49 (0)351 – 448 333-0
Telefax +49 (0)351 – 448 333-33
dresden@steinmeier.eu

Berlin
Kurfürstendamm 237
10719 Berlin
Telefon +49(0)30 - 88 71 00 88
Telefax +49(0)30 - 88 71 00 80
berlin@steinmeier.eu

www.steinmeier.eu

DKB Deutsche Kreditbank
Iban-Code: DE82 1203 0000 1067 1099 16
Swift-Code (BIC): BYLADEM1001

Umsatzsteuer-Identifikations-Nr. DE288263857

Amtsgericht Berlin (Charlottenburg) PR 1365 B

Das angerufene Amtsgericht Kiel ist entgegen der Beklagtenauffassung für die Entscheidung des Rechtstreits international zuständig.

Gemäß Art. 17 Abs. 1, c), 18 Abs. 1 EuGVVO hat der Kläger als Verbraucher die Wahl, ob er in Deutschland oder am Sitz der Beklagten Klage erhebt.

Der Verbraucherbegriff des Art. 17 Abs. 1 EuGVVO ist vertragsautonom auszulegen. Es kommt entscheidend darauf an, ob der Kläger mit der Beklagten ein Vertragsverhältnis einging, das seiner privaten Sphäre zuzurechnen ist. Vorliegend bestätigt die Beklagte, dass sie Anbieterin des streitgegenständlichen Facebook-Messengers ist und es sich hierbei um eine integrierte Chat-Lösung handelt. Der Kläger ist das Vertragsverhältnis mit der Beklagten zur Nutzung dieser Chat-Funktion sicher nicht aus unternehmerisch-gewerblichen Zwecken eingegangen. Er benötigt die Chat-Software nur zur Kommunikation mit Nutzern dieses Messenger-Dienstes. Die Einrichtung des Facebookauftritts erfolgte lange vor der Wahl des Klägers in das Europäische Parlament. Die politische Tätigkeit des Klägers in seiner Partei war ehrenamtlicher Natur. Auch eine Kandidatur für ein politisches Amt ist keine berufliche Tätigkeit, sondern ein privates staatsbürgerliches Engagement – übrigens nach Auffassung des Klägers auch das politische Amt eines Volksvertreters selbst. Bei Einrichtung der Facebookseite war der Kläger beruflich als Richter tätig. Er hat Facebook nie in diesem Zusammenhang, also zu beruflichen Zwecken, genutzt.

Gemäß Art. 17 Abs. 1 EuGVVO kommt es zudem entscheidend darauf an, für welche Zwecke der Kläger das Vertragsverhältnis zur Beklagten einging. Bei Abschluss des Vertrags ging der Kläger nicht davon aus, den Messenger-Dienst für berufliche Zwecke zu nutzen. Die Nutzung erfolgte ausschließlich zu privaten Zwecken mit anderen privaten Nutzern des Messenger-Dienstes mit denen der Kläger als Privatperson in Kontakt stand. Dies steht auch nicht in Widerspruch zum bisherigen Vortrag, wonach „private Kommunikation“ des Klägers betroffen ist und er über Informationen kommuniziert, die er in seiner Abgeordneteneigenschaft erhielt. Es handelt sich stets um Informationen, die er auch privat kommunizieren darf.

b) Zuständigkeit nach Art. 7 Abs. 1 Nr. 2 EuGVVO

Im Hinblick auf § 3 TTDSG begründet weiterhin Art. 7 Nr. 2 EuGVVO die internationale Zuständigkeit des AG Kiel (ebenso bereits allgemein § 1004 analog BGB i.V.m. § 823 Abs. 1 oder Abs. 2, vgl. BeckOK ZPO/Thode, 45. Ed. 1.7.2022, Brüssel Ia-VO Art. 7 Rn. 78.1).

Der Verstoß gegen das Fernmeldegeheimnis nach § 3 TTDSG stellt eine unerlaubte Handlung im Sinne des Art. 7 Nr. 2 EuGVVO dar. Die Begriffe "unerlaubte Handlung" und "Handlung, die einer unerlaubten Handlung gleichgestellt ist" sind autonom und weit auszulegen (BGH,

08.05.2012 - VI ZR 217/08). Abzugrenzen ist die unerlaubte Handlung ebenso wie die ihr gleichgestellte Handlung von einem Vertrag, d.h. von einer freiwillig eingegangenen Verpflichtung. Unter den Begriff der unerlaubten Handlung fallen daher etwa auch Persönlichkeitsrechtsverletzungen (vgl. BGH a.a.O.). Erfasst werden neben Ansprüchen auf Geldersatz auch Unterlassungsansprüche (BGH a.a.O.). Der hier streitgegenständliche § 3 TTDSG stellt – ähnlich wie das Persönlichkeitsrecht – keine vertragliche, freiwillige Verpflichtung dar, sondern eine von Gesetzes wegen auferlegte Pflicht.

„Eingetreten" ist das schädigende Ereignis i.S.d. Art. 7 Nr. 2 EuGVVO nach ständiger Rechtsprechung sowohl am Ort der Verwirklichung des Schadenserfolgs als auch am Ort des für den Schaden ursächlichen Geschehens. Rechtsprechung existiert zu Unterlassungsklagen in Bezug auf Persönlichkeitsrechtsverletzungen im Internet (vgl. Zöller, Zivilprozessordnung, 34. Aufl., 2022, Art. 7 EuGVVO, Rn. 93a). Demnach kann die Person, die sich in ihren Rechten verletzt fühlt, bei den Gerichten des Mitgliedsstaats, in dem sich der Mittelpunkt seiner Interessen befindet, klagen. Der Kläger, der in Kiel wohnend gewählt wurde und in Kiel auch weiter eine Wohnung unterhält, hat dort den Mittelpunkt seiner Interessen.

c) Zuständigkeit nach Art. 79 Abs.2 DSGVO

Sofern es danach noch auf die internationale Zuständigkeit nach Art. 79 Abs. 2 DSGVO ankommen sollte, leugnet die Beklagte nur, dass die Vorschrift auf Unterlassungsklagen anwendbar sei.

Ob Betroffenen bei Verstößen gegen die DSGVO ein Unterlassungsanspruch analog § 1004 BGB zusteht, ist umstritten. Allgemein ist die wesentliche Anspruchsvoraussetzung des § 1004 BGB analog, dass ein absolut geschütztes Recht verletzt ist oder eine solche Verletzung droht. Einen zivilrechtlichen Unterlassungsanspruch kann vor allem geltend machen, wer individuell in seinem Recht betroffen ist. Dass § 1004 BGB analog auf Verletzungen des allgemeinen Persönlichkeitsrechts als absolut geschütztes Recht anwendbar ist, ist allgemein anerkannt. Die DSGVO dient aber gerade dem Schutz des allgemeinen Persönlichkeitsrechts in seiner Ausprägung als Recht auf informationelle Selbstbestimmung.

Sowohl das LG Wiesbaden in der von der Beklagten zitierten Entscheidung (Urteil vom 20.1.2022 – 10 O 14/21), wie auch das VG Regensburg (ZD 2020, 601, 602 beck-Rn. 17), halten die Anwendung von § 1004 BGB analog für gesperrt. Kern des Arguments ist der abschließende Charakter der DSGVO als vollharmonisiertes Gemeinschaftsrecht. Demnach verweise Art. 79 Abs. 1 DSGVO explizit (nur) auf die „auf Grund dieser Verordnung zustehenden Rechte"; die DSGVO selbst normiere jedoch keinen Unterlassungsanspruch.

Dem widerspricht jedoch (zutreffend) die weit überwiegende Judikatur (etwa LG Karlsruhe, Urt. v. 11.10.2019 – 8 O 282/19; OLG Köln, MMR 2020, 186 = Urt v. 14.11.2019 – 15 U 126/19; OLG Stuttgart, Urteil vom 18.05.2021 - 12 U 296/20; LG Darmstadt, ZD 2020, 642; AG Köln, Urt. v. 22.9.2021 – 210 C 24/21; LG Frankfurt/M. Urt. v. 18.9.2020 – 2-27 O 100/20; OLG Frankfurt, Urt. v. 14.04.2022 - 3 U 21/20; OLG Frankfurt, Urt. v. 06.09.2018 – 16 U 193/17; OLG Dresden, NJW-RR 2019, 676; OLG Dresden, Urt. v. 14.12.2021 – 4 U 1278/21; OLG Frankfurt/M., ZD 2020, 638; LG München I, Urt. v. 20.1.2022 – 3 O 17493/20), wobei nur die dogmatische Herleitung des Unterlassungsanspruchs streitig ist. Vertreten wird im Wesentlichen entweder ein Rückgriff auf Art. 82 DSGVO i.V.m. § 249 BGB, Art. 17 f., 21 DSGVO oder auf den (mitunter öffentlich-rechtlichen) Unterlassungsanspruch aus § 823 Abs. 1 BGB i.V.m § 1004 BGB analog (wobei einige Gerichte auf eine Verletzung des allgemeinen Persönlichkeitsrechts abstellen, einige auf Art. 6 DSGVO bzw. § 823 Abs. 2 BGB, Art. 6 Abs. 1 DSGVO i.V.m § 1004 BGB analog). Die inhaltlichen Voraussetzungen – die Unterlassung einer unrechtmäßigen Datenverarbeitung – stimmen jedoch in all diesen Varianten überein.

Zu Recht argumentiert das VG Wiesbaden (VG Wiesbaden, Beschluss vom 1.12.2021 – 6 L 738/21.WI), Art. 79 Abs. 1 DSGVO entfalte bereits dem Wortlaut nach keine Sperrwirkung, da die Formulierung „auf Grund dieser VO zustehenden Rechte“ keinen Verweis (allein) auf Kapitel 3 der DSGVO darstellt, welches die Rechte des Betroffenen normiert. Ein „der betroffenen Person … zustehendes Recht“ ist auch, dass Datenverarbeitungen ohne Rechtsgrundlage (verboten durch Art. 5 Abs. 1 lit. a) und Art 6 DSGVO) unterbleiben. Weiter wird vom VG Wiesbaden zutreffend ausgeführt, dass der bloße, abschließende Verweis auf eine Beschwerde bei der Aufsichtsbehörde nach Art. 77 DS-GVO den europarechtlichen Effektivitätsgrundsatz sowie das Recht auf einen „wirksamen“ gerichtlichen Rechtsbehelf nach Art. 79 DS-GVO verletzen würde. Art. 79 DSGVO soll nach seinem Wortlaut sowie Sinn und Zweck den Rechtschutz für betroffene Personen eindeutig verbessern, nicht ihn einschränken.

Speziell das LG Kiel (Urteil vom 12.02.2021 - 2 O 10/21) hat auch bereits entschieden, dass § 1004 Abs. 1 BGB entsprechend auf die Abwehr von Beeinträchtigungen des Persönlichkeitsrechts durch Verletzung der DSGVO anzuwenden ist. Das OLG Schleswig-Holstein hat dies im Berufungsverfahren nicht beanstandet (OLG Schleswig, Urteil vom 2.7.2021 – 17 U 15/21).

Der EuGH hat entschieden, dass Art. 80 Abs. 2 DSGVO auch eine „Verbandsklage auf Unterlassung von gegen diese Verordnung verstoßenden Verarbeitungen“ abdeckt, um die Rechte der Betroffenen zu stärken (EuGH, Urt. v. 28.04.2022 - C-319/20, Rn. 74). Nach Art. 80 Abs. 2 DSGVO können bestimmte Verbände befugt werden, „die in den Artikeln 78 und 79 aufgeführten Rechte in Anspruch zu nehmen“. Daraus ergibt sich, dass nach (insoweit abschließend maßgeblicher) Auffassung des EuGH auch die Unterlassungsklage von den in Artikel 79 aufgeführten Klagerechten abgedeckt sein muss.

Tatsächlich garantiert Art. 79 Abs. 1 DSGVO ein Klagerecht, wenn eine Person der Ansicht ist, dass ihre Rechte „infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden“. Wie anders soll man gegen eine illegale Datenverarbeitung klagen als auf deren Unterlassung?

Auch der Bundesgerichtshof hat die Erwägung eines Berufungsgerichts nicht beanstandet, es könne dahinstehen, ob sich der Unterlassungsanspruch nach dem KUG angesichts des zwischenzeitlichen Inkrafttretens der Datenschutz-Grundverordnung weiterhin aus § 1004 Abs. 1 BGB analog, § 823 Abs. 2 BGB, §§ 22, 23 KUG ableiten lasse oder inzwischen auf § 1004 Abs. 1 BGB analog, § 823 Abs. 2 BGB, Art. 6 Abs. 1 DSGVO abzustellen sei, weil beides zum gleichen Ergebnis führen müsse (BGH, 21.01.2021 - I ZR 207/19).

Ergänzend hinzuweisen ist auf ein Gutachten des wissenschaftlichen Dienstes des Bundestags, welches ebenfalls für eine Anwendbarkeit des § 1004 i.V.m. § 823 Abs. 1 BGB analog plädiert (https://www.bundestag.de/resource/blob/565438/6c2433d7b0b7a4344f2022ec824fbd0c/WD-7-116-18-pdf-data.pdf, abgerufen am 11.10.2022).

d) Zuständigkeit aus § 32 ZPO

Die örtliche Zuständigkeit dürfte sich, soweit nicht bereits von Art. 7 Nr. 2 EuGVVO umfasst, jedenfalls aus § 32 ZPO ergeben. Wie zu Art. 7 Nr. 2 EuGVVO erläutert, tritt das schädigende Ereignis in Kiel ein, wenn das Fernmeldegeheimnis verletzt und die (auch) von Kiel aus geführte digitale Korrespondenz unbefugt durchleuchtet wird.

2. Sachliche Zuständigkeit

Es ist weder entscheidungserheblich, welcher Streitwert von der Beklagten – aufgrund vermeintlicher Ziele des Klägers – als „angemessen“ betrachtet wird, noch welche wirtschaftlichen Auswirkungen sich für die Beklagte mit dem vorliegenden Rechtstreit verbinden. Die anderslautenden Ausführungen der Beklagten gehen rechtlich fehl. Entscheidend für die Streitwertbestimmung ist allein die monetär bezifferte Bedeutung des Rechtstreits für den Kläger. Dies folgt aus § 2 ZPO i.V.m. §§ 23, 71 GVG und § 3 ZPO.

Der Klageantrag zu Ziff. 1 ist darauf gerichtet, die Beklagte dazu zu verurteilen, es zu unterlassen, Inhalt und nähere Umstände der über den Messenger-Dienst der Beklagten versandten Nachrichten zu analysieren, zu kontrollieren oder an Dritte weiterzugeben. Dieses Interesse des Klägers ist maßgeblich zur Ermittlung des Streitwerts und mit der vorläufigen Angabe i. H. v. EUR 5.000,00 absolut auskömmlich bemessen.

Entgegen der Beklagtenauffassung kommt es hierbei nur auf die Interessen des Klägers und nicht die der Beklagten an (anders jedoch die Beklagte, die die „möglichen Auswirkungen auf den Kommunikationsdienste der Beklagten“ zur Streitwertbemessung einbeziehen will, siehe Seite 3, Ab. 1 des Schriftsatzes vom 28.09.2022). Die Klage ist auch nicht auf die „Feststellung der Nichtigkeit der ePRIVACY-Ausnahme-VO“ gerichtet, sondern eben auf die Unterlassung der Analyse, Kontrolle und Weitergabe an Dritte von Nachrichten des Klägers. Der Kläger kommuniziert über den Dienst der Beklagten nicht sehr häufig, eher sporadisch.

Ausgangspunkt für die Wertbestimmung i.S.d. § 3 ZPO, § 48 Abs. 2 S. 1 GKG ist der zu schätzende Wert der Beeinträchtigung, die von dem beanstandeten Verhalten zu besorgen ist und die beseitigt werden soll (Zöller, Zivilprozessordnung, 34. Aufl. 2022, § 3 ZPO, Rn. 16.172). Bietet der Fall keine Anhaltspunkte für eine Anknüpfung an einen entsprechenden Wert, so kann in analoger Anwendung der Auffangstreitwert des § 52 Abs. 2 GKG (5.000 €) als Ausgangspunkt angesetzt werden (OLG Braunschweig, Beschl. v. 28.9.2020 – 1 W 3/20, Rn. 19). Dieser ist, je nach Ausübung des nach § 3 ZPO zustehenden Ermessens, hinauf- oder hinabzusetzen.

Die von der Beklagten angeführten Entscheidungen betrafen völlig andere Fallgestaltungen und sind nicht übertragbar. Es ging dort um die Zulässigkeit von öffentlichen Meinungsäußerungen in sozialen Netzwerken, während es hier nur um private Kommunikation im Zweipersonenverhältnis geht.

Ein Fall der Anwendung ausländischen Rechts liegt hier gerade nicht vor.

Den Kläger wegen seines politischen Engagements für den Grundrechtsschutz finanziell zu bestrafen, ist nicht zu rechtfertigen und findet keinerlei Anhaltspunkt in den gesetzlichen Vorgaben zur Streitwertbestimmung.

Wie in dem Beschluss des OLG Braunschweig vom 28.9.2020 (1 W 3/20) zutreffend ausgeführt, ist beim Streitwert zu berücksichtigen, ob (wie hier) nur einzelne Aspekte einer Kommunikation beanstandet werden.

Darüber hinaus ist bei der monetären Gewichtung zu beachten, dass der Kläger den streitgegenständlichen Dienst der Beklagten ebenso wie andere (alternativ verfügbare Dienste kostenlos bzw. in einigen Fällen für sehr niedriges Entgelt, jedenfalls weit unter dem Betrag von EUR 5.000 nutzen kann.

3. Bestimmtheit des Klageantrags

Soweit die Beklagte dazu sinngemäß meint, der Klageantrag gehe zu weit, betrifft dies nicht die Bestimmtheit (und damit Zulässigkeit) der Klage, sondern wäre allenfalls eine Frage der Begründetheit.

Insoweit sei bereits hier angemerkt: Dass der Klageantrag der Beklagten selbst die Mitwirkung an gesetzlich angeordneter Kommunikationsüberwachung verbieten würde, ist falsch. Eine Anordnung zur Telekommunikationsüberwachung verpflichtet die Beklagte zur „Überwachung und Aufzeichnung“ (§ 100a StPO), nicht aber dazu „den Inhalt und die näheren Umstände von ... Nachrichten ... zur Suche nach möglicherweise rechtswidrigen Inhalten oder Kontaktaufnahmen automatisiert zu analysieren, zu kontrollieren **und** an Dritte weiterzugeben“. Maßnahmen der Telekommunikationsüberwachung dienen der Aufklärung eines bestehenden Tatverdachts, nicht der verdachtsunabhängigen und anlasslosen Verdachtssuche. Sie erfordern auch keine automatisierte Analyse oder Kontrolle seitens der Beklagten.

II. Begründetheit

1. Verletzung des Fernmeldegeheimnisses (§ 3 Abs. 3 TTDSG)

a) Anwendbarkeit des TTDSG auf ausländische Anbieter von Diensten in Deutschland

aa) örtlicher Anwendungsbereich

Das TTDSG gilt gem. § 1 Abs. 3 S. 1 für alle Unternehmen, die im Geltungsbereich des TTDSG eine Niederlassung haben oder Dienstleistungen erbringen. Da die Beklagte unstreitig sowohl eine Niederlassung in Hamburg unterhält (Facebook Germany GmbH) als auch im Inland direkt TK-Dienstleistungen erbringt, ist der örtliche Anwendungsbereich eröffnet.

bb) sachlicher Anwendungsbereich

Auch der sachliche Anwendungsbereich ist eröffnet. Gem. § 2 Abs. 1 TTDSG sind für den Anwendungsbereich die Begriffsbestimmungen des § 3 TKG maßgeblich. Zwar ist der Facebook-Messengerdienst kein klassischer TK-Anbieter. Jedoch hat der Gesetzgeber in der Neufassung des TKG den Verpflichtetenkreis bzgl. der Einhaltung des sektorspezifischen Datenschutzes auf OTT-Dienste, worunter auch der Messenger von Facebook fällt, erweitert. Demnach gelten gem. § 3 Nr. 61 b) TKG interpersonelle TK-Dienste als TK-Dienste. Die Beklagte ist Anbieter des Dienstes i.S.d. § 3 Nr. 1 TKG und erbringt somit TK-Dienstleistungen i.S.v. § 1 Abs. 3 TTDSG.

b) ePrivacy-Ausnahmeverordnung 2021/1232/EU unerheblich

Die von der Beklagten angeführte ePrivacy-Ausnahmeverordnung 2021/1232/EU lässt § 3 Abs. 3 TTDSG völlig unberührt. Rechtsfolge dieser Verordnung ist ausweislich deren Artikel 3 nur, dass die Art. 5 und 6 der ePrivacy-Richtlinie 2002/58/EG zur Vertraulichkeit der Telekommunikation keine Anwendung finden sollen. Auch ohne diese Vorgaben der ePrivacy-Richtlinie aber gilt § 3 Abs. 3 TTDSG in Deutschland. Das einfachgesetzliche Fernmeldegeheimnis war lange vor Erlass der ePrivacy-Richtlinie gesetzlich verankert und gilt unabhängig von dieser weiter.

Soweit die Beklagte behauptet, die ePrivacy-Ausnahmeverordnung "erlaube" eine Chatkontrolle, ist dies eindeutig falsch. Diese Verordnung schafft ausdrücklich keine Rechtsgrundlage für derartige Maßnahmen (siehe Erwägungsgrund 10), sondern erklärt nur Vorschriften einer Richtlinie (Art. 5 und 6 der ePrivacy-Richtlinie 2002/58/EG) für nicht anwendbar.

Dies bedeutet nach allgemeiner EU-rechtlicher Systematik, dass die in den (nicht anwendbaren) Regeln der Richtlinie gesetzten Vorgaben für das nationale Recht der Mitgliedstaaten entfallen, die Mitgliedstaaten also frei und souverän regeln dürfen. Diese Möglichkeit ist in Deutschland durch § 3 Abs. 3 TTDSG genutzt.

c) ePrivacy-Ausnahmeverordnung 2021/1232/EU unwirksam

Von der mangelnden Erheblichkeit im vorliegenden Rechtsstreit abgesehen, ist die ePrivacy-Ausnahmeverordnung mit den EU-Grundrechten unvereinbar, wie in der Klageschrift ausgeführt.

aa) Legitimer Zweck

Unstreitig ist der Schutz von Kindern vor sexuellem Missbrauch und damit deren körperliche Unversehrtheit ein legitimes und wichtiges Schutzgut. Wie der EuGH u.a. in seinen Entscheidungen zur Vorratsdatenspeicherung ausgeführt hat, muss der Staat seinen Pflichten zum Schutz von Kindern allerdings im Einklang mit den Grundrechten und dem Verhältnismäßigkeitsgebot nachkommen. Die verschiedenen Grundrechtspostionen sind miteinander in sinnvollen Ausgleich zu bringen. Mit anderen Worten: Die unumschränkte Durchsetzung eines Grundrechts ohne Rücksicht auf dadurch beeinträchtigte andere Grundrechtspositionen ist rechtstaatlich unzulässig. Eine solche andere Grundrechtsposition ist z.B. das Recht auf Achtung der Privatsphäre.

Auch muss der Versuch der Beklagten zurückgewiesen werden, den Besitz oder die Verbreitung von Ausbeutungsdarstellungen mit dem Missbrauch von Kindern oder Jugendlichen bzw. sexueller Gewalt gleichzusetzen. Auch wenn es sich bei beiden Tatbeständen um schwere Straftaten handelt, zeigt schon der gesetzliche Strafrahmen die unterschiedliche Qualität der Verbrechen. Die Beklagte selbst hat eine Studie veröffentlicht, derzufolge der Austausch von Ausbeutungsdarstellungen in den meisten Fällen ohne den Vorsatz erfolge, Kinder zu schädigen (https://research.facebook.com/blog/2021/02/understanding-the-intentions-of-child-sexual-abuse-material-csam-sharers/). Als Beispiele genannt werden dort fehlendes Bewusstsein der Strafbarkeit, fehlendes Bewusstsein der Minderjährigkeit z.B. bei Aufnahme einer 17-jährigen Person, vermeintlich lustige Darstellung des Bisses eines Tiers in die Genitalien eines Kindes, einvernehmlicher Austausch von Nacktfotos durch 16-jährige.

Eine internationale Arbeitsgruppe aus Kinderschutzinstitutionen weist darauf hin, dass das strafbare Material weit über Aufnahmen sexuellen Missbrauchs hinausgeht (https://www.ohchr.org/sites/default/files/TerminologyGuidelines_en.pdf). Als Beispiele nennt die Arbeitsgruppe in Alltagssituationen entstandene Aufnahmen wie ein Familienbild eines Mädchens im Bikini oder nackt in den Stiefeln ihrer Mutter, ohne Wissen der minderjährigen Person angefertigte oder weitergegebene Aufnahmen, Comics, Zeichnungen, Manga/Anime und computergenerierte Darstellungen sowie selbstgemachte sexuelle Aufnahmen Minderjähriger etwa zur Weiterleitung an gleichaltrige Partner („Sexting“).

bb) Fehlende Geeignetheit der Maßnahme zum Schutz des Rechtsguts

Die Ermächtigung privater Unternehmen, nach eigener Entscheidung private Kommunikation zu durchleuchten, ist völlig ungeeignet zum effektiven Schutz vor Missbrauch und Ausbeutung Minderjähriger.

Wie der EuGH u.a. in seinen Entscheidungen zur Vorratsdatenspeicherung ausgeführt hat, muss der Staat seinen Pflichten zum Schutz von Kindern im Einklang mit den Grundrechten und dem Verhältnismäßigkeitsgebot nachkommen. Diese Schutzpflichten rechtfertigen also (selbstverständlich) keine unverhältnismäßigen Grundrechtseingriffe, insbesondere keine Maßnahmen, die zur Erreichung des angestrebten Ziels erkennbar ungeeignet sind.

Die Grundrechte garantieren auch das Telekommunikationsgeheimnis von Kindern, die auf den Schutz ihrer privaten Kommunikation und Fotos besonders angewiesen

sind. Dazu hat der UN-Kinderrechtsausschuss in seinem Kommentar ("general comment") Nr. 25 aus dem Jahr 2021 hervorgehoben: "Jede digitale Überwachung von Kindern und jede damit verbundene automatisierte Verarbeitung personenbezogener Daten sollte das Recht des Kindes auf Privatsphäre respektieren und nicht routinemäßig, wahllos oder ohne das Wissen des Kindes durchgeführt werden…" Die von der Beklagten praktizierte routinemäßige und wahllose Durchleuchtung privater Kommunikation auch von Kindern ist mit deren Rechten somit gerade unvereinbar.

Zum Hintergrund und mit Blick auf die Verhältnismäßigkeitsprüfung soll erläutert werden, warum die beklagtenseits praktizierte, privatisierte Nachrichtendurchleuchtung Minderjährige nicht schützt, sondern ihnen schadet:

- Das Scannen privater Nachrichten und Chats dämmt die Verbreitung ausbeutender ("kinderpornografischer") Darstellungen nicht ein. Die Beklagte beispielsweise praktiziert eine Chatkontrolle seit Jahren (lange Zeit insgeheim) und die Zahl ihrer automatisierten Strafanzeigen steigt von Jahr zu Jahr an, auf zuletzt 22 Millionen im Jahr 2021. Die Verdrängung in andere Kanäle kommt hinzu.

- Die Chatkontrolle der Beklagten trifft die Täter, die Kindesmissbrauch aufnehmen und weitergeben, nicht. Missbrauchstäter tauschen ihr Material nicht über kommerzielle E-Mail-, Messenger- oder Chatdienste, sondern organisieren sich über selbst betriebene geheime Foren. Bilder und Videos laden Missbrauchstäter außerdem typischerweise als verschlüsselte Archive hoch und teilen nur die Links und Passwörter. Die Algorithmen der Beklagten erkennen solche Links nicht.

- Legale selbst aufgenommene Nacktaufnahmen von Minderjährigen (Sexting) geraten durch die fehleranfälligen Algorithmen der Beklagten vielfach in die Hände von Unternehmensmitarbeitern und Polizei, wo sie nicht hingehören und nicht sicher sind.

- Jugendliche werden überproportional kriminalisiert. Laut Kriminalstatistik richten sich 54% aller eingeleiteten Ermittlungsverfahren wegen Kinderpornografie gegen Minderjährige, obwohl Jugendlichen eine sexuelle Motivation fehlt. Die Beklagte ist in einer Untersuchung sogar zu dem Ergebnis gekommen, dass ihre Verdächtigungsmaschinen zu 75% Nutzer anzeigen, die ohne "böswillige Absicht" handeln, sondern etwa aus Empörung oder zur Belustigung (https://research.facebook.com/blog/2021/02/understanding-the-intentions-of-child-sexual-abuse-material-csam-sharers/).

- Die Chatkontrollen dämmen den Austausch illegalen Materials nicht ein, sondern erschweren die Strafverfolgung von Kindesmissbrauch zusätzlich. Denn sie verdrängen kriminelle Täter in den Untergrund, wo sie kaum noch zu überwachen sind.

- Chatkontrolle schadet der Verfolgung von Kindesmissbrauch, weil sie Ermittler millionenfach mit Computermeldungen überlastet, die zum Großteil strafrechtlich irrelevant sind. Aus dem größten Bundesland NRW wird berichtet, dass für Ermittlungen gegen die Hintermänner, Hersteller der Darstellungen und Missbrauchstäter keine Zeit mehr bleibt: "*Trotzdem kann Sven Schneiders Team momentan nicht mehr an der Aufdeckung großer Kinderpornografie-Ringe mitarbeiten. Aktuell sind seine 85 Mitarbeiterinnen und Mitarbeiter derart ausgelastet mit der Verarbeitung der NCMEC-Hinweise, dass für andere Ermittlungen keine Zeit mehr bleibt.*" (https://www.deutschlandfunk.de/strafverfolgung-sexueller-kindesmissbrauch-datenschutz-100.html).

- Wirklich wirksam wäre die Löschung bekannter Speicherorte ausbeutender Darstellungen im Netz. Weder Bundeskriminalamt noch Europol melden aber bekanntes Missbrauchsmaterial den Speicherdiensten zur Löschung.

Das Max-Planck-Instituts für ausländisches und internationales Strafrecht stellte im Auftrag des Bundesamtes für Justiz schon 2012 fest (http://www.vorratsdatenspeicherung.de/images/mpi_vds_studie.pdf): „Insbesondere gibt es bislang keinen Hinweis dafür, dass durch eine umfängliche Verfolgung aller Spuren, die auf das Herunterladen von Kinderpornografie hindeuten, sexueller Missbrauch über den Zufall hinaus verhindert werden kann." Die Verfolgung von „Kinderpornografie" auf kommerziellen Plattformen führt also – von seltenen Zufällen abgesehen – in aller Regel nicht zu den Missbrauchstätern, die sich in abgeschlossenen Foren austauschen.

Insofern wird die Behauptung der Beklagten entschieden bestritten, ihre „Chatkontrolle" leiste einen „wertvollen Beitrag sowohl zur Identifizierung und Rettung von Opfern als auch zur Ermittlung und Verfolgung von Straftaten im Zusammenhang mit sexuellem Missbrauch von Kindern". Die Beklagte vermag dafür nicht auch nur ein einziges Beispiel anzuführen, geschweige denn eine über Zufälle hinaus gehende, signifikante Zahl von Fällen. Dass die „Chatkontrolle" nicht signifikant zur Verfolgung von Missbrauchsdelikten beiträgt, wurde bereits ausgeführt. Zur Identifizierung und Rettung von Opfern kann die Chatkontrolle der Beklagten schon deshalb nicht beitragen, weil sie sich nach deren eigenem Vortrag auf „Systeme zur Erkennung bekannter

CSAM“ beschränkt. Die Suche nach bereits bekannten Ausbeutungsdarstellungen leistet offensichtlich keinen weiteren Beitrag zur Identifizierung von Opfern.

Bestritten wird auch, die „Chatkontrolle“ der Beklagten trage „zur Verringerung der Weiterverbreitung“ von Ausbeutungsdarstellungen bei. In Wahrheit befindet sich die Zahl der Verdachtsmeldungen der Beklagten auf einem historischen Höchststand – offensichtlich völlig unbeeindruckt von deren Chatkontrolle. Dass bestimmte Nutzer durch die Chatkontrolle der Beklagten in geschützte (z.B. selbst betriebene, verschlüsselte) Kanäle verdrängt worden sein mögen und dort überhaupt nicht mehr zu verfolgen sind, wäre kein Vorteil, sondern ein erheblicher Nachteil der Chatkontrolle.

Richtig ist allein, dass sich mit der verdachtslosen „Chatkontrolle“ der Beklagten die Verbreitung bereits bekannter Ausbeutungsdarstellungen über den „Facebook Messenger“ häufiger verfolgen lässt. Dieser Nutzen steht jedoch außer jedem Verhältnis zu dem Schaden infolge einer flächendeckenden Durchsuchung privater Nachrichten sowie auch der kontraproduktiven Effekte.

Die Regelung der ePrivacy-Ausnahmeverordnung 2021/1232/EU und die sich darauf berufende, streitgegenständliche Kommunikationsdurchleuchtung der Beklagte, sind – wie oben zitiert – nach wissenschaftlicher, kriminologischer Einschätzung für den Schutz von Kindern wertlos. Es handelt sich um Aktionismus und werbende Selbstdarstellung.

cc) Verhältnismäßigkeit im engeren Sinne

Die Zulassung privatisierter, flächendeckender anlassloser Überwachung privater Kommunikation ist kein verhältnismäßiges Mittel, um den sexuellen Missbrauch von Kindern im digitalen Bereich zu bekämpfen.

Zusätzlich zu den bereits in der Klageschrift angeführten Nachweisen kommt nun auch der wissenschaftliche Dienst des Bundestages zu dem Ergebnis (https://www.bundestag.de/resource/blob/914580/9eba1ff3a5daa7708fca92e3184a1ae3/WD-10-026-22-pdf-data.pdf): „Es erscheint unwahrscheinlich, dass eine grundsätzliche Überwachung von Individualkommunikation der Überprüfung der (europäischen) Grundrechte standhalten würde.“

Dass die ePrivacy-Ausnahme-VO die deutschen Vorschriften über das Berufsgeheimnis „unberührt“ lasse, wie die Beklagte vorträgt, ist eine absurde und eindeutig falsche Behauptung. Wie soll etwa ein Nebenklagevertreter im Strafprozess, der ein

Missbrauchsopfer vertritt und mit diesem digital kommuniziert, das Berufsgeheimnis noch gewährleisten? Wie soll ein Psychotherapeut, der ein Opfer oder einen Täter therapiert und mit diesem in digitalem Kontakt steht, noch die Vertraulichkeit gewährleisten?

Die Beklagte möge darstellen, ob und durch welche Maßnahmen sie verhindert, dass auch die Kommunikation von Missbrauchsopfern sowie deren Therapeuten und Rechtsberatern automatisch durchleuchtet und weitergegeben wird. Sie ist dazu nicht imstande.

Die Beklagte zitiert das EuGH-Grundsatzurteil vom 6. Oktober 2020 – La Quadrature du Net u. a. -, C-511/18 u.a. selektiv und dadurch falsch. Dieses Urteil befasst sich mitnichten nur mit einer anlasslosen Speicherung von Verkehrs- oder Standortdaten, sondern auch mit der automatisierten Analyse von Telekommunikationsdaten. Nach Rn. 43 des Urteils war verfahrensgegenständlich nämlich u.a. ein Gesetz, nach dem Telekommunikationsanbieter automatisiert anhand bestimmter Parameter bestimmte verdächtige „Verbindungen aufspüren“ sollten. Dieses Verfahren ist der beklagtenseite praktizierten Chatkontrolle ähnlich. In Ziff. 2 des Tenors hat der Gerichtshof dazu wörtlich entschieden (Auszug):

„Art. 15 Abs. 1 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung ist im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte dahin auszulegen, dass er einer nationalen Regelung nicht entgegensteht, mit der den Betreibern elektronischer Kommunikationsdienste auferlegt wird, … eine automatisierte Analyse … insbesondere von Verkehrs- und Standortdaten … vorzunehmen, sofern … der Rückgriff auf die automatisierte Analyse auf Situationen beschränkt ist, in denen sich ein Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht...“

Zur Verfolgung schwerer Straftaten hat der Gerichtshof eine automatisierte Analyse der Telekommunikation gerade nicht zugelassen (vgl. Rn. 177 des Urteils). Zur Begründung hat er ausgeführt, dass eine automatisierte Überwachung abschreckende Wirkung auf die freie Meinungsäußerung haben kann und auch Personen betrifft, die in keinem auch nur mittelbaren oder entfernten Zusammenhang mit terroristischen Aktivitäten stehen. Es handele sich um einen „besonders schweren“ Grundrechtseingriff (Rn. 177).

Wenn also schon die automatisierte Analyse der näheren Umstände der Telekommunikation auf Ausnahmefälle einer Bedrohung der nationalen Sicherheit (z.B.

drohender Terroranschlag) beschränkt ist, so muss dies erst recht für eine automatisierte Analyse der Inhalte der Telekommunikation gelten.
Das EuGH-Urteil bezieht sich auf eine verpflichtende Kommunikationsanalyse, jedoch erläutert bereits die Klageschrift, warum mit einer „freiwilligen" Kommunikationsanalyse kein weniger tiefer Grundrechtseingriff verbunden ist.

Dass der EuGH demgegenüber eine automatisierte Analyse von Flugreisedaten für verhältnismäßig hält, steht dem nicht entgegen. Diese Rechtsprechung ist aus verschiedenen Gründen nicht auf die beklagtenseits praktizierte Chatkontrolle privater Korrespondenz übertragbar:

- Flugreisedaten geben zwar über Flugreisebewegungen zwischen Flughäfen Aufschluss. Diese Information ist aber nicht annähernd so sensibel wie die Gesamtheit der Inhalte privater Kommunikation zum privaten und geschäftlichen Umfeld einer Person. Schon die Menge und Häufigkeit privater Kommunikation, die täglich und häufig erfolgt, ist mit Flugreisen nicht zu vergleichen. Auch ist der Inhalt privater Korrespondenz offensichtlich sehr viel sensibler als Flugrouten. Nicht umsonst ist die private Kommunikation durch das Telekommunikationsgeheimnis besonders geschützt. Und nur bezüglich privater Kommunikation hebt der EuGH den gleichzeitigen Eingriff in die freie Meinungsäußerung hervor, während dieser bei einer Flugreisedatenspeicherung keine Rolle spielt. Dementsprechend spricht der EuGH bei der automatisierten Analyse von Telekommunikation von einem „**besonders** schweren" Grundrechtseingriff (EuGH, vom 6. Oktober 2020 – La Quadrature du Net u. a. -, C-511/18 u.a., Rn. 177), bei Flugreisedaten aber nur von „schwerwiegenden Eingriffen" (EuGH, Urteil vom 21. Juni 2022 – Ligue des droits humains –, C-817/19, Rn. 111).
- Auch bei Flugreisedaten hat der EuGH eine automatisierte Analyse nur zugelassen, soweit Flüge in oder aus der EU betroffen sind. Innereuropäische Flüge dürfen demgegenüber in der Regel nicht verarbeitet werden (EuGH, Urteil vom 21. Juni 2022 – Ligue des droits humains –, C-817/19, Ziff. 7 des Tenors). Wenn nicht eine akute Terrorgefahr besteht, muss die Analyse auf besonders gefahrenträchtige Flugverbindungen, Reisemuster oder Flughäfen beschränkt werden (a.a.O.). Eine völlig wahlloses und flächendeckendes Scannen, wie es die Beklagte für private Kommunikation vornimmt, wurde somit nicht (einmal) für Flugreisedaten zugelassen.

Dass der EuGH mit seinem Urteil vom 21. Juni 2022 zu Flugreisedaten nicht von seiner Rechtsprechung zum besonderen Schutz privater Kommunikation abweichen wollte,

ergibt sich auch daraus, dass er diese Rechtsprechung nachfolgend mit Urteil 20. September 2022 – Spacenet u.a. -, C-793/19 u.a. erneut bestätigt und bekräftigt hat.

2. Verletzung des allgemeinen Persönlichkeitsrechts und des Rechts auf informationelle Selbstbestimmung des Klägers

Den entsprechenden Ausführungen des Klägers tritt die Beklagte nicht entgegen.

3. Verletzung der Art. 5 Abs. 1 lit. a und Abs. 2 i.V.m. Art. 6 Abs. 1 DSGVO

Obwohl es wegen der vorgenannten Rechtsverletzungen unerheblich ist, ob außerdem ein Verstoß gegen die DSGVO vorliegt, soll vorsorglich auf den Vortrag der Beklagten dazu eingegangen werden.

Die Verarbeitung der klägerischen Kommunikationsinhalte durch die Beklagte im Rahmen der „Chatkontrolle“ ist rechtswidrig, weil keine der in Art. 6 Abs. 1 DSGVO aufgezählten Bedingungen erfüllt sind.

a) Das CSAM-Scanning ist nicht unter Art. 6 Abs.1 lit.d) DSGVO zu fassen. Unter das Tatbestandsmerkmal fallen Notstandssituationen sowie schwere medizinische Fälle, wie etwa die Blutabnahme zur Ermittlung der Blutgruppe bei bewusstlosen Unfallopfern (s. Ehmann/Selmayr/Heberlein, 2. Aufl. 2018, DSGVO Art. 6 Rn. 18, vgl. auch Kühling/Buchner/Buchner/Petri, 3. Aufl. 2020, DS-GVO Art. 6 Rn. 106).

   Die Beklagte hat schon nicht dargetan (und kann nicht dartun), dass das Leben irgendeiner Person in Gefahr sei. Im Übrigen kann die „Chatkontrolle“ wie bereits ausgeführt zur Identifizierung von Opfern und Verhinderung weiterer Übergriffe schon deshalb nicht beitragen, weil nach eigenem Vortrag der Beklagten nur „Systeme zur Erkennung bekannter CSAM“ eingesetzt werden. Die Suche nach bereits bekannten Ausbeutungsdarstellungen leistet offensichtlich keinen weiteren Beitrag zur Identifizierung von Opfern und deren Schutz.

b) Art. 6 Abs. 1 lit.e) (Erfüllung einer dem öffentlichen Interesse dienenden Aufgabe)

   Der Rechtfertigungsgrund des Art. 6 Abs. 1 lit.e) DSGVO ist nicht einschlägig.

   Gemäß Art. 6 Abs. 3 DSGVO setzt er nämlich voraus, dass ein Spezialgesetz eine Rechtsgrundlage für die Datenverarbeitung schafft. Ein solches Spezialgesetz gibt es nicht. Insbesondere schafft die ePrivacy-Ausnahmeverordnung 2021/1232/EU keine Rechtgrundlage. Sie soll laut Erwägungsgrund 9 lediglich sicherstellen, dass die DSGVO anstelle der ePrivacy-Richtlinie

Anwendung findet. Sie soll die Rechtslage wiederherstellen, die bestand, bevor der Anwendungsbereich der ePrivacy-Richtlinie auf Internet-Kommunikationsdienste (sog. OTT-Dienste) erstreckt wurde. Laut Erwägungsgrund 10 schafft die ePrivacy-Ausnahmeverordnung folglich „keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch Anbieter zum alleinigen Zweck der Aufdeckung von sexuellem Missbrauch von Kindern im Internet“.

Auch ist der Anwendungsbereich des Art. 6 Abs. 1 lit.e) DSGVO auf behördliche oder staatlich veranlasste Verarbeitungsvorgänge beschränkt (vgl. z.B. BVerwG, Urteil vom 27.03.2019 - BVerwG 6 C 2.18, Rn. 45). Die eigenmächtige „Chatkontrolle“ der Beklagten ist nicht staatlich veranlasst. Die Beklagte ist (wohl unstreitig) weder Hoheitsträger, noch Beliehene.

c) Art. 6 Abs. 1 lit.f) (berechtigte Interessen Dritter)

Die Voraussetzungen des Art. 6 Abs. 1 lit.f) DSGVO liegen nicht vor.

Gem. Art. 6 Abs. 1 lit. f DSGVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die datenschutzbezogenen Interessen, Grundrechte und Grundfreiheiten des Betroffenen nicht überwiegen (vgl. BeckOK DatenschutzR/Albers/Veit, 41. Ed. 1.11.2021, DS-GVO Art. 6 Rn. 63).

Die auf Ausbeutungsdarstellungen abgebildeten Kinder haben ein berechtigtes Interesse daran, dass ihre Darstellungen nicht weiterverbreitet werden. Zur Wahrung dieses Interesses wäre es aber ausreichend, wenn die Beklagte den Versand entsprechender Darstellungen über ihren Dienst blockieren würde. Darüber hinaus den Kommunikationsinhalt gegenüber Unternehmensmitarbeitern, der US-Nichtregierungsorganisation NCMEC und Behörden gegenüber zu offenbaren, ist nicht erforderlich, um die Weiterverbreitung zu verhindern (sondern stellt selbst eine Weiterverbreitung dieses Materials dar).

Art. 6 Abs. 1 lit.f) DSGVO kann es rechtfertigen, Daten zur Verhinderung und Aufklärung von Straftaten zu verarbeiten, allerdings nur von Straftaten zulasten des Datenverarbeiters (z.B. Videoüberwachung zur Verhinderung von Raub). Es ist nicht Aufgabe eines Privatunternehmens, allgemein die Rechtmäßigkeit des Verhaltens seiner Kunden zu überwachen, schon gar nicht im Fall privater Telekommunikation. Dabei handelt es sich um ein öffentliches Strafverfolgungsinteresse, welches wahrzunehmen Sache des Staates gemäß Art. 6 Abs. 1 lit. e DSGVO wäre; dieser setzt allerdings aus guten Gründen nicht auf eine verdachtslose Chatkontrolle (dazu sogleich).

Darüber hinaus kommt Art. 6 Abs. 1 lit.f) DSGVO zur Verhinderung und Aufklärung von Straftaten nur in Betracht, wo eine Gefährdungslage besteht, die über das allgemeine Lebensrisiko hinausgeht (BVerwG, Urteil vom 27.03.2019 - BVerwG 6 C 2.18, Rn. 28). Dies ist bei der Beklagten, dem Dienst „Facebook Messenger“ und auch dem Kläger, der in keiner auch nur entferntesten Verbindung mit entsprechenden Delikten steht, nicht der Fall. Die wahllose, flächendeckende Durchsuchung jeglicher privaten Korrespondenz zielt vielmehr offensichtlich auf das allgemeine Risiko des Missbrauchs der Telekommunikationstechnik zum Versand strafbarer Inhalte ab, welches bei jeglicher Telekommunikation nicht auszuschließen ist, aber sich bei 99,9% der Nutzer nie realisiert. Dieses allgemeine Lebensrisiko kann eine Überwachung nicht rechtfertigen, weil es sonst keine überwachungsfreien Räume mehr gäbe.

Schließlich und vor allem scheitert eine Rechtfertigung der Chatkontrolle nach Art. 6 Abs. 1 lit.f) DSGVO daran, dass die datenschutzbezogenen Interessen, Grundrechte und Grundfreiheiten des Betroffenen das berechtigte Interesse an einer Eindämmung der Verbreitung bekannter Ausbeutungsdarstellungen überwiegen. Die Chatkontrolle der Beklagten ist völlig ungeeignet, um der Verbreitung bekannter Aufnahmen Einhalt zu gebieten, weil die Verbreitung über ihren eigenen Dienst ungeachtet der Chatkontrolle zunimmt (siehe Höchststand der Verdachtsmeldungen der Beklagten) und eine Verbreitung über andere Dienste, insbesondere über selbstverwaltete, dezentrale oder verschlüsselte Dienste, ohnehin technisch nicht zu verhindern ist. Demgegenüber ist der Schaden durch eine wahllose, allgemeine Überwachung sämtlicher privater Kommunikation mithilfe fehleranfälliger Algorithmen extrem groß. Menschen (z.B. Rat- und Hilfesuchende, Patienten, Whistleblower, Kinder, politische Aktivisten) und Berufsgruppen (z.B. Berufsgeheimnisträger), die auf absolut vertrauliche Kommunikation angewiesen sind, können digitale Kommunikationsmittel im Fall einer Chatkontrolle schlicht nicht mehr einsetzen. Da oft (z.B. in Pandemiezeiten) keine zumutbaren Alternativen zur Verfügung stehen, verursacht die Vermeidung wichtiger digitaler Korrespondenz massive Schäden für Einzelpersonen und die Gesellschaft insgesamt. Letztlich entsteht durch die Zerstörung des digitalen Briefgeheimnisses ein Gefühl der ständigen Überwachung, dass eine freie und unbefangene Kommunikation unmöglich macht.

Ergänzend ist anzuführen, dass im Rahmen der durchzuführenden Abwägung gemäß Erwägungsgrund 47 S.1 DSGVO „die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen“, einzubeziehen sind. Die vernünftigen Erwartungen werden dabei geprägt durch das Angebot des Dienstes. Auf ihrer Website (abrufbar unter: https://www.messenger.com/privacy) wirbt die Beklagte unter anderem mit folgendem Absatz für ihren Messenger-Dienst:

> „Mit der Ende-zu-Ende-Verschlüsselung für Nachrichten und Anrufe profitierst du von zusätzlichem Datenschutz und erhöhter Sicherheit. Diese Nachrichten und Anrufe sind nur

für dich und dein Gegenüber zugänglich. Niemand sonst kann diese Chats entschlüsseln – auch wir nicht. Nur wenn du sie uns meldest, können wir darauf zugreifen. Da uns deine Privatsphäre wichtig ist, wird die Ende-zu-Ende-Verschlüsselung standardmäßig für den Messenger festgelegt werden."

Hierdurch entsteht für den Betroffenen der Eindruck, die gesendete Kommunikation finde standardmäßig, durch die erfolgte Ende-zu-Ende Verschlüsselung, in einem besonders geschützten Rahmen statt und die kommunizierten Inhalte seien dem Zugriff des Unternehmens entzogen. Der Betroffene kann daher nicht vernünftigerweise damit rechnen, dass die Beklagte entgegen ihrer Äußerungen in der Beschreibung ihres Dienstes sämtliche Kommunikationsinhalte durchleuchtet und die Ende-zu-Ende Verschlüsselung durch die Datenverarbeitung faktisch umgeht. Dass die Beklagte an anderer Stelle in ihren seitenlangen Bedingungen versteckt und verklausuliert auf die Chatkontrolle hinweist, verschafft dem Durchschnittsnutzer gerade keine Kenntnis.

Ohnehin ist die Chatkontrolle durch die Beklagte wenig wert, wenn vorsätzlich handelnde Straftäter sie durch Aktivierung der Verschlüsselung im Messengerdienst jederzeit abschalten können. Infolgedessen verwundert es nicht, dass die Algorithmen der Beklagten in aller Regel Minderjährige, fahrlässig Handelnde oder überhaupt Unschuldige melden und nur im einstelligen Prozentbereich (https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMST17-4176.pdf. Ermittlungsverfahren überhaupt auch nur eingeleitet werden.

Einzubeziehen in die Beurteilung, ob der Betroffene vernünftigerweise mit der Datenverarbeitung rechnen kann, ist weiter die Branchenüblichkeit der Datenverarbeitung. Die Durchführung eines CSAM-Scannings ist in der Branche der Messengerdienste nicht üblich. Anzuführen sind viele andere Messenger-Dienste, die kein entsprechendes Scanning vornehmen, angeführt von einem anderen Dienst der Beklagten, dem Marktführer Whatsapp, über iMessage, Telegram, Threema oder Signal. Die Beklagte hat selbst angekündigt, im Laufe des nächsten Jahres Nachrichten über den „Messenger" standardmäßig Ende-zu-Ende zu verschlüsseln, und testet diese Funktion bereits (https://about.fb.com/news/2022/08/testing-end-to-end-encrypted-backups-and-more-on-messenger/). Die Ende-zu-Ende-Verschlüsselung wird das Ende der Durchsuchung vertraulicher Kommunikationsinhalte durch die Beklagte bedeuten. Es wird immer weniger Dienste geben, die eine derartige wahllose Durchleuchtung praktizieren. Insofern trifft es nicht zu, dass die Chatkontrolle-Algorithmen der Beklagten „branchenweit anerkannt" wären.

4. Verstoß gegen Art. 9 Abs. 1 DSGVO

Die Verarbeitung der personenbezogenen Daten durch die Beklagte ist weiterhin nach Art. 9 Abs. 1 DSGVO unzulässig.

Im Rahmen des CSAM-Scannings verarbeitet die Beklagte Daten der unter Art. 9 Abs. 1 DSGVO fallenden Kategorien. Bei der Durchleuchtung der Kommunikationsinhalte u.a. werden Informationen betreffend politische Meinungen und Gesundheitsdaten verarbeitet.
Einen Rechtfertigungsgrund hat die Beklagte selbst nicht behauptet. Insbesondere rechtfertigt ein „berechtigtes Interesse“ die Verarbeitung besonders sensibler Daten von vornherein nicht.

5. Verstoß gegen Art. 44, 46 DSGVO

Die Beklagte verstößt ferner gegen die Art. 44, 46 DSGVO dadurch, dass sie personenbezogene Verdachtsmeldungen an die US-amerikanische Nichtregierungsorganisation NCMEC übermittelt. Für die USA liegt kein Angemessenheitsbeschluss nach Artikel 45 Absatz 3 DSGVO vor. Es fehlt auch an geeigneten Garantien und wirksamen Rechtsbehelfen. Dementsprechend hat die irische Datenschutzbehörde im Sommer angekündigt, der Beklagten die Übermittlung personenbezogener Daten in die USA zu untersagen (https://www.politico.eu/article/europe-faces-facebook-blackout-instagram-meta-data-protection/amp/.

Sollten aus Sicht des Gerichts entscheidungsrelevante Sachverhaltsfragen bestehen, wird höflich um Hinweis gebeten.

Prof. Dr. Ralph Wagner LL.M.
Rechtsanwalt