Stellungnahme zum Referentenentwurf eines Gesetzes zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt (GgdG-E)

SO DONE GmbH

22.05.2026

1. Einleitung und zusammenfassende Bewertung 2
1.1 Zivilrechtliche Säule 2
1.2 Strafrechtliche Säule 4
2. Ausführliche Bewertung des zivilrechtlichen Regelungsteils 5
2.1 Identifizierung rechtsverletzender Nutzer 5
2.1.1 Vorgesehenes Auskunfts- und Beweissicherungsverfahren 5
2.1.2 Erweiterung auf mittelbar beteiligte Dienste- und Telekommunikationsanbieter 5
2.1.3 Gerichtsfeste Identifizierbarkeit der Anspruchsgegner 7
2.1.4 Handlungsempfehlungen 8
2.2 Internationale Zuständigkeit 9
2.2.1 Dem Entwurf widersprechende Rechtsprechung 9
2.2.2 Doppelte Schutzlücke 13
2.2.3 Eigener internationaler Gerichtsstand; DSGVO analog 14
2.2.4 Handlungsempfehlungen 15
2.3 Gebührenfreiheit 16
2.3.1 Von der Annahme des Entwurfs abweichende Praxis 17
2.3.2 Handlungsempfehlungen 18
2.4 Durchsetzung von Löschansprüchen gegen Diensteanbieter 20
2.4.1 Schutzlücke im geltenden Recht 20
2.4.2 Handlungsempfehlungen 21

1. Einleitung und zusammenfassende Bewertung

Der Referentenentwurf reagiert auf ein reales und dringendes Problem: Betroffene digitaler Gewalt sind bislang aufgrund materieller Schutzlücken im Strafrecht und prozessualer, kostenrechtlicher und struktureller Hürden im Zivilrecht unzureichend geschützt, so dass die große Mehrheit bestehender straf- und zivilrechtlicher Schutzansprüche nicht durchgesetzt werden kann. Dieser Schutz muss verbessert werden, um zu verhindern, dass sich Menschen vorsorglich aus dem demokratischen Diskurs zurückziehen, weil sie beobachten, wie andere für ihre öffentlichen Meinungsäußerungen mit Beleidigungen und Bedrohungen überzogen werden. Deshalb verdient es entschiedene Zustimmung, den Schutz gegen digitale Gewalt in einigen entscheidenden Aspekten zu verbessern. Um dieses Ziel erfolgreich zu erreichen, bedarf der Entwurf allerdings an zentralen Stellen der Überarbeitung.

1.1 Zivilrechtliche Säule

Trotz des im Grundsatz entschieden zu befürwortenden Gesetzentwurfs weist der zivilrechtliche Regelungsteil an vier zentralen Stellen erhebliche Lücken auf, die seine Schutzwirkung in der Praxis weitgehend gefährden:

1. **Identifizierung der rechtsverletzenden Nutzer:** Der Auskunftsanspruch des § 2 GgdG-E ist auf Diensteanbieter und Internetzugangsdienste beschränkt, deren Dienst unmittelbar zur Begehung der Rechtsverletzung genutzt wurde. Mittelbar beteiligte Anbieter – insbesondere E-Mail-Provider, Mobilfunkanbieter und VPN-Dienste – sind nicht erfasst, obwohl bei ihnen gespeicherte Bestandsdaten regelmäßig zur Identifizierung der Anspruchsgegner erforderlich sind (siehe Abschnitt 2.1). Die beauskunfteten Daten müssen zur gerichtssicheren Durchsetzung gegenüber dem Anspruchsgegner geeignet sein.

2. **Internationale Zuständigkeit:** Die bisherige instanzgerichtliche Rechtsprechung geht – anders als der Referentenentwurf annimmt – nicht davon aus, dass deutsche Gerichte regelmäßig nach Art. 7 Nr. 2 EuGVVO für Auskunftsverfahren gegenüber Plattformen im EU-Ausland zuständig sind. Vielmehr werden Betroffene von einer Vielzahl an Landgerichten und Oberlandesgerichten darauf verwiesen, Verfahren im Ausland anzustrengen. Zudem sind gerade öffentlich sichtbare Personen wie AmtsträgerInnen, JournalistInnen oder WissenschaftlerInnen, die der Entwurf besonders schützen will, vom Verbrauchergerichtsstand in der Regel ausgeschlossen. Ohne eine Änderung dieses Umstandes auf europäischer Ebene droht das neue Instrumentarium in diesem zentralen Bereich somit gänzlich ohne

Wirkung zu bleiben, weil die Ansprüche vor deutschen Gerichten nicht durchgesetzt werden können.

3. **Gerichtskosten:** Der Entwurf nimmt an, die bisherigen Auskunftsverfahren seien gerichtskostenfrei gewesen und daran werde festgehalten – in der Praxis ist allerdings das Gegenteil der Fall. Gerichte erheben in vergleichbaren Fällen des § 21 TDDDG einheitlich Kostenvorschüsse und legen die Verfahrenskosten den Betroffenen auf. Die aktuelle Diskrepanz zwischen intendierter und gelebter Gebührenfreiheit kann nur aufgelöst werden, wenn der Gesetzgeber sie ausdrücklich adressiert – ansonsten bleiben Auskunftsverfahren für Betroffene eine Kostenfalle, insbesondere da Kostenerstattungsansprüche gegenüber Anspruchsgegnern in einer Vielzahl der Fälle nicht durchgesetzt werden können.

4. **Durchsetzung von Löschansprüchen gegen Diensteanbieter**: Eine richterliche Löschanordnung gegen den Plattformbetreiber sieht der Entwurf weder im Rahmen des Auskunftsverfahrens noch als eigenständigen Anspruch vor; eine gerichtliche Löschung ist lediglich akzessorisch zur Accountsperre nach § 4 GgdG-E vorgesehen und an die hohe Schwelle der schwerwiegenden Beeinträchtigung des Persönlichkeitsrechts geknüpft. Außerhalb dieser Konstellation wird eine Löschpflicht nach Art. 6 DSA in Folge einer Inkenntnissetzung des Diensteanbieters nur beim Vorliegen einer offensichtlichen Rechtswidrigkeit ausgelöst. Bei rechtswidrigen, aber nicht offensichtlich rechtswidrigen Äußerungen – etwa Beleidigungen, die erst durch eine rechtliche Prüfung als solche erkennbar sind – können Löschansprüche bisher gegenüber Plattformbetreibern nicht durchgesetzt werden. In diesen Fällen besteht - sofern im Rahmen des Auskunftsverfahrens kein Anspruchsgegner identifiziert werden kann – trotz der Rechtswidrigkeit keine Möglichkeit, die Entfernung der Äußerungen durchzusetzen.

1.2 Strafrechtliche Säule

Die Schließung bestehender strafrechtlicher Schutzlücken, insbesondere durch die Erfassung nicht einvernehmlicher sexualisierter Deepfakes als eigenständigen Straftatbestand, ist zu begrüßen. Dass sowohl das Herstellen als auch das Zugänglichmachen sexualisierter Deepfakes erstmals strafbar sein soll, ist ein wichtiger Fortschritt. Lediglich die Ausgestaltung von § 184k Absatz 1 und § 201b Absatz 1 StGB als Privatklagedelikt kann hinterfragt werden. Die Erfahrung zeigt, dass Verfahren in diesem Rahmen regelmäßig eingestellt und die Geschädigten auf den Privatklageweg verwiesen werden. Da Geschädigte den beschwerlichen und mit hohem Kostenrisiko verbundenen Weg der Privatklage regelmäßig nicht gehen, sind in der Praxis kaum Verurteilungen von Tätern zu erwarten.

Neben den im Gesetzentwurf neu geschaffenen Normen besteht aktuell noch ein gewichtiges Durchsetzungsdefizit bezüglich bestehender strafrechtlicher Vorschriften, sofern zur Begehung einer Straftat ein Digitaler Dienst genutzt wurde, dessen Anbieter seinen Sitz im EU-Ausland hat. Hierbei verweigern einige Diensteanbieter seit einiger Zeit systematisch in vielen der in § 1 Absatz 1 Nr. 2a des Gesetzentwurfs aufgelisteten Straftatbestände kategorisch die Beantwortung von Bestandsdatenauskunftsanfragen deutscher Strafverfolgungsbehörden[1]. Faktisch können deutsche Gesetze auf den betreffenden Plattformen somit von den deutschen Strafverfolgungsbehörden zurzeit nicht mehr durchgesetzt werden, da Rechtshilfeersuchen im Sitzstaat der Diensteanbieter hinsichtlich vieler der in § 1 Absatz 1 Nr. 2a des Gesetzentwurfs genannten Fälle bisher grundsätzlich nicht betrieben werden. Damit in Zukunft geltendes Recht auch im digitalen Raum wieder durchgesetzt werden kann, wird eine konsequente Anwendung der „E-Evidence"-Gesetzgebung[2] entscheidend sein.

[1] Hoppenstedt, Max für DER SPIEGEL: Elon Musk behindert deutsche Ermittlungsbehörden, https://www.spiegel.de/netzwelt/elon-musk-x-gibt-weniger-daten-in-hatespeech-verfahren-an-das-bka-a-58e0b8c2-49aa-44b0-8c4a-8e88150ca198

[2] Verordnung (EU) 2023/1543 und Richtlinie (EU) 2023/1544 sowie deutsches Durchführungs- und Umsetzungsgesetz (*BGBl. 2026 I Nr. 64 vom 12.03.2026)*

2. Ausführliche Bewertung des zivilrechtlichen Regelungsteils

2.1 Identifizierung rechtsverletzender Nutzer

2.1.1 Vorgesehenes Auskunfts- und Beweissicherungsverfahren

Der Entwurf verankert einen eigenständigen Auskunftsanspruch gegenüber bestimmten Diensteanbietern und Anbietern von Internetzugangsdiensten, der über die bisherige Regelung des § 21 TDDDG hinausgeht. Erfasst werden neben Bestandsdaten insbesondere IP-Adressen und Portnummern zum Zeitpunkt der Rechtsverletzung und des letzten Logins sowie eine Kopie des angegriffenen Inhalts. Die Auskunft steht unter Richtervorbehalt; das Gericht prüft die Voraussetzungen in einem an den Grundsätzen des FamFG orientierten Verfahren.

Damit adressiert der Entwurf unmittelbar zwei zentrale Kernprobleme der Praxis: Zum einen das wiederkehrende Scheitern der Rechtsdurchsetzung an der fehlenden Identifizierbarkeit des Verletzers, zum anderen den drohenden Verlust der zur Identifizierung erforderlichen Daten durch kurze Speicherfristen bei Internetzugangsdiensten und Plattformbetreibern.

Positiv hervorzuheben ist zudem die gesetzliche Klarstellung, dass die Auskunftserteilung sowohl gegenüber Diensteanbietern als auch gegenüber Internetzugangsdiensten in einem einheitlichen Verfahren zu erfolgen hat. Dies reduziert bislang notwendige, aufwendig über mehrere Verfahren und Rechtswege zu klärende Schnittstellen und erhöht die Verfahrenseffizienz.

Die Begründung zeichnet zutreffend nach, dass zwischen Rechtsverletzung, Kenntnisnahme durch die betroffene Person, anwaltlicher Beratung, Antragstellung, einer gegebenenfalls notwendigen Zustellung im Ausland und der gerichtlichen Entscheidung regelmäßig mehrere Monate vergehen können. Ohne flankierende Sicherungsmaßnahmen wären die für die Auskunft erforderlichen Daten typischerweise nicht mehr vorhanden. Die Anknüpfung an die Rechtsprechung des Bundesgerichtshofs zur urheberrechtlichen Drittauskunft und zur Sicherung von Verkehrsdaten ist insoweit konsequent.

2.1.2 Erweiterung auf mittelbar beteiligte Dienste- und Telekommunikationsanbieter

Der Anwendungsbereich des Auskunftsanspruchs nach § 2 GgdG-E beschränkt sich auf Diensteanbieter im Sinne des § 1 Abs. 2 GgdG-E sowie Anbieter von Internetzugangsdiensten nach § 1 Abs. 3 GgdG-E, deren Dienste zur Begehung der Rechtsverletzung selbst genutzt wurden. Nicht erfasst sind insbesondere E-Mail-Provider, Mobilfunkanbieter und VPN-Dienste, deren Dienste mittelbar – etwa zur Registrierung

oder Authentifizierung des bei der Rechtsverletzung verwendeten Nutzerkontos – verwendet wurden. Praktisch verbleiben dem Betroffenen damit als verwertbare Anknüpfungspunkte allein die IP-Adresse und Portnummer des inkriminierten Uploads sowie des letzten Logins.

Dies erzeugt einen systematischen Widerspruch innerhalb des Entwurfs selbst: § 2 Abs. 2 Nr. 1 lit. a und Nr. 2 GgdG-E verpflichten Diensteanbieter und Internetzugangsdienste zur Herausgabe gerade auch von E-Mail-Adressen und Telefonnummern. Diese Datenpunkte sind jedoch in der überwiegenden Zahl der praxisrelevanten Konstellationen für sich genommen nicht identifizierend, weil sie bei der Registrierung üblicherweise weder verifiziert noch auf reale Personendaten zurückführbar sind. Ihren Wert für die Identifizierung eines Anspruchsgegners entfalten sie erst, wenn sie als Anknüpfungspunkt für einen weitergehenden Auskunftsanspruch gegenüber dem jeweiligen E-Mail- oder Telekommunikationsanbieter genutzt werden können – genau diese Möglichkeit sieht der Entwurf aber nicht vor.

Die Erfolgschancen eines Auskunftsverfahrens hängen vor diesem Hintergrund maßgeblich davon ab, ob im konkreten Fall mit Hilfe einer beauskunfteten IP-Adresse und Portnummer mit hinreichender Sicherheit ein einzelner Rechtsverletzer als Urheber des rechtsverletzenden Inhalts identifiziert werden kann. Kommen jedoch beispielsweise mehrere Bewohner eines Haushalts, die einen Internetanschluss gemeinschaftlich nutzen, als Urheber in Frage (siehe 2.1.3) oder wurde die Rechtsverletzung unter Nutzung eines VPN-Dienst begangen, läuft die Spur ins Leere. Praktisch verbleibende Anhaltspunkte zur Identifizierung – etwa eine bei der Registrierung hinterlegte Mobilfunknummer oder E-Mail-Adresse – können nach derzeitiger Entwurfsfassung nicht weiterverfolgt werden, weil jeweilig mittelbar beteiligte Drittanbieter vom Auskunftsverfahren nicht erfasst sind.

Dass diese Lücke nicht hypothetisch ist, belegen mehrere obergerichtliche Entscheidungen zum bisher geltenden Recht: Die Rechtsprechung qualifiziert E-Mail-Provider als „nummernunabhängige interpersonelle Telekommunikationsdienste“ im Sinne von § 3 Nr. 61 lit. b TKG. Damit ist bisher der Anwendungsbereich von § 21 Abs. 2 und Abs. 3 TDDDG (vormals TTDSG) nicht eröffnet; eine analoge Anwendung wird mangels planwidriger Regelungslücke abgelehnt, weil der Gesetzgeber E-Mail-Dienste bei Schaffung des § 21 TTDSG bewusst als interpersonelle Telekommunikationsdienste eingeordnet und nicht in den Anwendungsbereich einbezogen habe (BT-Drs. 19/26108, S. 236). Belegt wird dies durch LG Stuttgart, Beschluss vom 27.11.2023 – 24 O 130/23; bestätigt durch OLG Karlsruhe, Beschluss vom 27.10.2023 – 14 U 56/23; OLG Oldenburg, Beschluss vom 15.06.2023 – 13 W 13/23; LG Osnabrück, Beschluss vom 08.03.2023 – 11 O 2554/21. Der Referentenentwurf nimmt diese Rechtsprechungslinie nicht auf und perpetuiert damit eine bereits heute existierende Schutzlücke, die die Erfolgsaussichten von Auskunftsverfahren nach GgdG-E stark verringern wird.

Dasselbe gilt für Mobilfunkanbieter, soweit beim Diensteanbieter, auf dessen Plattform die Rechtsverletzung begangen wurde, eine Mobilfunknummer als Bestands- oder

Verifizierungsdatum hinterlegt war. Die zur Identifizierung der dahinterstehenden Person erforderlichen Bestandsdaten (Vor- und Zuname, Anschrift, ggf. Vertragsdaten) liegen ausschließlich beim jeweiligen Mobilfunkanbieter. Der Referentenentwurf eröffnet jedoch keinen Auskunftsanspruch gegen Mobilfunkanbieter, deren Dienste nicht selbst zur Begehung der Rechtsverletzung, sondern lediglich zur Registrierung oder Verifizierung des Nutzerkontos verwendet wurden. Die im Auskunftsverfahren von der Tatplattform herausgegebene Mobilfunknummer (§ 2 Abs. 2 Nr. 2 GgdG-E) bleibt damit für die Rechtsdurchsetzung regelmäßig wertlos, obwohl gerade dieses Datum in strafrechtlichen Verfahren bisher einer der vielversprechendsten Ansatzpunkte für Identifizierungen ist. Basierend auf den Erfahrungen der Rechtspraxis ist nachdrücklich zu empfehlen, die „sekundären" Auskunftsansprüche nicht auf Internetzugangsanbieter zu beschränken, sondern auf E-Mail-Diensteanbieter und Mobilfunkanbieter zu erweitern, damit in den Bestandsdaten hinterlegte E-Mailadressen und Mobilfunknummern für die Identifizierung von Rechtsverletzern genutzt werden können.

Eine eigenständige, in der Praxis besonders gravierende Konstellation betrifft die Nutzung von VPN-Diensten. Wird die Rechtsverletzung über einen VPN-Anbieter geleitet, ist die beim Internetzugangsdienst des unmittelbar tatbeteiligten Diensteanbieters abgefragte IP-Adresse diejenige des VPN-Servers, nicht des tatsächlichen Nutzers. Ein Rückgriff auf die der VPN-Verbindung zugrunde liegenden Verbindungsdaten – und damit auf den tatsächlichen Anschlussinhaber – ist nach derzeitiger Entwurfsfassung nicht vorgesehen, weil auch VPN-Anbieter nicht zu den im Auskunftsverfahren verpflichteten Anbietern zählen. Die Identifizierungsspur endet damit regelmäßig beim VPN-Server, ohne dass ein zivilrechtlich verwertbares Identifizierungsergebnis erzielt werden kann, was eine sekundäre Auskunftspflicht von E-Mail-Diensteanbietern und Mobilfunkanbietern zu als Bestands- oder Authentifizierungsdaten beim primären Diensteanbieter hinterlegten E-Mail-Adressen und Mobilfunknummern umso wichtiger macht.

2.1.3 Gerichtsfeste Identifizierbarkeit der Anspruchsgegner

Für die effektive Durchsetzung der im Gesetzentwurf vorgesehenen Auskunftsansprüche wird es von entscheidender Bedeutung sein, dass die im Wege des Auskunftsverfahrens erhaltenen Daten geeignet sind, einen Anspruchsgegner eindeutig genug zu identifizieren, sodass die Identifizierung eine für ein zivilgerichtliches Verfahren ausreichende Beweisführung ermöglicht. Personen, denen digitale Persönlichkeitsrechtsverletzungen vorgeworfen werden, ziehen sich regelmäßig auf Schutzbehauptungen zur Gerät- und Accountnutzung zurück; das Auskunftsverfahren muss diesem Verhalten praktisch standhalten können.

In einer typischen Konstellation – ein Mehrpersonen-Haushalt mit einem gemeinschaftlich genutzten Internetanschluss – wird die nach dem Entwurf erlangte Auskunft regelmäßig nicht zu einem eindeutig identifizierbaren Accountinhaber, sondern lediglich zum

Anschlussinhaber führen. Hierbei bleibt sowohl im vorliegenden Gesetzentwurf als auch dem begleitenden Dokument „Ablauf des zivilrechtlichen Verfahrens nach dem Gesetz gegen digitale Gewalt“[3] offen, wie konkret in ihren Rechten verletzte Betroffene weiter vorgehen sollen, nachdem ihnen im Rahmen des Auskunftsverfahrens der Anschlussinhaber bekannt wird. Es sollte daher sorgfältig geprüft werden, wie der Entwurf mit derartigen, in der Praxis sehr typischen Konstellationen umgeht

2.1.4 Handlungsempfehlungen

Um eine effektive Durchführung des Auskunftsverfahrens zu ermöglichen, sollten folgende Anpassungen vorgenommen werden:

- Der Auskunftsanspruch des § 2 GgdG-E sollte auf mittelbar beteiligte Anbieter erstreckt werden, deren Dienste z.B. zur Registrierung bei dem unmittelbar tatbeteiligten Diensteanbieter oder zur Verifizierung des dortigen Nutzerkontos genutzt wurden oder die bei der Rechtsverletzung hilfsweise zum Einsatz kamen, sofern die diesen Anbietern vorliegenden Informationen zur Identifizierung des Rechtsverletzenden erforderlich sind. Hierzu zählen insbesondere E-Mail-Diensteanbieter, Mobilfunkanbieter sowie VPN-Anbieter.

- Das Auskunftsverfahren sollte so ausgestaltet werden, dass es in Mehrpersonen-Konstellationen über die bloße Identifizierung des Anschlussinhabers hinaus zu einer für die zivilrechtliche Rechtsdurchsetzung tragfähigen Identifizierung des tatsächlich verantwortlichen Anspruchsgegners führt.

[3] https://www.bmjv.de/SharedDocs/Downloads/DE/Gesetzgebung/Dokumente/Ablauf_zivilrechtliches_Verfahren_GgdG.html?nn=18816

2.2 Internationale Zuständigkeit

Der Referentenentwurf geht von der internationalen Zuständigkeit deutscher Gerichte für Anträge nach dem GgdG aus und weist darauf hin, dass sich diese „regelmäßig" aus Art. 7 Nr. 2 EuGVVO ergeben wird. Diese internationale Zuständigkeit nach Art. 7 Nr. 2 EuGVVO wird allerdings in der aktuellen Rechtsprechung zu Auskunftsansprüchen nach § 21 TTDSG beziehungsweise § 21 TDDDG, insbesondere in Verfahren gegen große soziale Netzwerke mit Sitz in Irland, regelmäßig abgelehnt. Diese Stellungnahme weist daher eindringlich auf die Erforderlichkeit einer klarstellenden gesetzlichen Regelung zur internationalen Zuständigkeit deutscher Gerichte hin.

2.2.1 Dem Entwurf widersprechende Rechtsprechung

Für die Praxis ist entscheidend, ob die im GgdG-E vorgesehenen Ansprüche überhaupt vor deutschen Gerichten verwirklicht werden können, wenn große Plattformen mit Sitz in Irland betroffen sind. An dieser Stelle klafft eine Lücke zwischen gesetzgeberischer Intention und tatsächlicher Rechtsprechungspraxis.

Der Entwurf geht in seiner Begründung davon aus, dass in Fällen digitaler Gewalt der deliktische Gerichtsstand nach Art. 7 Nr. 2 EuGVVO „regelmäßig" eröffnet sei, wenn sich der Diensteanbieter als Mittelsperson durch Bereitstellung seiner Dienste kausal an der Rechtsverletzung beteilige. Die dokumentierte Rechtsprechung zeigt jedoch, dass die Gerichte gerade diesen Weg nahezu durchgängig versperren. Stattdessen werden Betroffenen auf die Gerichte am Sitz der Plattformen in Irland verwiesen.

Die Landgerichte Ellwangen, Heidelberg, Gießen, Berlin, Mainz, Bamberg, Stendal, München I, Münster, Düsseldorf sowie Bad Kreuznach und die Oberlandesgerichte Stuttgart, Karlsruhe und Köln haben in uns bekannten Auskunftsverfahren nach § 21 TTDSG / § 21 TDDDG die internationale Zuständigkeit deutscher Gerichte verneint. Sie stützen sich dabei übereinstimmend auf eine restriktive Auslegung des Art. 7 Nr. 2 EuGVVO, teilweise ausdrücklich unter Bezugnahme auf den Beschluss des Bundesgerichtshofs vom 28. September 2023 – III ZB 25/21.

Zur Rechtsprechung im Einzelnen:

Das **Landgericht Ellwangen (Jagst)** hat mit Beschluss vom 9. September 2022 – 1 O 27/22 – den Antrag auf Auskunft nach § 21 TTDSG als unzulässig zurückgewiesen, weil es seine internationale Zuständigkeit verneint. Wörtlich heißt es: „Der Antrag ist bereits unzulässig. Es fehlt die internationale Zuständigkeit des angerufenen Landgerichts Ellwangen." Art. 7 Nr. 2 EuGVVO sei nicht einschlägig, weil mit dem Antrag ein Drittauskunftsanspruch gegen die Plattform als Nicht-Störerin geltend gemacht werde; auf Handlungen von Personen, die nicht Partei des Rechtsstreits sind, sei Art. 7 Nr. 2 EuGVVO nicht anzuwenden, und die Verweigerung der Bestandsdatenauskunft stelle keine unerlaubte Handlung dar.

In einem parallel gelagerten Fall hat das **Landgericht Heidelberg** mit Beschluss vom 9. September 2022 – 6 O 8/22 – den Auskunftsantrag ebenfalls als unzulässig verworfen. Es stellt klar, dass „der Antrag […] unzulässig [ist], weil es an der internationalen Zuständigkeit der deutschen Gerichte fehlt". Eine Zuständigkeit nach Art. 7 Nr. 2 EuGVVO verneint das Gericht, weil der Auskunftsanspruch keinen Anspruch aus unerlaubter Handlung gegen die Plattform darstelle, sondern einen eigenständigen gesetzlichen Anspruch; eine unerlaubte Handlung der Plattform liege nicht vor, eine mittelbare Störerhaftung sei nicht erkennbar, und die Verweigerung der Auskunft sei ebenfalls keine unerlaubte Handlung.

Basierend auf ebendieser Begründung hat das **Landgericht Gießen** mit Beschluss vom 18. November 2022 – 4 O 53/22 – den Antrag eines Betroffenen auf Bestandsdatenauskunft zu einem ihn als „Vergewaltiger" bezeichnenden Tweet als unzulässig verworfen, da es an der „internationalen, jedenfalls aber an der örtlichen Zuständigkeit des Landgerichts Gießen fehlt." Art. 7 Nr. 2 EuGVVO sei nicht anwendbar, da der Auskunftsanspruch kein Anspruch aus unerlaubter Handlung sei und die Beteiligte als Nicht-Störerin in Anspruch genommen werde.

Das **Landgericht Berlin** hat mit Beschluss vom 20. April 2023 – 27 O 462/22 – die Anträge eines politisch tätigen Antragstellers auf Gestattung und Verpflichtung zur Auskunftserteilung zurückgewiesen. Das Gericht verweist ausführlich auf den Beschluss des Oberlandesgerichts Stuttgart vom 24. Dezember 2022 – 4 W 91/22 – und übernimmt dessen Argumentation, wonach das Gestattungsverfahren nach § 21 TTDSG zwar eine Zivilsache im Sinne der EuGVVO ist, der deliktische Gerichtsstand nach Art. 7 Nr. 2 EuGVVO aber nicht eröffnet ist, weil eine unerlaubte Handlung der Plattformbetreiberin nicht geltend gemacht wird und die Verweigerung der Bestandsdatenauskunft keine unerlaubte Handlung darstellt.

Das **Landgericht Mainz** hat im Verfahren eines politisch aktiven Antragstellers mit Beschluss vom 16. Dezember 2024 – 1 O 141/24 – den Antrag auf Gestattung der Auskunftserteilung zurückgewiesen. Das Gericht hält fest: „Der Antrag ist als unzulässig zurückzuweisen. Das Landgericht Mainz ist für den Antrag international nicht zuständig." Die internationale Zuständigkeit ergebe sich weder aus Art. 7 Nr. 2 EuGVVO, weil Verfahrensgegenstand nicht eine unerlaubte Handlung der Plattform sei, noch aus Art. 17, 18 EuGVVO, da § 21 TDDDG eine eigene, nicht vertragliche Anspruchsgrundlage darstelle und keine vertraglichen Ansprüche zwischen Nutzer und Plattform Streitgegenstand seien.

Das **Landgericht Stendal** hatte mit Beschluss vom 2. Januar 2025 – 23 O 310/24 – über einen weiteren Auskunftsantrag zu entscheiden. Es weist den Antrag mit der Begründung zurück, das Gericht sei international unzuständig: „Der Antrag ist aufgrund fehlender internationaler Zuständigkeit des Landgerichts Stendal als unzulässig zurückzuweisen." Eine internationale Zuständigkeit aus Art. 7 Abs. 2 EuGVVO bestehe nicht, da das Betreiben der Plattform X als solches keine unerlaubte oder ihr gleichgestellte Handlung darstelle und mit dem Auskunftsverfahren keine Schadenshaftung des Diensteanbieters geltend

gemacht werde; den Anwendungsbereich des Art. 7 Nr. 2 EuGVVO hierauf zu erweitern, liefe dem Grundsatz der restriktiven Auslegung der Ausnahmetatbestände zuwider.

Das **Landgericht München I** hatte im Verfahren einer öffentlich exponierten Person mit Beschluss vom 16. Januar 2025 – 25 O 12737/24 – über einen Auskunftsantrag zu einem Tweet zu entscheiden. Das Gericht formuliert: „Der Antrag erweist sich als unzulässig. Entgegen der Ansicht der Antragstellerin ist das angerufene Gericht für die Entscheidung über den Antrag aus § 21 Abs. 2 TDDDG international unzuständig." Der Anspruch aus § 21 Abs. 2 TDDDG sei nicht deliktischer Natur, setze keinen ursächlichen Beitrag des Diensteanbieters voraus und könne nicht als bloßer Hilfsanspruch zur Durchsetzung deliktischer Hauptansprüche gegen den Verfasser unter Art. 7 Nr. 2 EuGVVO subsumiert werden.

Das **Landgericht Bamberg** hat mit Beschluss vom 18. Dezember 2024 – 32 SH 3/24 e – den Auskunftsantrag einer im Gerichtsbezirk wohnhaften Antragstellerin ebenfalls als unzulässig verworfen. Das Gericht betont, dass die internationale Zuständigkeit nach der EuGVVO zu bestimmen ist und stellt unter ausdrücklicher Bezugnahme auf den Beschluss des Bundesgerichtshofs vom 28. September 2023 – III ZB 25/21 – fest, dass keine deliktischen Ansprüche im Sinne des Art. 7 Nr. 2 EuGVVO Streitgegenstand sind: Das Verfahren nach § 21 TDDDG begründe lediglich einen Auskunftsanspruch „aus Anlass einer unerlaubten Handlung", ohne dass dem Diensteanbieter eine unerlaubte Handlung vorzuwerfen sei.

Das **Landgericht Münster** hat mit Beschluss vom 5. Februar 2025 – 014 O 337/24 – die Anträge eines Antragstellers auf Bestandsdatenauskunft als unzulässig zurückgewiesen. Es führt aus: „Das Landgericht Münster ist international unzuständig." Der besondere Gerichtsstand der unerlaubten Handlung nach Art. 7 Nr. 2 EuGVVO sei nicht eröffnet; zwar diene die Auskunft der Durchsetzung deliktischer Ansprüche gegen einen unbekannten Nutzer, doch genüge dies nach der Rechtsprechung des Bundesgerichtshofs nicht, um im Verfahren nach § 21 Abs. 3 TDDDG den Deliktsgerichtsstand zu begründen. Die Bereitstellung der Plattform allein sei keine unerlaubte Handlung und keine ihr gleichgestellte Handlung, da keine Schadenshaftung der Plattform geltend gemacht werde. Eine Zuständigkeit nach Art. 17, 18 EuGVVO verneint das Gericht ausdrücklich für politisch Tätige; für einen Politiker sei ein privater Verbraucherstatus in der Plattformnutzung nicht dargetan.

Schließlich hat das **Landgericht Düsseldorf** mit Beschluss vom 23. September 2024 – 12 O 164/24 – die internationale Zuständigkeit im Auskunftsverfahren verneint. Der 15. Zivilsenat des Oberlandesgerichts Köln hat die Beschwerde der Antragstellerin mit Beschluss vom 17. Dezember 2024 – 15 W 107/24 – zurückgewiesen. Das OLG Köln hält fest: „Die nach § 21 Abs. 3 Satz 8 TDDDG statthafte und auch im Übrigen zulässige Beschwerde hat in der Sache keinen Erfolg. Das Landgericht hat […] seine internationale Zuständigkeit zutreffend verneint." Der besondere Gerichtsstand der unerlaubten Handlung nach Art. 7 Nr. 2 EuGVVO sei nicht eröffnet, weil die Antragstellerin sich lediglich

auf deliktische Ansprüche gegen einen unbekannten Nutzer berufe; die Bereitstellung der Plattform und die Verweigerung der Auskunft seien keine unerlaubten Handlungen im Sinne von Art. 7 Nr. 2 EuGVVO. Zudem scheide eine Zuständigkeit nach Art. 17, 18 EuGVVO aus, da die Antragstellerin den Nutzungsvertrag mit der Plattform nicht zu einem Zweck geschlossen habe, der nicht ihrer beruflichen Tätigkeit zuzurechnen sei.

Die obergerichtliche Linie wird vor allem vom Oberlandesgericht Stuttgart und vom Oberlandesgericht Karlsruhe geprägt.

Das **Oberlandesgericht Stuttgart** hat mit Beschluss vom 24. Dezember 2022 – 4 W 91/22 – die sofortige Beschwerde gegen den Beschluss des Landgerichts Ellwangen zurückgewiesen. Der Senat formuliert: „Die Beschwerde ist unbegründet. Das Landgericht Ellwangen ist international nicht zuständig." Nach ausführlicher Begründung stellt das Gericht fest, dass das Gestattungsverfahren nach § 21 TTDSG eine Zivilsache im Sinne der EuGVVO ist, die internationale Zuständigkeit aber nach Art. 4 Abs. 1, Art. 63 EuGVVO bei den Gerichten am Sitz der Plattform in Dublin liegt. Art. 7 Nr. 2 EuGVVO sei nicht anwendbar, weil mit dem Antrag „ein Anspruch auf sogenannte Drittauskunft nach § 21 Abs. 2, Abs. 3 TTDSG gegen die Beteiligte als Nicht-Störerin" geltend gemacht werde; auf Handlungen von Personen, die nicht Partei des Rechtsstreits sind, sei Art. 7 Nr. 2 EuGVVO nicht anzuwenden, und die Verweigerung der Bestandsdatenauskunft stelle keine unerlaubte Handlung dar. Eine allgemeine Annexzuständigkeit aus Art. 7 Nr. 2 EuGVVO lehnt das OLG „bereits zum Schutz des Nicht-Störers" ausdrücklich ab.

Das **Oberlandesgericht Karlsruhe** hat mit Beschluss vom 6. Februar 2023 – 7 W 50/22 – die sofortige Beschwerde gegen einen Beschluss des Landgerichts Heidelberg (6 O 8/22) zurückgewiesen. Es bestätigt, dass das Gestattungsverfahren nach § 21 TTDSG eine Zivilsache im Sinne des Art. 1 Abs. 1 EuGVVO ist und die internationale Zuständigkeit daher nach der EuGVVO zu bestimmen ist. Nach ausführlicher Darstellung der Systematik des Art. 7 Nr. 2 EuGVVO kommt der Senat zu dem Ergebnis, dass „keine unerlaubte Handlung der Beteiligten nach Art. 7 Nr. 2 EuGVVO vorliegt", weil der Auskunftsanspruch lediglich formell an eine unerlaubte Handlung eines Dritten anknüpfe und gegen die Beteiligte als Nicht-Störerin gerichtet sei. Die Verweigerung der Auskunft sei „keine eigene unerlaubte Handlung der Beteiligten" im Sinne des Art. 7 Nr. 2 EuGVVO. Auch Art. 8 (Sachzusammenhang) und Art. 18 EuGVVO sind nach Auffassung des Senats nicht einschlägig. Zuständig seien mithin die Gerichte am satzungsmäßigen Sitz der Plattform in Dublin.

Das **Oberlandesgericht Köln** hat in dem bereits genannten Beschluss vom 17. Dezember 2024 – 15 W 107/24 – diese Linie ausdrücklich bestätigt und auf die Entscheidungen des OLG Stuttgart und des OLG Karlsruhe verwiesen. Es kommt zu dem Schluss, dass die im Verfahren entscheidungserheblichen Rechtsfragen durch den EuGH und den Bundesgerichtshof geklärt seien und dass die Verneinung der Voraussetzungen des Art. 7 Nr. 2 EuGVVO den vorgelegten Entscheidungen der Oberlandesgerichte Stuttgart und Karlsruhe entspricht.

Die Linie der Landgerichte wird inhaltlich von diesen obergerichtlichen Entscheidungen getragen und von weiteren Gerichten, etwa dem Landgericht Bamberg, dem Landgericht Münster und dem Landgericht Bad Kreuznach, aufgegriffen. Das **Landgericht Bad Kreuznach** weist in einer Verfügung vom 6. Januar 2025 – 2 O 259/24 – darauf hin, dass sich die internationale Zuständigkeit nach der EuGVVO richtet und Art. 7 Nr. 2 EuGVVO die Zuständigkeit nicht begründet, weil die Antragstellerin deliktische Ansprüche nur gegen den Nutzer, nicht gegen die Plattformbetreiberin geltend macht; eine Zurechnung der Nutzerhandlung und eine unerlaubte Handlung der Plattform seien nicht ersichtlich.

2.2.2 Doppelte Schutzlücke

Die dargestellte Rechtsprechung hat unmittelbare Auswirkungen auf die Zielerreichung des Referentenentwurfs.

Der Entwurf geht in seiner Begründung davon aus, dass sich die internationale Zuständigkeit in Fällen digitaler Gewalt „regelmäßig" über den deliktischen Gerichtsstand nach Art. 7 Nr. 2 EuGVVO begründen lässt, sofern der Diensteanbieter als Mittelsperson einen kausalen Beitrag zur Verbreitung der Rechtsverletzung leistet. Die Gerichte verneinen demgegenüber übereinstimmend eine deliktische Qualifikation von Auskunftsansprüchen nach § 21 TTDSG / § 21 TDDDG gegenüber Plattformbetreibern, solange keine eigene unerlaubte Handlung der Plattform (insbesondere in Form einer Störerhaftung) konkret geltend gemacht wird. Sie stützen sich dabei auf die autonome, restriktive Auslegung des Art. 7 Nr. 2 EuGVVO durch den EuGH und auf den Beschluss des Bundesgerichtshofs vom 28. September 2023 – III ZB 25/21.

Der Bundesgerichtshof hat in III ZB 25/21 entschieden, dass das Gestattungsverfahren nach § 21 Abs. 3 TTDSG in den sachlichen Anwendungsbereich der EuGVVO fällt und der Auskunftsanspruch in diesem Fall keinen deliktischen Gerichtsstand nach Art. 7 Nr. 2 EuGVVO eröffnet, wenn lediglich Auskunft zur Durchsetzung deliktischer Ansprüche gegen einen Dritten begehrt wird. Er hat ausdrücklich offengelassen, ob etwas anderes gilt, wenn sich der Antragsteller zur Begründung seines Auskunftsverlangens auf eine unerlaubte Handlung auch des Anbieters beruft. Die Instanzgerichte lesen diese Offenheit im Zweifel zugunsten einer restriktiven Linie: Sie verlangen, dass im konkreten Verfahren eine Schadenshaftung der Plattform selbst Streitgegenstand ist, und lehnen eine bloße deliktische „Anbindung" über einen Hilfs- oder Annexcharakter des Auskunftsanspruchs gegen die Plattform ab.

Dies führt zu einer doppelten Schutzlücke: zum einen werden Betroffene schwerer digitaler Gewalt faktisch darauf verwiesen, Auskunftsklagen in Irland zu führen. Dies gilt selbst in Fällen offensichtlicher schwerer Persönlichkeitsrechtsverletzungen und strafbarer Inhalte. Zum anderen sind gerade exponierte Personen des politischen Lebens, JournalistInnen, WissenschaftlerInnen, SportlerInnen und andere öffentliche Personen von der Möglichkeit eines Verbrauchergerichtsstands abgeschnitten und damit schlechter gestellt. Das OLG Köln hat explizit entschieden, dass eine Politikerin, die die Plattform

beruflich nutzt, nicht als Verbraucherin im Sinne von Art. 17, 18 EuGVVO anzusehen ist. Das Landgericht Münster verweist in gleicher Richtung darauf, dass ein Politiker seinen Nutzungsvertrag nicht „zu einem Zweck, der nicht seiner beruflichen Tätigkeit zugerechnet werden kann", schließt und daher der Verbrauchergerichtsstand ausscheidet.

Somit werden ausgerechnet Gruppen, die quantitativ und qualitativ mit am stärksten von schwerer digitaler Gewalt betroffen sind, von der Geltendmachung der im GgdG-E vorgesehenen Ansprüche vor deutschen Gerichten ausgeschlossen, da sie weder auf Art. 17, 18 EuGVVO zurückgreifen noch den vom Entwurf angenommenen Art. 7 Nr. 2 EuGVVO für Auskunftsverfahren nutzen können.

Aus der Perspektive des Referentenentwurfs ist die Situation besonders prekär, weil der Entwurf seine verfahrensrechtliche Konzeption – Auskunftsansprüche, Datensicherungsanordnungen, Kontosperren – auf die Prämisse stützt, dass deutsche Gerichte zuständig sind. Dies ist in der tatsächlichen Rechtsprechung faktisch nicht der Fall. Die zitierten Gerichtsentscheidungen machen deutlich, dass die gesetzliche Konzeption ohne eine Klärung der internationalen Zuständigkeit und ohne eine Anpassung des unionsrechtlichen Rahmens Gefahr läuft, die Situation der Betroffenen nicht zu verbessern und damit das eigentliche Ziel des Gesetzes komplett zu verfehlen.

2.2.3 Eigener internationaler Gerichtsstand; DSGVO analog

Im unionsrechtlichen Kontext ist zudem hervorzuheben, dass der europäische Gesetzgeber in anderen Materien bereits gezeigt hat, dass er zur Sicherstellung eines effektiven Individualrechtsschutzes bereit ist, von der allgemeinen Systematik der EuGVVO abzuweichen und in sektorspezifischen Verordnungen eigene Gerichtsstände zu schaffen. Besonders deutlich wird dies im Datenschutzrecht: Art. 79 Abs. 2 DSGVO eröffnet betroffenen Personen ausdrücklich die Möglichkeit, Klage gegen einen Verantwortlichen oder Auftragsverarbeiter wahlweise am Sitz des Verantwortlichen oder an ihrem eigenen gewöhnlichen Aufenthaltsort zu erheben. Diese Norm wird in Rechtsprechung und Literatur als spezielle Zuständigkeitsregel eines besonderen Rechtsgebiets verstanden, die im Anwendungsbereich der DSGVO den allgemeinen Vorschriften der EuGVVO als lex specialis vorgeht. Die DSGVO trägt damit dem Umstand Rechnung, dass Betroffene ihre unionsrechtlich verbürgten Datenschutzrechte realistisch nur dann wahrnehmen können, wenn ihnen ein wohnsitznaher Gerichtsstand zur Verfügung steht und sie nicht auf Verfahren in anderen Mitgliedstaaten verwiesen werden.

Eine vergleichbare Konstellation liegt im Bereich der digitalen Gewalt vor. Auch hier besteht ein unionsweit harmonisiertes materielles Regelungsregime, namentlich durch den Digital Services Act, der die Verantwortlichkeiten von Vermittlungsdiensten und Plattformen sowie Verfahrensrechte für Nutzerinnen und Nutzer bei illegalen Inhalten und Hassrede festlegt. Zugleich zeigt die dargestellte instanzgerichtliche Rechtsprechung zu § 21 TTDSG / § 21 TDDDG und Art. 7 Nr. 2 EuGVVO, dass Betroffene digitaler Gewalt faktisch daran gehindert sind, ihre aus dem nationalen und unionsrechtlichen Rahmen folgenden

Ansprüche vor den Gerichten ihres Wohnsitzstaates geltend zu machen, weil die internationale Zuständigkeit regelmäßig am Sitz der Plattform, etwa in Irland, verortet wird. Wenn der europäische Gesetzgeber im Datenschutzrecht einen eigenständigen, betroffenenfreundlichen Gerichtsstand geschaffen hat, um die praktische Wirksamkeit der Datenschutzrechte zu sichern, spricht alles dafür, im Bereich des DSA und der Bekämpfung digitaler Gewalt eine vergleichbare Lösung vorzusehen. Es liegt nahe, auch hier eine spezielle Zuständigkeitsnorm zu schaffen, die den betroffenen Personen einen Gerichtsstand an ihrem gewöhnlichen Aufenthaltsort eröffnet und damit sicherstellt, dass die materiellen Schutzmechanismen des DSA und der nationalen Umsetzungsakte nicht an der Frage der internationalen Zuständigkeit scheitern. Das dies ansonsten zwar in Fällen von Datenschutzverstößen, nicht aber in Fällen von digitaler Gewalt möglich wäre, scheint denkbar unlogisch.

2.2.4 Handlungsempfehlungen

Es drängt sich daher auf, dass der Gesetzgeber im Rahmen des Gesetzgebungsverfahrens zum Gesetz gegen digitale Gewalt

- die dargestellte Rechtsprechung ausdrücklich in der Gesetzesbegründung aufgreift und nicht nur abstrakt auf Art. 7 Nr. 2 und Art. 17, 18 EuGVVO verweist,

- klarstellt, dass für die typischen Konstellationen digitaler Gewalt, in denen der Plattformbetreiber mittelspersonenhaft an der Rechtsverletzung beteiligt ist, eine unionsrechtliche Klärung oder Ergänzung notwendig ist,

- insbesondere eine Initiative auf europäischer Ebene anregt, die eine ausdrückliche Zuständigkeitsnorm für Drittauskunftsansprüche gegenüber Plattformen in Fällen digitaler Gewalt schafft,

- die besondere, schlechtergestellte Situation exponierter Personen – vor allem Mandatsträger:innen, Journalist:innen und vergleichbare Personengruppen – anerkennt und ausdrücklich festhält, dass der Verbrauchergerichtsstand für sie regelmäßig nicht zur Verfügung steht

- und auf die in 2.2.3 skizzierte europarechtliche Flankierung hinwirkt.

Nur wenn der Gesetzgeber die Diskrepanz zwischen der intendierten Zuständigkeitslösung und der tatsächlich angewandten Rechtsprechung offen anspricht und politisch wie rechtlich adressiert, kann das Gesetz gegen digitale Gewalt seine Schutzwirkung insbesondere im Verhältnis zu großen Plattformen mit Sitz in Irland entfalten.

Vor diesem Hintergrund ist der Referentenentwurf nachdrücklich zu begrüßen, bedarf aber gesetzgeberischer Klarstellungen und einer europarechtlichen Flankierung, um zu verhindern, dass effektiver Rechtsschutz vor digitaler Gewalt weiterhin an Fragen der internationalen Zuständigkeit scheitert und somit für Betroffene unbrauchbar bleibt.

2.3 Gebührenfreiheit

Ein weiterer Aspekt mit erheblicher Bedeutung für den Referentenentwurf ist die Streitwert- und Kostenpraxis, da die Effektivität des neuen Instrumentariums maßgeblich davon abhängt, ob Betroffene das Verfahren mit einem vertretbaren Kostenrisiko überhaupt anstrengen können. Erschwerend kommt hinzu, dass Qualität, Vollständigkeit und Verwertbarkeit der im Auskunftsverfahren erlangten Daten zum Zeitpunkt der Antragstellung aus Sicht des Betroffenen nicht seriös prognostizierbar sind. Ob die Auskunft am Ende einen klar bestimmbaren Namen und eine ladungsfähige Anschrift liefert oder lediglich eine nicht überprüfbare E-Mail-Adresse und Mobilfunknummer oder eine IP-Adresse, die nur auf einen offenen WLAN-Zugang oder einen Drittanschluss verweist, entzieht sich der Kenntnissphäre des Betroffenen. Gleichwohl trägt er nach geltender Rechtspraxis das volle Kostenrisiko, selbst wenn sich das Auskunftsverfahren im Ergebnis als nutzlos erweist. Der Entwurf ordnet das Verfahren dem FamFG zu und hebt die bisherige Sonderregelung des § 21 Abs. 3 Satz 7 TDDDG auf, die den Verletzten typisiert mit den „Kosten des Verfahrens" belastete. Zugleich wird in der Begründung ausgeführt, an der Gebührenfreiheit des bisherigen Auskunftsverfahrens nach § 21 TDDDG solle festgehalten und diese auf Kontosperrungsverfahren erstreckt werden.

Positiv hervorzuheben ist, dass die Verweisung auf § 81 FamFG die starre Abweichung der bisherigen Rechtslage beendet und dem Gericht die Möglichkeit eröffnet, die außergerichtlichen Kosten nach Billigkeit zu verteilen. Dies erlaubt im Einzelfall eine sachgerechte Kostenverteilung.

Allerdings bedarf diese gesetzgeberische Konzeption klarstellender Optimierung, um dem erklärten Ziel eines „einfachen und kostengünstigen" Instruments zum Schutz vor digitaler Gewalt gerecht zu werden. Der Entwurf geht davon aus, dass es bislang keinen eigenen Gebührentatbestand für das Auskunftsverfahren gegeben habe und die Verfahren daher „gerichtskostenfrei" gewesen seien. Die dokumentierte Praxis der Instanzgerichte zeigt allerdings, ähnlich wie bei der internationalen Zuständigkeit der deutschen Gerichte, ein anderes Bild als der Referentenentwurf annimmt – sie gehen regelmäßig nicht von einer faktischen Gerichtskostenfreiheit aus. Auskunftsverfahren werden in der Praxis als gebührenpflichtige Verfahren behandelt und Kostenvorschüsse erhoben. Hinzu kommt, dass die Gerichte nahezu einheitlich einen Verfahrenswert festgesetzt und die „Kosten des Verfahrens" – einschließlich der gerichtlichen und außergerichtlichen Kosten – unter Hinweis auf § 21 Abs. 3 Satz 7 TTDSG / TDDDG vollständig dem Antragsteller auferlegt haben.

Vor dem Hintergrund, dass ein großer Teil der Urheber digitaler Persönlichkeitsrechtsverletzungen entweder gar nicht erst ausfindig gemacht werden kann und sich ein Großteil der Kostenerstattungsansprüche aufgrund fehlender Zahlungsfähigkeit der Erstschuldner nicht vollstrecken lässt, erzeugt dies ein nicht kalkulierbares und unverhältnismäßiges Gerichtskostenrisiko für die Antragsteller. Diese Lage wird zusätzlich dadurch verschärft, dass ein erheblicher Teil der Verfahren bereits an

der Frage der internationalen Zuständigkeit scheitert. Auch in diesen Fällen, in denen die Gerichte sich für international unzuständig erklären und der Betroffene keinerlei Auskunft erhält, trägt er derzeit dennoch die gesamten Kosten des Verfahrens. Das Kostenrisiko ist damit nicht nur inhaltlich, sondern auch prozessual kaum beherrschbar und gerade für regelmäßig von digitalen Persönlichkeitsrechtsverletzungen betroffenen Personen so unverhältnismäßig hoch, dass die im GgdG-E verankerten Auskunftsansprüche ohne echte und vollständige Gerichtskostenfreiheit für einen beträchtlichen Teil der Opfer von digitaler Gewalt keine systematische Lösung darstellen.

Vor diesem Hintergrund reicht es nicht aus, im Entwurf lediglich deklaratorisch darauf zu verweisen, an der bisherigen Gerichtskostenfreiheit werde festgehalten. Es bedarf vielmehr einer Klarstellung im Gesetzestext, dass für die Verfahren nach dem GgdG – sowohl im Auskunfts- als auch im Kontosperrungsregime – keine Gerichtsgebühren erhoben werden dürfen und Kostenvorschüsse nach dem GNotKG ausgeschlossen sind. Andernfalls wird die bisherige, betroffenenfeindliche Praxis fortwirken, obwohl der Gesetzgeber eine kostenentlastende Neuausrichtung intendiert.

2.3.1 Von der Annahme des Entwurfs abweichende Praxis

Im Kontext der Kostenregelung bietet es sich an, zur Verdeutlichung der Fehleinschätzung des Referentenentwurfs zur bisherigen „Gerichtskostenfreiheit" den Beschluss des Landgerichts Münster vom 28.10.2024 als Beispiel für die tatsächliche Rechtsprechungspraxis heranzuziehen.

Das Landgericht Münster hat in diesem Auskunftsverfahren nach § 21 TDDDG im Verfahren mit Beschluss vom 28. Oktober 2024 (Az. 14 O 337/24) entschieden, „Die beantragte Handlung wird von der Zahlung eines Vorschusses in Höhe von 200 € abhängig gemacht." In den Gründen stellt die 14. Zivilkammer klar, dass nach § 21 Abs. 3 Satz 6 TDDDG in Verbindung mit § 13 GNotKG in erstinstanzlichen gerichtlichen Verfahren, in denen der Antragsteller die Kosten schuldet, die beantragte Handlung von der Zahlung eines Vorschusses in Höhe der für die Handlung oder der für das Verfahren im Allgemeinen bestimmten Gebühr abhängig gemacht werden kann. Das Gericht qualifiziert das Verfahren ausdrücklich als „gerichtliches Antragsverfahren" nach § 21 Abs. 2, 3 Satz 1 TDDDG und leitet die Kostenhaftung der Antragsteller aus § 21 Abs. 3 Satz 7 TDDDG ab. Zur Begründung heißt es weiter, die beantragte Handlung sei „von der Vorschusszahlung durch gerichtlichen Beschluss […] abhängig zu machen, um das Kosteninteresse des Staates zu sichern"; die Höhe des Vorschusses bemisst die Kammer „analog KV GNotKG Nr. 15213"[4].

Diese Entscheidung zeigt in aller Deutlichkeit, dass die spruchrichterliche Praxis nicht von einer faktischen Gerichtskostenfreiheit der Auskunftsverfahren ausgeht, sondern im

[4] Dieser Gebührentatbestand im Kostenverzeichnis in Anlage 1 (zu § 3 Absatz 2) GNotKG bezieht sich auf *„Verfahren über den Antrag auf Erlass einer Anordnung über die Zulässigkeit der Verwendung von Verkehrsdaten*", worunter 6 verschiedene Verfahrensarten, jedoch explizit nicht § 21 TDDDG gelistet sind.

Gegenteil von einem gebührenpflichtigen gerichtlichen Verfahren, in dem ein Vorschuss bis zur Höhe der für die Handlung oder das Verfahren bestimmten Gebühr verlangt werden kann. Das Landgericht Münster stützt sich ausdrücklich auf § 13 GNotKG und das Kostenverzeichnis des GNotKG und behandelt das Auskunftsverfahren kostenrechtlich wie ein reguläres, gebührenpflichtiges Verfahren, in dem das „Kosteninteresse des Staates“ zu sichern sei. Die gerichtliche Praxis, Kostenvorschüsse zu erheben und entsprechende Gebührenpositionen heranzuziehen, steht damit im Widerspruch zu der Annahme des Referentenentwurfs.

Der Referentenentwurf führt aus, für die Durchführung des Auskunftsverfahrens nach § 21 Abs. 2 bis 4 TDDDG gebe es keinen Gebührentatbestand und an diesem Rechtszustand solle festgehalten werden; die Gebührenfreiheit solle zusätzlich auf Kontosperrverfahren erstreckt werden. Zugleich wird betont, dass § 5 GgdG-E – anders als § 21 Abs. 3 TDDDG – keine Abweichung von § 81 Abs. 1 FamFG mehr enthält und damit zur Billigkeitsentscheidung über die Verteilung der Verfahrenskosten unter den Beteiligten zurückkehrt. In der Zusammenschau soll das Verfahren also sowohl gerichtskostenfrei als auch hinsichtlich der außergerichtlichen Kosten durch § 81 FamFG gesteuert sein.

Die dokumentierte Praxis der Instanzgerichte belegt demgegenüber, dass die Gerichte die Auskunftsverfahren nach § 21 TDDDG sehr wohl als gebührenpflichtige Verfahren behandeln und auf dieser Grundlage Kostenvorschüsse anfordern. Damit wird ein konkretes Gerichtskostenrisiko begründet, das sich in der Praxis spürbar auswirkt und vor dem Hintergrund der in einer Vielzahl der Verfahren zur Geltung kommenden Zweitschuldnerhaftung den Opfern ein systematisches Vorgehen gegen erlittene Rechtsverletzungen verunmöglicht.

2.3.2 Handlungsempfehlungen

1. Vor diesem Hintergrund bedarf die Aussage des Referentenentwurfs, an der Gerichtskostenfreiheit der Auskunftsverfahren werde festgehalten, einer gesetzgeberischen Klarstellung: Es sollte unmissverständlich normiert werden, dass das gerichtliche Verfahren nach dem Gesetz gegen digitale Gewalt gerichtskostenfrei im Sinne des Gerichtskostenrechts ist. Dies erfordert eine eindeutige gesetzliche Anordnung, die sowohl die Anwendung des FamGKG als auch des GNotKG insoweit ausschließt und sicherstellt, dass weder Gerichtskosten noch Kostenvorschüsse erhoben werden dürfen. Dies würde der besonderen Struktur des Auskunftsverfahrens Rechnung tragen, in dem der Betroffene die Qualität und Verwertbarkeit der begehrten Daten sowie die Vollstreckbarkeit möglicher Verfahrenskostenerstattungsansprüche ex ante gänzlich nicht überblicken kann und sich die erlangte Auskunft in der Praxis als wertlos für die Rechtsdurchsetzung erweisen kann.

2. Der Gesetzgeber sollte dabei ausdrücklich klarstellen, dass die Verfahrenswertfestsetzung in Auskunfts- und Kontosperrverfahren allein der Bestimmung der außergerichtlichen Kosten dient, nicht jedoch als Grundlage für die Erhebung von Gerichtsgebühren oder Kostenvorschüssen herangezogen werden darf. Nur so kann verhindert werden, dass Gerichte – wie im Fall des Landgerichts Münster – unter Rückgriff auf allgemeine Vorschriften (§ 13 GNotKG, Kostenverzeichnis) weiterhin Vorschüsse und Gebühren festsetzen.

3. Drittens sollte im Hinblick auf die außergerichtlichen Kosten an die Systematik des FamFG angeknüpft und zugleich ein gesetzlich verankerter Regeltypus geschaffen werden, wonach die außergerichtlichen Kosten der Diensteanbieter im Regelfall nicht dem Betroffenen auferlegt werden, soweit sein Antrag nicht offensichtlich missbräuchlich oder völlig aussichtslos war. Dies trägt dem Umstand Rechnung, dass das Auskunftsverfahren eine vorgelagerte, vom Gesetzgeber selbst angeordnete Klärungsstufe ist, deren Nutzen für den Betroffenen von Faktoren abhängt, die außerhalb seiner Einflusssphäre liegen. In der Systematik des FamFG existieren bereits zahlreiche Verfahrensarten, die gerichtskostenfrei geführt werden und bei denen die Kostentragung unter den Beteiligten nach § 81 FamFG gerade nicht schematisch, sondern nach Billigkeit erfolgt – insbesondere im Bereich der Kindschaftssachen und weiterer Schutzverfahren, in denen der Gesetzgeber bewusst auf Gerichtskosten verzichtet, um den Zugang zu gerichtlichem Rechtsschutz unabhängig von der wirtschaftlichen Leistungsfähigkeit zu gewährleisten. An diese bewährte Linie knüpft das Gesetz gegen digitale Gewalt für die Auskunftsverfahren und Kontosperren konzeptionell bereits an; sie sollte folgerichtig auch im Gesetzestext klar verankert werden.

Der Referentenentwurf kann sich daher nicht darauf beschränken, den bisherigen Zustand deklaratorisch als „gerichtskostenfrei" zu beschreiben und fortschreiben zu wollen, sondern muss durch eine eindeutige gesetzliche Regelung sicherstellen, dass Gerichtskosten – einschließlich Vorschüssen – in diesen Verfahren tatsächlich nicht anfallen und die Betroffenen nicht weiterhin einem unkalkulierbaren Kostenrisiko ausgesetzt sind.

Eine solche Klarstellung ist unerlässlich, um den vom Entwurf selbst formulierten Anspruch einer „einfachen und kostengünstigen" Rechtsverfolgung bei digitaler Gewalt rechtlich und praktisch einzulösen. So kann verhindert werden, dass Betroffene einem doppelten Kostenrisiko ausgesetzt sind: einerseits in Bezug auf mögliche Gerichtsgebühren (einschließlich Vorschüssen), andererseits hinsichtlich der eigenen und gegnerischen außergerichtlichen Kosten.

2.4 Durchsetzung von Löschansprüchen gegen Diensteanbieter

Auch wenn das im GgdG-E vorgesehene Auskunftsverfahren begrüßenswerte Fortschritte mit sich bringt, wird eine Vielzahl der Urheber rechtsverletzender Inhalte voraussichtlich auch in Zukunft unidentifizierbar bleiben. In diesen Fällen können Unterlassungs- und Löschansprüche nicht unmittelbar gegen den Rechtsverletzenden durchgesetzt werden; Betroffene sind darauf angewiesen, die Löschung des Inhalts gegenüber dem Plattformbetreiber zu erwirken. Hierfür weist die geltende Rechtslage eine strukturelle Schutzlücke auf, die der Entwurf nicht schließt.

2.4.1 Schutzlücke im geltenden Recht

Eine richterliche Löschanordnung gegen den Plattformbetreiber sieht der Entwurf weder im Rahmen des Auskunftsverfahrens noch als eigenständigen Anspruch vor. Eine gerichtliche Löschung ist lediglich akzessorisch zur Accountsperre nach § 4 GgdG-E vorgesehen (§ 4 Abs. 4 S. 2 GgdG-E) und damit an die hohe Schwelle einer schwerwiegenden Beeinträchtigung des Persönlichkeitsrechts geknüpft. Unterhalb dieser Schwelle – sprich in Fällen von Äußerungen, die rechtswidrig, aber nicht rechtswidrig genug, dass die Rechtswidrigkeit für einen Laien offensichtlich ist, sind – besteht keine Möglichkeit, die Löschung des rechtswidrigen Inhalts gegenüber dem Plattformbetreiber durchzusetzen.

Nach Art. 6 Abs. 1 DSA bleibt die Haftungsprivilegierung eines Hostingdiensteanbieters bestehen, solange er weder „tatsächliche Kenntnis von einer rechtswidrigen Tätigkeit oder rechtswidrigen Inhalten" hat noch sich „Tatsachen oder Umstände bewusst" ist, „aus denen eine rechtswidrige Tätigkeit oder rechtswidrige Inhalte offensichtlich hervorgeht" (lit. a); sie entfällt erst, wenn er nach Erlangung dieser Kenntnis nicht zügig zur Sperrung oder Entfernung der Inhalte tätig wird (lit. b). Die Rechtsprechung – im Anschluss an die zur Störerhaftung entwickelte Linie des BGH – konkretisiert diesen Maßstab dahingehend, dass der Hinweis so konkret gefasst sein muss, dass der Rechtsverstoß ohne eingehende rechtliche oder tatsächliche Überprüfung bejaht werden kann (vgl. LG Münster, Urt. v. 21.10.2022 – 12 O 15/22, m.w.N.). Daraus folgt im Umkehrschluss: In Konstellationen, in denen die Rechtswidrigkeit einer Äußerung erst nach einer ausführlichen rechtlichen Abwägung – etwa zwischen Persönlichkeitsrecht und Meinungsfreiheit – feststellbar ist, geht sie aus dem Inhalt nicht „offensichtlich hervor"; der Plattformbetreiber ist nach derzeitiger Auslegung des DSA nicht zur Löschung verpflichtet.

Die Folge ist eine strukturelle Schutzlücke in all jenen Konstellationen, in denen die Rechtswidrigkeit einer Äußerung nicht auf den ersten Blick erkennbar ist, sondern erst nach einer Abwägung der widerstreitenden grundrechtlich geschützten Belange – insbesondere zwischen allgemeinem Persönlichkeitsrecht und Meinungs- oder Pressefreiheit – feststellbar ist. Solche Äußerungen können nach materiellem Recht regelmäßig rechtswidrig und nicht selten zugleich strafbar sein; die Rechtswidrigkeit geht

aus dem Inhalt jedoch nicht immer im Sinne von Art. 6 Abs. 1 lit. a DSA „offensichtlich hervor" und lässt sich regelmäßig auch nicht „ohne eingehende rechtliche oder tatsächliche Überprüfung" bejahen. Eine Löschpflicht des Plattformbetreibers wird damit gerade in der Konstellation, in der die Rechtswidrigkeit zwar feststeht, ihre Feststellung aber eine rechtliche Prüfung verlangt, regelmäßig nicht ausgelöst.

Für die Betroffenen entsteht hieraus eine doppelt unbefriedigende Lage. Bleiben sie passiv, verbleibt der rechtsverletzende Inhalt dauerhaft online. Gehen sie außergerichtlich gegen den Plattformbetreiber vor und klagen sie im Falle der Nichtlöschung auf Unterlassung, tragen sie das volle Kostenrisiko: Greift die Haftungsprivilegierung nach Auffassung des Gerichts noch, weil die Rechtswidrigkeit nicht hinreichend offensichtlich war, tragen die Geschädigten die vollen Gerichts- und Anwaltskosten, obwohl die Äußerung in der Sache nicht zulässig oder sogar strafbar war. Gerade im Kontext kurzweiliger und dynamischer Debatten in den sozialen Medien, in denen eine zeitnahe Entfernung rechtswidriger Inhalte für die Funktionsfähigkeit des öffentlichen Diskurses besonders wichtig wäre, ist der zivilrechtliche Weg damit faktisch versperrt.

2.4.2 Handlungsempfehlungen

Der Referentenentwurf sollte diese Lücke schließen. Dem steht der DSA nicht entgegen: Art. 6 DSA regelt allein die außergerichtliche Haftung der Plattform für nicht selbst erkannte Inhalte, nicht aber die Befolgung gerichtlicher Anordnungen. Dass eine nationale Regelung den Plattformbetreibern eine richterliche Löschanordnung auferlegen kann, setzt der Entwurf in § 4 Abs. 4 S. 2 GgdG-E selbst voraus – allerdings nur akzessorisch zur Accountsperre. Konsequent wäre es, diesen Mechanismus auf eine eigenständige Löschanordnung im Rahmen des Auskunftsverfahrens nach § 2 GgdG-E zu erweitern: Das Gericht sollte auf Antrag des Betroffenen eine Löschung anordnen können, sobald die Rechtswidrigkeit der Äußerung nach materiellem Recht festgestellt ist – was im Rahmen der Auskunftsanordnung ohnehin vom Gericht geprüft wird.

Zur SO DONE GmbH

Die **SO DONE GmbH** wurde 2022 mit dem Ziel gegründet, Betroffenen digitaler Persönlichkeitsrechtsverletzungen den Zugang zum Recht zu ermöglichen. Im Mittelpunkt steht die Übernahme von Prozesskosten, die für viele Betroffene andernfalls eine unüberwindbare Hürde darstellen.

Zur Identifikation potenzieller Persönlichkeitsrechtsverletzungen zu Lasten Betroffener in den sozialen Medien setzt SO DONE zur Vorfilterung eine eigene Softwarelösung ein. Herausgefilterte Inhalte werden anschließend von einer Partnerkanzlei im Einzelfall geprüft und rechtlich gewürdigt. In aussichtsreichen Fällen unterstützt SO DONE Betroffene durch Prozesskostenfinanzierung die Durchsetzung von Unterlassungs-, Lösch- und Geldentschädigungsansprüchen gegen Urheber digitaler Persönlichkeits-rechtsverletzungen sowie gegen Plattformbetreiber.

SO DONE verbindet technologische Innovation mit einer Lösung, die Betroffenen den Zugang zu rechtsstaatlichen Mitteln ermöglicht und leistet dadurch einen strukturellen Beitrag zur Rechtsdurchsetzung im digitalen Raum.