

**Stellungnahme zu den
Eckpunkten für ein Gesetz gegen digitale Gewalt
des Bundesministeriums der Justiz
(Mai 2023)**



A. Einleitung

Digitale Gewalt und Desinformation sind in ihrer organisierten und massiven Form eine der größten Gefahren für unsere Demokratie. Nicht nur Einzelpersonen werden durch sie aus digitalen Räumen herausgedrängt. Strukturell diskriminierende Angriffe zielen vor allem darauf ab, ganze Personengruppen wie Frauen, LGBTQIA+, Juden und Jüdinnen und viele andere marginalisierte Gruppen, aber auch Kommunalpolitiker*innen, Aktivist*innen und Journalist*innen, einzuschüchtern und aus dem öffentlichen Diskurs herauszudrängen. Ein digitales Gewaltschutzgesetz muss den Anspruch haben, allen Bürger*innen effektiven und effizienten Schutz und die Durchsetzung ihrer Rechte zu ermöglichen. Nur so kann sichergestellt werden, dass in einer offenen und liberalen Demokratie freie Meinungsäußerung im öffentlichen Raum langfristig gewährt bleibt.

Dafür ist in den vergangenen Jahren vor allem im Bereich des Strafrechts durch die Schaffung neuer Straftatbestände viel getan worden. Durch umfangreiche Gesetzespakete konnten einige wichtige Schutzlücken geschlossen werden, sodass durchaus nicht mehr vom „rechtsfreien Raum Internet“ gesprochen werden kann. Dennoch ist das Internet leider noch immer ein rechtsdurchsetzungsfreier Raum. Dies gilt in Teilen für das Strafrecht, wo Ermittler*innen allzu oft an der Identifizierung der Täter*innen scheitern. Es gilt aber vor allem auch für das Zivilrecht, wo die Hürden der Rechtsdurchsetzung für Betroffene schier unüberwindbar erscheinen. Es sind nicht nur die Verfahrenslaufzeiten von mehreren Monaten oder die ungewissen Erfolgsaussichten, die Betroffene von der Inanspruchnahme eines zivilrechtlichen Verfahrens abschrecken. Es sind vor allem die exorbitant hohen Kostenrisiken. In der Regel beträgt der Gegenstandswert bei der Geltendmachung eines Unterlassungsanspruchs 5.000 bis 10.000 Euro pro Äußerung, was Verfahrenskosten in Höhe von mehreren tausend Euro mit sich bringt. Die wenigsten Betroffenen ziehen daher eine zivilrechtliche Rechtsdurchsetzung überhaupt für sich in Erwägung. Beratungsstellen beobachten in der Folge einen erschreckenden Vertrauensverlust in staatliche Institutionen und die Wehrhaftigkeit des Rechtsstaats, wenn es um die Bekämpfung digitaler Gewalt geht. Das Recht scheint den Betroffenen nicht zugänglich und ist es bei objektiver Betrachtung auch nicht, zumindest nicht für Privatpersonen.

Wir begrüßen es daher, dass das Eckpunktepapier nun mehr konkrete verfahrensrechtliche Erleichterungen schaffen will. Diese werden von uns im Grundsatz überwiegend befürwortet. Wir glauben jedoch, dass es einer weiteren Konkretisierung und Ergänzung um weitere Maßnahmen zur Förderung der Rechtsdurchsetzung bei digitaler Gewalt bedarf. Alle angedachten Maßnahmen sollten immer vor dem Hintergrund ihrer Effektivität und Praktikabilität für Privatpersonen bewertet werden.

Konkret geht es hierbei vor allem darum, Verfahren nicht nur zu beschleunigen, sondern auch niedrigschwelliger auszugestalten und kostengünstiger zu machen.

Digitalisierung kann hierbei helfen, Anträge bei den Gerichten durch elektronische Formulare zu ermöglichen. Auskunftsansprüche sollten aus Effizienzgründen verbunden werden. Darüber hinaus müssen Gegenstandswerte von Verfahren bei Äußerungsdelikten herabgesetzt werden, um die Kosten zu senken.

Wir müssen Betroffene wehrhaft machen und befähigen, ihr Recht nicht nur auf dem Papier zu haben, sondern auch in der Praxis durchzusetzen. Dies bedeutet zwangsläufig nicht nur neue Rechtsgrundlagen zu schaffen, sondern deren Umsetzbarkeit für Privatpersonen auch verfahrensrechtlich abzusichern. Das Internet hat in wesentlichen Bereichen auch die Natur von Rechtsverletzungen verändert. Das Recht muss hierauf reagieren. Andernfalls droht das Allgemeine Persönlichkeitsrecht im Internet in der Praxis zur leeren Floskel zu verkommen.

B. Der Auskunftsanspruch, § 21 TTDSG

Das Eckpunktepapier legt zu Recht einen Fokus auf eine Reform der Bestandsdatenauskunft gemäß § 21 Abs. 2, 3 TTDSG. Diese hat aktuell für Betroffene digitaler Gewalt kaum eine praktische Relevanz, was nicht allein den Kosten des Verfahrens geschuldet ist. Vor allem der Umstand, dass das Verfahren derzeit auf die reine Freigabe von Bestandsdaten beschränkt ist, macht es faktisch obsolet. Denn als Bestandsdaten liegen den sozialen Netzwerken oftmals nur ein Pseudonym der jeweiligen Accountinhaber*innen vor, welches im besten Fall auf einen Klarnamen schließen lässt und im schlechtesten Fall keinen zusätzlichen Erkenntniswert mit sich bringt. Ggf. liegt noch eine E-Mail-Adresse oder Telefonnummer vor, die aber nur selten eine Ermittlung der Täter*innen zulässt. Liegen diese Daten vor, können Betroffene sie an die Staatsanwaltschaft weiterleiten, wenn gleichzeitig eine Strafanzeige erstattet wurde. Über eine Akteneinsicht, für die in der Regel eine kostenpflichtige anwaltliche Vertretung erforderlich ist, können sie so mit etwas Glück an die Identität von Täter*innen gelangen. Das aufwändige Prozedere ist aber nur selten erfolgreich. Denn in den meisten Fällen sind die im Zuge des Auskunftsverfahrens nach § 21 TTDSG aktuell beauskunfteten Daten für Privatpersonen schlicht nicht verwertbar.

Aus diesem Grund ist es unbedingt erforderlich und begrüßenswert, den Auskunftsanspruch zu reformieren. Das Eckpunktepapier ist in vielerlei Hinsicht erfreulich detailliert, bedarf jedoch vor allem im Hinblick auf den prozessualen Ablauf der Datenherausgabe weiterer Konkretisierung.

1. Herausgabe von Nutzungsdaten

Die explizite Erstreckung des Auskunftsanspruchs auf die Herausgabe von Nutzungsdaten ist unbedingt zu begrüßen. Während diese früher unter der Geltung des Auskunftsanspruchs gemäß TMG aufgrund des Verweises in § 15 Abs. 5 S. 4 TMG a.F. bereits möglich war, sieht das TTDSG eine solche Möglichkeit bisher nicht vor. Die Rechtsprechung ist bzgl. der Auslegung der Norm in ihrer aktuellen Fassung

jedenfalls eindeutig (OLG Schleswig [9. Zivilsenat], Beschluss vom 23.03.2022 – 9 Wx 23/21), so dass es einer Gesetzesänderung bedarf.

Die Erstreckung der Auskunft auf Nutzungsdaten ermöglicht in erster Linie die zusätzliche Beauskunftung von IP-Adressen. Auch wenn kein Nutzungs- oder Bestandsdatum die Identifizierung der Accountinhaber*innen garantieren kann, ist die IP-Adresse wesentlich wertvoller als ein beim sozialen Netzwerk hinterlegtes Pseudonym oder eine E-Mail-Adresse. Sie sollte daher Bestandteil jeder Auskunft sein.

Da es in Deutschland berechtigterweise keine Vorratsdatenspeicherung gibt, sollte sich der Auskunftsanspruch jedoch nicht lediglich auf die IP-Adresse des Uploads beschränken. Er sollte vielmehr auch die IP-Adresse des letzten Logins enthalten. Diese wurde bereits in früheren von HateAid unterstützten Auskunftsverfahren auf Grundlage des TMG von Diensteanbietern beauskunftet und sollte künftig auch explizit erfasst sein.

IP-Adressen werden abhängig vom Zugangsanbieter (Access-Provider) nur fünf bis sieben Tage, zum Teil jedoch auch nur wenige Stunden, gespeichert. Aus diesem Grund droht selbst im einstweiligen Rechtsschutz und bei Durchführung einer Sicherungsanordnung immer ein Datenverlust, wenn der Zugangsanbieter die IP-Adresse bereits gelöscht haben sollte. Ist diese bereits gelöscht, können auch keine Daten mehr gesichert werden. Die IP-Adresse des letzten Logins ist ein zusätzliches Datum, welches dieses Risiko nicht ausräumt, aber wenigstens eindämmt.

Darüber hinaus sollte das befassende Gericht auf Antrag aussprechen können, dass die Diensteanbieter relevante und konkret bezeichnete Nutzungsdaten wie bspw. die IP-Adresse einer künftigen Anmeldung unverzüglich gegenüber dem Gericht mitteilen muss. Auf diese Weise kann eine Ermittlung der Täter*innen auch in den Fällen gestärkt werden, in welchen die IP-Adressen bereits gelöscht wurden oder für Fallgestaltungen, in welchen bspw. eine Online-Plattform von der Speicherung sonst absieht.

2. Erstreckung auf Fälle der Verletzung absoluter Rechte

Auch diese Anpassung ist grundsätzlich zu begrüßen. Aktuell gilt durch die Beschränkung auf ausgewählte Straftaten für den Auskunftsanspruch nach § 21 TTDSG eine höhere Schwelle als für die zivilrechtliche Rechtsdurchsetzung, die die Auskunft vorbereiten soll. Für die Geltendmachung von Unterlassungs- und Ersatzansprüchen reicht eine Verletzung von Persönlichkeitsrechten nämlich aus, während die Auskunft nur in Bezug auf ganz bestimmte strafbare Äußerungen in Betracht kommt. Dies führt in der Praxis zu Rechtsunsicherheiten, da um die Abgrenzung zwischen „einfachen“ und strafbaren Persönlichkeitsrechtsverletzungen umfangreich gestritten werden kann. Es erscheint sachgerecht, für die Auskunft die gleiche Schwelle anzusetzen, wie für die zivilrechtliche Rechtsdurchsetzung, die sie im Nachgang ermöglichen soll.

Die im Eckpunktepapier angedachte Ausweitung auf alle absoluten Rechte, halten wir jedoch für zu weitreichend. Dies gilt insbesondere wegen der sich hieraus ergebenden Erstreckung auf die Verletzung gewerblicher Schutzrechte, die nicht zwangsläufig als "digitale Gewalt" einzustufen wäre und daher ohnehin außerhalb des Gesetzeszwecks liegt. Insbesondere, weil das Verfahren gerichtskostenfrei ausgestaltet werden sollte, sollte genau hinterfragt werden, welchen Interessen hiermit gedient werden soll. Dies ist auch deswegen wünschenswert, weil so Konkurrenzen zu anderen Rechtsgebieten vermieden werden können. Der überwiegende Teil der hier relevanten Fälle digitaler Gewalt sollte durch eine Erfassung des Allgemeinen Persönlichkeitsrechts abgedeckt sein. Dies erscheint vorzugswürdig gegenüber der limitierenden Einschränkung auf bestimmte Straftaten. Hierdurch könnte eine unbeabsichtigte Erstreckung auf gewerbliche Schutzrechte nach unserem Dafürhalten ausgeräumt werden. Unerwünschte Konkurrenzen könnten sich bspw. beim Richtervorbehalt für eine Drittauskunft in Bezug auf § 101 UrhG ergeben. Dieser ist nämlich weniger streng ausgestaltet und auf die Fälle des § 101 Abs. 9 UrhG beschränkt. Hieraus ergeben sich unter Umständen auch Konkurrenzen mit der dortigen Kostenregelung (Nr. 15213 Anlage 1 GNotKG).

Eine Ausweitung des status quo ist jedoch insbesondere deswegen erforderlich, weil der aktuell geltende Katalog der erfassten Delikte gemäß § 1 Abs. 3 NetzDG zu kurz greift. Er bildet in der Praxis bedeutsame Erscheinungsformen digitaler Gewalt nämlich nicht ab. Hierzu zählen nicht nur Persönlichkeitsverletzungen unterhalb der Strafbarkeitsschwelle, sondern auch Bildrechtsverletzungen, sowie diverse erst kürzlich hinzugefügte Straftatbestände, u. a. die gefährdende Verbreitung personenbezogener Daten gemäß § 126a StGB. Sollte also erneut der Anwendungsbereich des Auskunftsanspruchs über einen Straftatenkatalog erwogen werden, sollte dieser nicht die auf die aktuelle Fassung des NetzDG beschränkt, sondern wenigstens noch um die §§ 192a, 126a, 238, 184, 184c, 184k, 188, 238 StGB, sowie § 33 KUG ausgeweitet werden.

3. Erstreckung auf Anbieter von Messenger- und Internetzugangsdiensten

Die Erstreckung des Anspruchs auf Messenger- und Internetzugangsdienste (Telekommunikationsunternehmen) ist unbedingt erforderlich, um dem Auskunftsanspruch zu einer praktischen Relevanz zu verhelfen. Insbesondere die praxisrelevante IP-Adresse ist für Privatpersonen in Bezug auf eine zivilrechtliche Rechtsdurchsetzung nur nutzbringend, wenn sie mit den dazugehörigen Anschlussinhaber*innendaten verbunden werden kann. Diese können nur von den Zugangs anbietenden beauskunftet werden. Durch weitere Auskunft der Zugangs anbietenden kann dann ein Bezug zum Klarnamen des*der Accountinhaber*in hergestellt werden kann. Es ist daher unentbehrlich, dass künftig auch ein Anspruch gegen Zugangs- bzw. Telekommunikationsanbieter besteht, um die vom sozialen Netzwerk erhaltenen Daten nutzbringend zu verwerten.

Das Eckpunktepapier lässt jedoch den konkreten Ablauf der Datenherausgabe offen. Wir halten es für unerlässlich, dass ein nutzungsfreundliches Verfahren eingeführt

wird. Dieses würde voraussetzen, dass Betroffene digitaler Gewalt mit einer einzigen Antragstellung sowohl die Auskunft vom sozialen Netzwerk als auch den Zugangs- bzw. Telekommunikationsanbietenden erhalten. Praktisch würde dies bedeuten, dass beide Auskünfte aufgrund des gleichen Gerichtsbeschlusses direkt an die Betroffenen zu erteilen sind oder durch das Gericht eingeholt werden müssen.

Zudem sollte sichergestellt werden, dass sich der Anspruch auch auf E-Mail-Provider und Telefonanbietende erstreckt. Regelmäßig sind die E-Mail-Adresse oder eine Telefonnummer die einzigen Bestandsdaten, die beauskunftet werden können. Sie sollten daher auch mit den jeweiligen beim E-Mail-Provider oder Telefonanbietenden hinterlegten Informationen verknüpft werden können.

Nicht durch das Eckpunktepapier geklärt ist die Frage, ob die weiteren Anbietenden u.a. von Telekommunikationsdienstleistungen gemäß § 21 Abs. 4 S. 1 TTDSG auch als Beteiligte im Verfahren auftreten müssen. Obwohl dies dogmatisch richtig wäre, hätte dies bedenkliche Auswirkungen auf die Kosten des Verfahrens, so dass jedenfalls bezüglich der Kostenregelung eine Klarstellung geboten erscheint. Auf diese wird unter Punkt 4. d) noch eingegangen.

4. Effektivere Ausgestaltung des Auskunftsverfahrens

Wie bereits dargelegt, halten wir eine effektive Ausgestaltung des Verfahrens für unerlässlich, um dem Auskunftsverfahren zu praktischer Relevanz zu verhelfen. Das Auskunftsverfahren sollte insbesondere einstufig ausgestaltet werden.

a) Beweissicherungsanordnung

Die geplante, an die gängige Praxis im Urheberrecht angelehnte Sicherung von verfahrensgegenständlichen Daten, ist uneingeschränkt zu begrüßen. Während soziale Netzwerke sowohl Bestandsdaten als auch IP-Adressen ohnehin über lange Zeiträume hinweg speichern, gilt dies nicht für Telekommunikationsanbietende. Eine anlassbezogene Speicherung von IP-Adressen, bzw. deren Zuordnung zu Accountinhaber*innendaten ist von einer anlasslosen Vorratsdatenspeicherung zu unterscheiden. Sie unterliegt nicht den diesbezüglich einschlägigen Bedenken, da die Speicherung der IP-Adressen zu Sicherungszwecken beim Zugangs- bzw. Telekommunikationsanbietenden dann gerade nicht anlasslos, sondern anlassbezogen wegen des Verdachts einer konkreten Persönlichkeitsrechtsverletzung erfolgt. Sie sollte zunächst für die gesamte Dauer des Verfahrens angeordnet werden. Sofern die Einholung der Daten den Betroffenen überlassen werden soll, auch für einen klar umgrenzten Zeitraum nach dessen Abschluss (vgl. Punkt 3). Für diesen Fall ist zu berücksichtigen, dass sich Betroffene nach Zustellung des Auskunftsbeschlusses durch das Gericht zunächst postalisch und unter Fristsetzung von in der Regel zwei Wochen an den Anbietenden, z. B. das soziale Netzwerk wenden müssen, um die Herausgabe der IP-Adresse zu verlangen. Erst im Anschluss daran, könnten sich Betroffene überhaupt an die Zugangsdienst- oder Telekommunikationsanbietenden wenden, um die Herausgabe der

dazugehörigen Anschlussinhaber*innendaten zu verlangen. Die Speicherung sollte nach Abschluss des Verfahrens für drei bis sechs Monate gewährleistet sein.

In der Kommunikation des Gesetzgebungsverfahrens sollte Missverständnissen zum Umfang der Datenspeicherung proaktiv entgegengewirkt werden, um die Akzeptanz des Vorschlags in der Bevölkerung zu erhöhen. Bereits nach Veröffentlichung des Eckpunktepapiers wurde dies z. T. als Vorratsdatenspeicherung durch die Hintertür interpretiert, weil der Eindruck entstand, dass eine neue Pflicht für soziale Netzwerke oder sogar Messengerdienste eingeführt werden solle, Daten von Nutzenden anlasslos zu speichern. Dies ist jedoch nicht der Fall. Das Eckpunktepapier deutet nicht einmal an, dass zusätzliche Speicherpflichten geschaffen werden sollen. Für das Auskunftsverfahren gilt vielmehr: Was nicht gespeichert wird, kann auch nicht herausgegeben werden. Dies muss kommunikativ herausgestellt werden. Es sollte zudem betont werden, dass der Richtervorbehalt eine besonders hohe Hürde darstellt, die vor Missbrauch schützt.

b) Einstweilige Anordnung

Die Geltendmachung des Auskunftsanspruchs per einstweiliger Anordnung ist ebenfalls zu begrüßen. Es ermöglicht einerseits, Datenverlust vorzubeugen und andererseits, Betroffenen digitaler Gewalt eine schnellstmögliche Abhilfe in Aussicht zu stellen. Da das Internet sehr schnelllebig ist und Inhalte digitaler Gewalt hier in kürzester Zeit breite Verbreitung finden, ist Geschwindigkeit auch bei der Rechtsdurchsetzung entscheidend.

c) Video-Verhandlung

Um gerichtliche Verfahren zu beschleunigen und zu modernisieren, ist der Einsatz von Videotechnik begrüßenswert. In Bezug auf das Auskunftsverfahren wird der praktische Nutzen geringer sein als in anderen Bereichen. Er schadet jedoch nach unserer Einschätzung nicht.

d) Klarstellung zur Kostentragung und Deckelung der Streitwerte

Die Auskunftsverfahren sind aktuell mit niedrigen Erfolgsaussichten und hohen Verfahrenskosten verbunden. Die Gerichte erlegen den Antragstellenden regelmäßig nicht nur die Gerichtskosten, sondern auch die eigenen außergerichtlichen Anwaltskosten und die der beteiligten Plattformanbietenden auf. Dies geschieht vor allem unter Berufung auf die Kostenregelung des § 21 Abs. 3 S. 7 TTDSG, die dahingehend ausgelegt wird, dass die gesamten Kosten des Verfahrens von den Antragstellenden zu tragen sind. Dies dürfte wohl dem Wortlaut und der Intention des Gesetzes widersprechen. Denn obwohl gemäß § 21 Abs. 3 S. 7 TTDSG die Kosten der „richterlichen Anordnung“ durch den*die Verletzte*n zu tragen sind, ermöglicht § 81 Abs. 1 FamFG die Teilung der weiteren Verfahrenskosten nach Ermessen des Gerichts. Von dieser Option wird nach der Erfahrung u.a. von HateAid jedoch kaum je Gebrauch gemacht.

Nach unserer Auffassung besteht daher Anlass zu Klarstellungen bei den Kostenregelungen zum Auskunftsverfahren, vor allem in Bezug auf außergerichtliche Kosten. Denn die Praxis, den Antragstellenden die gesamten Kosten des Verfahrens aufzuerlegen, gestützt auf § 21 Abs. 3 S. 7 TTDSG, widerspricht sowohl dem Regelungswortlaut, als auch der gesetzlichen Intention. So war mit dem Regelungsvorbild zu § 21 TTDSG in § 14 Abs. 3 - 5 TMG a.F. bezweckt, dass sich das Verfahren an § 101 Abs. 9 UrhG anlehnt (BT-Drs. 18/13013, S. 24). Dort ist anerkannt, dass sich die gleichlautende Formulierung in § 101 Abs. 9 S. 5 UrhG lediglich auf etwaige Gerichtskosten bezieht. Die Kosten der anwaltlichen Vertretung im Verfahren hingegen sind nach den allgemeinen Regeln zur Kostentragung in §§ 81 ff. FamFG nach Ermessen des Gerichts zu verteilen (BeckOK UrhR/Reber, 37. Ed. 15.01.2022, UrhG § 101 Rn. 20). So kann in der Praxis auch eine entsprechend getrennte Kostentragung ausgesprochen werden (z. B. Schleswig-Holsteinisches Oberlandesgericht, Beschluss vom 5. Februar 2010 – 6 W 26/09). Praktisch bedeutet dies, dass die jeweilige Kostentragung auch separat tenoriert werden muss.

Um hier der jetzigen Praxis entgegenzuwirken, bedarf es einer Klarstellung dahingehend, dass die Antragstellenden nicht automatisch auch die Kosten der anwaltlichen Vertretung der Beteiligten zu tragen haben. Dies ist entscheidend dafür, dass das Verfahren von Betroffenen überhaupt in Anspruch genommen wird. Denn das einseitige Aufkommen für die Anwaltskosten aller Beteiligten stellt schon jetzt eine enorme finanzielle Belastung von mehreren hundert Euro dar und schreckt von der Verfahrensaufnahme ab. Kommen nun weitere Beteiligte im Verfahren hinzu, wie z. B. Zugangs anbietende, könnten sich diese Kosten sogar noch mehr erhöhen. Angesichts dessen, dass im Auskunftsverfahren nach dem FamFG kein Anwaltszwang besteht und der Amtsermittlungsgrundsatz gilt, ist eine anwaltliche Vertretung für professionelle Akteur*innen nicht erforderlich. Diese sollte daher auf eigene Kosten erfolgen.

Insofern ist es uns ein wichtiges Anliegen, dass die Gesetzesbegründung bei der Neuregelung deutlich zum Ausdruck bringen muss, welche Kostenverteilung das Gesetz intendiert. Sollte es hierfür einer Klarstellung im Regelungstext bedürfen, würde HateAid dies ebenso begrüßen.

Darüber hinaus treiben exorbitant hohen Streitwerte die Kosten für ein solches Auskunftsverfahren in die Höhe. Aktuell wird regelmäßig ein Gegenstandswert von 2.000 bis 5.000 Euro pro Äußerung angenommen.

Man gelangt demnach für eine Auskunft zu einer Äußerung zu folgender Kalkulation, wonach für die Kosten einer anwaltlichen Vertretung ca. 400 Euro für die erste Instanz anfallen. Das bedeutet Kosten von mindestens 800 Euro, wenn ein beteiligter Anbieter ebenfalls anwaltlich vertreten ist. Dies sind nur die Kosten für die erste Instanz. Leider kam es in der Vergangenheit in von HateAid unterstützten Fällen bereits vor, dass Diensteanbietende Beschwerde gegen den Beschluss einlegten. Selbst wenn diese unmittelbar zurückgenommen wurde, löst dies regelmäßig die

Gebühren der zweiten Instanz aus, welche ebenfalls den Betroffenen auferlegt wurden.

Wir plädieren daher, wie bereits an anderer Stelle im Familienrecht (z. B. § 51 Abs. 3 FamGKG) geregelt, für das Auskunftsverfahren einen pauschalen Gegenstandswert von 250 Euro, maximal jedoch 500 Euro pro Äußerung festzusetzen. Wir betrachten dies als vorläufige Sofortmaßnahme bis bessere Wege zur Digitalisierung und Vereinfachung des Zivilverfahrens ausgereift sind, die das Verfahren zugänglicher und günstiger machen.

e) Amtsermittlungsgrundsatz

Die Beibehaltung des Amtsermittlungsgrundsatzes nach FamFG ist zu begrüßen. Insbesondere verringert dieser für nicht anwaltlich vertretene Antragstellende die Gefahr einer Präklusion mit Tatsachenvortrag und macht das Verfahren so niedrighschwelliger.

Nach unserem Dafürhalten sollte grundsätzlich bei der Rechtsdurchsetzung gegen digitale Gewalt erwogen werden, Digitalisierung zu nutzen, um Gerichte für Betroffene zugänglich zu machen. Über digitale Formulare könnten Vorfälle digitaler Gewalt für einen strukturierten Tatsachenvortrag leicht abgebildet werden. Insbesondere für einen Auskunftsantrag bestünde wegen der Geltung des Amtsermittlungsgrundsatzes durchaus die Möglichkeit, dass Betroffene den Antrag über ein standardisiertes Formular oder sogar über eine digitale Eingabemaske stellen. Eine Präklusion mit Tatsachenvortrag steht hier gerade nicht zu befürchten. Vielmehr könnten die notwendigen Informationen (URL, die in Rede stehende Äußerung, der in Bezug genommene Inhalte, sowie Screenshots) sehr niedrighschwellig über eine Eingabemaske erfasst werden. Wegen der klaren Zuständigkeitsregel wäre dies sogar recht unkompliziert möglich.

f) Bündelung gerichtlicher Zuständigkeit

Aufgrund der hohen Streitwerte kommt der Bündelung der gerichtlichen Zuständigkeit aktuell keine praktische Relevanz zu. Bei einer Klage auf Unterlassung gegen rechtsverletzende Äußerungen wird regelmäßig ein Streitwert von 5.000 bis 10.000 Euro pro Äußerung angesetzt. Eine Bündelung der Verfahren wird jedenfalls wegen der unterschiedlichen Verfahrensordnungen nicht möglich sein.

Einen echten Mehrwert würde nicht nur eine Bündelung der gerichtlichen Zuständigkeiten beim Landgericht generieren, sondern eine Bündelung des Auskunftsverfahrens mit dem Verfahren zur Entfernung rechtsverletzender Inhalte. Denn obwohl ein Auskunftsverfahren den Plattformen grundsätzlich Kenntnis einer rechtsverletzenden Äußerungen verschaffen kann, kann die Entfernung dieser Inhalte durch die Plattformen damit nicht immer vorausgesetzt werden.

C. Richterlich angeordnete Accountsperrern

Wir befürworten grundsätzlich die durch das BMJ angedachte Einführung richterlicher Accountsperrern als weiteren Baustein zur Rechtsdurchsetzung für Betroffene digitaler Gewalt in hierfür geeigneten Fällen. Der Vorschlag bedarf jedoch an einigen Stellen einer Konkretisierung und Nachbesserung, um die praktische Relevanz zu erhöhen. Dies kann insbesondere durch eine Einbindung zivilgesellschaftlicher Organisationen in die Durchsetzung der Accountsperrern erreicht werden. Zudem muss ein Referentenentwurf die Effektivität eines solchen Verfahrens adressieren, die nach unserem Dafürhalten wegen der hohen Umgehungsgefahr nicht überschätzt werden sollte.

1. Effektivität der Maßnahme

Bedenken in Bezug auf die Effektivität der Maßnahme ergeben sich vor allem aus der Tatsache, dass diese sehr leicht umgangen werden kann. Es liegt auf der Hand, dass sich die gesperrten Accountinhaber*innen jederzeit binnen Minuten neue Accounts anlegen können oder ohnehin bereits über mehrere Accounts verfügen. Zuweilen ist dies sogar offensichtlich. Nach unserer Beobachtung gehen die größten Rechtsverletzungen häufig von Accounts aus, die nur wenige Vernetzungen, bspw. Freund*innen oder Follower*innen, haben und deren Aktivitäten sich vor allem auf das Schreiben von Kommentaren und Teilen von Inhalten beschränken. Dies ist nicht verwunderlich: Um mit gewaltvollen Inhalten eine große Reichweite zu erreichen, braucht ein Account nicht zwingend selbst eine eigene große Reichweite. Es genügt, die eigenen Inhalte in Kommentarspalten anderer großer Accounts zu platzieren und so von deren Reichweite zu profitieren. Denn in der Regel sollen mit diesen Inhalten ohnehin nicht die Personen der eigenen Filterblase erreicht werden. Es geht vielmehr darum, die Betroffenen und ihre Communities einzuschüchtern und mundtot zu machen. Gehen Angriffe von Inhaber*innen sehr großer Accounts aus, sind diese oft (gerade so) nicht rechtsverletzend oder die Identität des*der Täter*in ist bekannt.

Dies betrachten wir vor allem aus Sicht der Betroffenen digitaler Gewalt, die sich dazu entschließen auf eigenes (Kosten-)Risiko ein solches Verfahren zu führen, als kritisch. Denn ein solches Verfahren zu führen ist nicht nur mit dem Einsatz nicht unerheblicher Ressourcen, sondern auch mit einer emotionalen Belastung verbunden. Aus diesem Grund wäre es für Betroffene besonders enttäuschend nach Abschluss des Verfahrens festzustellen, dass dieses wirkungslos geblieben ist und die Täter*innen ihnen nun über andere Accounts nachstellen. Die Gefahr der Umgehung einer solchen Accountsperrern sollte daher durch den Gesetzgeber adressiert und mit entsprechenden Maßnahmen zu ihrer Minimierung bedacht werden. Andernfalls könnte die Maßnahme das ohnehin schon niedrige Vertrauen der Betroffenen in das Funktionieren des Rechtsstaats im Internet weiter schwächen.

Es ist zudem nicht so, dass Betroffene nach der aktuellen Gesetzeslage gegenüber unbekanntem Täter*innen schutzlos gestellt sind. Es besteht bereits jetzt in der Regel eine Störerhaftung der jeweiligen Plattform, wenn diese Inhalte auf eine Meldung hin

nicht entfernen. Dies macht es für Betroffene langfristig erfolgsversprechender, die Plattform selbst in Anspruch zu nehmen, wenn sie untätig bleibt. Infolgedessen können Betroffene – [bei Vorliegen der Voraussetzungen sogar im einstweiligen Rechtsschutz](#)¹ – von der Plattform auch Unterlassen künftiger Verletzungen verlangen, und zwar nicht nur auf den Account des*der Täters*in beschränkt. In Bezug auf die rechtsverletzende Äußerung ist dieser Anspruch durchaus weitreichend, da er eine Verbreitung des Inhalts auch für die Zukunft unterbindet und keiner zeitlichen Beschränkung unterliegt. Dieser Anspruch ist weitreichend und erstreckt sich auch auf [gleiche und sinngleiche Inhalte](#)². Wenn die Plattform den Inhalt trotz Kenntnis nicht entfernt, kommt sogar ein [Anspruch auf Schadenersatz](#)³ bereits jetzt in Betracht (LG Frankfurt am Main, Urteil vom 10.12.2021, Az.: 2-03 O 422/20, nicht rechtskräftig). Diese Verfahren werden von Betroffenen jedoch nur selten proaktiv in Anspruch genommen.

Wir betrachten es zudem als richtig, dass die Accountsperre die ultima ratio bleiben muss. Die Sperrung eines Accounts ist selbst dann, wenn sie vorübergehend ist, eine drastische Maßnahme. Ihre Wirkung im Verhältnis zum*zur Accountinhaber*in geht weit über die Entfernung eines Inhalts hinaus. Dies gilt zumindest dann, wenn es sich tatsächlich um eine Person handelt, die nur diesen einen Account unterhält. Dies lässt sich nicht zweifelsfrei überprüfen. Es ist daher richtig, die Accountsperre an hohe Hürden zu knüpfen. Solche sieht das Eckpunktepapier vor. Es sollte jedoch darauf geachtet werden, dass angesichts der hohen Hürden ein Anwendungsbereich verbleibt. Es ist daher zu hinterfragen, ob eine schwerwiegende und wiederholte Rechtsverletzung wirklich kumulativ vorliegen muss. Denkbar wäre es, diese alternativ auszugestalten oder eine einfache, wiederholte Rechtsverletzung generell ausreichen zu lassen. Denkbar ist sonst allenfalls noch eine Anwendung auf Stalkingfälle oder Accounts, welche sich die gezielte Diffamierung von Politiker*innen und Aktivist*innen zum Ziel gesetzt haben.

2. Alternativen im Digital Services Act

Das Modell der Accountsperre findet jedenfalls bereits im Digital Services Act Berücksichtigung. Dort ist bereits eine generelle Pflicht von Online-Plattformen zur Vornahme von Accountsperren bei wiederholten Rechtsverletzungen vorgesehen, Art. 23 Abs. 1 DSA. Im Gegensatz zum Vorschlag der richterlich angeordneten Accountsperren im Eckpunktepapier ist es hierfür gerade nicht notwendig, dass eine Person mehrfach von einem Account angegriffen wurde. Es genügt vielmehr auch, wenn von einem Account wiederholte Verstöße ausgingen. Die Accountsperren auf Grundlage des DSA haben somit einen breiteren Anwendungsbereich und demnach auch eine höhere praktische Relevanz. Durchgesetzt werden können diese gemäß

¹ LG Frankfurt am Main, Urt. v. 14.12.2022, Az.: 2 03 O 325/22; mehr Informationen unter: <https://hateaid.org/einstweilige-verfuegung-gegen-twitter/>

² LG Frankfurt am Main, Urt. v. 8.4.2022, Az.: 2 03 O 188/21; mehr Informationen unter: <https://hateaid.org/urteil-kuenast-facebook/>

³ LG Frankfurt am Main, Urt. v. 10.12.2021; Az.: 2 03 O 422/20; Urteilstext: <https://hateaid.org/twitter-geldentschaedigung/>

Art. 23 Abs. 1 DSA durch die Aufsichtsbehörde und auch auf Antrag der Betroffenen. Es erscheint uns vorzugswürdig, die Durchsetzung der Aufsichtsbehörde zuzuweisen, anstatt sie den Betroffenen aufzubürden.

Wir regen daher an, dass auch in Deutschland die diesbezüglichen Behörden handlungsfähig ausgestattet werden. Ggfs. sollte gesondert überlegt werden, welche Behörde die Zuständigkeit für die Durchsetzung von Accountsperrern nach dem DSA in Deutschland übernehmen soll. Denkbar erscheint, dass die Landesmedienanstalten, welche bereits jetzt für bestimmte Einzelfallanordnungen gegenüber Online-Plattformen zuständig sind, diese Aufgabe übernehmen. [Auch dies wurde bereits an anderer Stelle vorgeschlagen](#)⁴.

3. Durchsetzung durch NGOs?

Den Praktikabilitätsbedenken könnte man dadurch begegnen, dass gemeinnützige Organisation in Anlehnung an die Vertretungsbefugnis in Art. 86 DSA befähigt würden, die Accountsperrere durchzusetzen. Sie sollten zudem die Möglichkeit haben, nicht nur gegen Accounts vorzugehen, die in der Vergangenheit schon mehrfach eine Person angegriffen haben, sondern auch gegen solche, die wiederholt strafbare und gegen die Allgemeinheit gerichtete Inhalte verbreitet haben. In der Regel wird es sich hierbei wohl auch nicht um unbekannt Accountinhaber*innen handeln, sondern vielmehr um solche, gegen die man andernfalls kaum eine Handhabe hat. Dies entspricht einem [Vorschlag](#)⁵, den die Gesellschaft für Freiheitsrechte bereits früher in den Diskurs einbrachte.

Dies setzt jedoch voraus, dass zivilgesellschaftliche Organisationen auch mit den entsprechenden Ressourcen ausgestattet werden, um dieser Verantwortung nachzukommen. Zivilgesellschaftlichen Organisationen mangelt es bekanntlich an finanziellen und personellen Ressourcen, sodass diese Verantwortung eine zusätzliche Belastung darstellen würde. Für zivilgesellschaftliche Beratungsorganisationen käme der Aufwand für ein solches Verfahren wohl nur in Bezug auf Accounts in Betracht, die entweder Klient*innen der Organisation regelmäßig angreifen oder von denen regelmäßig eine provozierende Agitation ausgeht, welche Klient*innen gefährdet. Dies setzt natürlich voraus, dass diese Agitationen rechtsverletzend sind. Dies ist gerade bei professionellen Akteur*innen oft nicht der Fall.

⁴ Daniel Holznagel, CR-online, 13.4.2023:

<https://www.cr-online.de/blog/2023/04/13/bmj-stellt-eckpunkte-fuer-ein-gesetz-gegen-digitale-gewalt-vor/>

⁵ Gesellschaft für Freiheitsrechte e.V.:

<https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/pm-eckpunkte-gewaltschutzgesetz>

4. Verbindung mit dem Auskunftsverfahren, gleichzeitige Löschanordnung

Will der Gesetzgeber trotz der genannten Bedenken an dem Vorhaben der Anordnung richterlicher Accountsperrern festhalten, sollten gewisse Verfahrenserleichterungen erfolgen:

Die Accountsperrere sollte mit dem Auskunftsverfahren verbunden werden können. So könnten Betroffene, die ohnehin schon zu einer Rechtsdurchsetzung entschlossen sind und den Weg ins Gericht gefunden haben, gleichzeitig eine Accountsperrere als Annex beantragen, wenn sie mehrfach angegriffen wurden.

Zuletzt ist eine temporäre Sperrere von Accounts ohnehin nur dann hilfreich, wenn gleichzeitig die Entfernung der rechtsverletzenden Inhalte bei erneuter Freischaltung sichergestellt wird. Zwar ist eine Onlineplattform theoretisch ab Kenntniserlangung zur Entfernung rechtsverletzender Inhalte nach dem NetzDG verpflichtet und eine solche Kenntnis kann auch durch die Beteiligung in einem solchen Verfahren erlangt werden, allerdings ist nach unserer Erfahrung die bestehende Verpflichtung allein keinesfalls ein Garant für die tatsächliche Entfernung von Inhalten durch die Plattformen. Wird die Entfernung also nicht explizit sichergestellt, werden nach dem Ablauf einer temporären Accountsperrere nicht nur die betreffenden Accounts wieder freigeschaltet, sondern mit ihnen auch die gleichen rechtsverletzenden Inhalte, die zu einer Sperrung geführt haben.

D. Zustellungsbevollmächtigte im Inland

Die Einrichtung von Zustellungsbevollmächtigten im Inland ist aus rein praktischen Gründen uneingeschränkt zu begrüßen. Denn die aktuelle Rechtslage bei der Durchführung zivilrechtlicher Verfahren wird uneinheitlich gehandhabt. Der Zustellungsbevollmächtigte gemäß § 5 NetzDG hat nur einen eng umgrenzten Anwendungsbereich (BGH, Beschluss vom 10.11.2022 – I ZB 10/22). Ist dieser Anwendungsbereich nicht gegeben, wird eine Zustellung bei zufälliger Kenntnis der üblichen Prozessbevollmächtigten direkt an diese unternommen. Andernfalls bleibt aber nur eine Zustellung ins Ausland. Im Fall der großen sozialen Netzwerke ist dies meistens Irland. Im außergerichtlichen Bereich kann eine Zustellung oftmals nicht rechtssicher nachvollzogen werden, was die Einleitung gerichtlicher Schritte verkomplizieren kann. Gelegentlich verlangen die Gerichte auch eine beglaubigte Übersetzung ins Englische, bevor eine Zustellung unternommen wird, und fordern hierfür schnell Vorschüsse von bis zu 2.000 Euro ein. Die Bundesregierung sollte hier alle vorhandenen Spielräume ausschöpfen, statt wegen der bloßen Möglichkeit von europarechtlichen Bedenken auf eine Regelung zu verzichten. Die Vorgaben des DSA sind aus Sicht von Betroffenen digitaler Gewalt unzureichend. Dieser sieht die Einrichtung eines*r Zustellungsbevollmächtigten in lediglich für Behörden und in einem einzigen europäischen Mitgliedstaat vor. Nutzende von Onlineplattformen werden indes an eine elektronische Kontaktstelle verwiesen oder sollen eine

Beschwerde bei der Aufsichtsbehörde einreichen. Beide Verfahren erlauben den Nutzenden jedoch keine rechtssichere Zustellung von Dokumenten, z. B. zur Vorbereitung oder Durchführung gerichtlicher Verfahren.

Langfristig scheint es im Interesse der Betroffenen geboten, einfache und rechtssichere Zustellmöglichkeiten innerhalb der EU durch gesamteuropäische Regeln zum elektronischen Rechtsverkehr zu sichern. So sollte sich die Bundesregierung dafür einsetzen, dass eine rechtssichere und wirksame Zustellung auch auf elektronischem Wege z. B. an eine Kontaktstelle gemäß Art. 12 DSA erfolgen kann.

E. Weitere Empfehlungen

Ein Gesetz zum Schutz vor digitaler Gewalt sollte über die Vorschläge des Eckpunktepapiers hinaus außerdem Regelungen enthalten, um Betroffene bei der Rechtsdurchsetzung zu stärken.

1. Anzeigeformulare und Schriftform des Strafantrags

Eine nicht zu verkennende Hürde bei der Anzeige von Beleidigungsdelikten ist das Strafantragserfordernis gemäß § 194 StGB. Dies gilt vor allem deswegen, weil ein Strafantrag gemäß § 158 Abs. 2 StPO schriftlich gestellt werden muss. Dass eine elektronische Antragstellung, z. B. per E-Mail nicht möglich ist, hat der BGH erst kürzlich durch Beschluss vom 12.05.2022, Az.: 5 StR 398/21, bekräftigt. Die extrem engen Voraussetzungen für den elektronischen Rechtsverkehr im Strafprozessrecht sind in § 32a Abs. 3 StPO geregelt und setzen eine qualifizierte elektronische Signatur sowie einen sicheren Übermittlungsweg voraus. Ob die Übersendung eines gescannten und handschriftlich unterzeichneten Dokuments diesen Anforderungen genügen könnte, ließ der BGH dabei offen.

Praktisch bedeutet dies für Betroffene von Hasskriminalität im Internet, dass diese aktuell sicherheitshalber immer binnen drei Monaten ab der Kenntnisnahme der rechtsverletzenden Inhalte einen handschriftlich unterzeichneten Strafantrag in Papierform einreichen müssen. Dies gilt selbst dann, wenn sie regelmäßig von einer Vielzahl von Hasskommentaren oder -nachrichten betroffen sind. Betroffenen von digitaler Gewalt ist dieser Aufwand aus Kapazitätsgründen nicht zumutbar. Im Ergebnis werden viele Delikte auf diese Weise nur aufgrund bürokratischer Hürden nicht angezeigt. Das Schriftformerfordernis des § 158 Abs. 2 StPO ist schlicht nicht mehr zeitgemäß und sollte in eine Textform umgewandelt werden.

Auf diese Weise wäre sichergestellt, dass wenigstens eine Übersendung eines Strafantrags als PDF-Dokument (§ 32a Abs. 2 StPO; BeckOK StPO/Valerius, 44. Ed.

1.7.2022, StPO § 32a Rn. 6.1) möglich wäre, welches jedoch nicht an die weiteren Voraussetzungen des § 32a StPO gebunden ist. Eine einfache E-Mail wäre jedoch noch immer nicht ausreichend. Fraglich bleibt zudem, ob eine Antragstellung über eine Onlinewache den Vorgaben genügen kann. Da das Schriftformerfordernis hier wohl nach dem Verständnis des BGH unstreitig nicht gewahrt sein wird, käme es darauf an, ob dies der Antragstellung „zu Protokoll“ bei der Staatsanwaltschaft gleichgestellt werden kann, § 158 Abs. 2 StPO. Dies ist ebenfalls fraglich.

Bedauerlicherweise stellt der BGH darauf ab, dass dem Schriftformerfordernis vor allem eine Verifizierungsfunktion zukommen soll. Ausweislich der Gesetzesbegründung ist dies jedoch gerade nicht der vorrangige Zweck. Das Schriftformerfordernis soll vielmehr eigentlich sicherstellen, dass nicht versehentlich Entwürfe in den Umlauf gelangen. Dieser Zweck kann aber auch ohne ein Schriftformerfordernis gewahrt werden. Um die Verifizierung zu gewährleisten, könnten auch technische Wege zur sicheren Übermittlung erwogen werden, solange diese die Belange des Zeug*innenschutzes nicht konterkarieren. Eine Registrierung mit einem Personalausweis z. B. wäre daher abzulehnen.

Wir begrüßen außerdem ausdrücklich die Intention der Bundesregierung, eine bundeseinheitliche Möglichkeit der elektronischen Anzeigeerstattung zu schaffen. In vielen Bundesländern haben sich Online-Meldeportale bewährt, die speziell auf die Meldung von Äußerungsdelikten im Netz zugeschnitten sind (z. B. [Hessen gegen Hetze](#)⁶). Hierbei werden systematisch die relevanten Informationen abgefragt, Screenshots können hochgeladen und URLs eingefügt werden. Zudem werden an den relevanten Stellen auf Möglichkeiten des Zeug*innenschutzes hingewiesen oder sogar eine (zunächst) anonyme Anzeigeerstattung ermöglicht. Diese Angebote halten wir für geeignet, die Zahl der Strafanzeigen zu erhöhen. Ein solches Angebot sollte es flächendeckend geben, wobei ein bundeseinheitliches Formular sinnhaft erscheint. Denn ein umfangreiches Angebot an gut ausgestatteten Anzeigeportalen ist eben nicht einheitlich in allen Bundesländern vorhanden. Dadurch entstehen Bürger*innen in Bundesländern mit unzureichenden Meldemöglichkeiten Nachteile. Wie bereits dargelegt, sollten diese Online-Meldeformulare das Stellenformwirksamer Strafanträge ermöglichen.

Strafverfolgung ist Ländersache. Dem kann und muss in der Ausgestaltung des bundeseinheitlichen Meldeformulars Rechnung getragen werden. So könnte ein solches Meldeformular bspw. durch die Abfrage der Postleitzahl des Wohnsitzes Anzeigeerstatter*innen eine Zuordnung der örtlichen Zuständigkeit ermöglichen und an die zuständigen Stellen in den Ländern ausgeleitet werden. Die Weiterleitung von Sachverhalten innerhalb der Länder sollte zudem unmittelbar an eine auf

⁶ <https://hessengegenhetze.de/>

Internetkriminalität spezialisierte Stelle beim Landeskriminalamt oder der Staatsanwaltschaft erfolgen, wo zeitnah Ermittlungen aufzunehmen sind, um Datenverlust vorzubeugen.

Jedoch haben nicht alle Bundesländer eine solche Stelle und/oder können eine schnelle Bearbeitung der Fälle sicherstellen. Gesteigert werden könnte die Effizienz eines solchen Systems ggf. dadurch, dass eine zentrale Stelle eine Vorsortierung der Sachverhalte vornimmt, wodurch u. a. Duplikate festgestellt werden könnten. Ggf. Wäre das Bundeskriminalamt als Zentralstelle (§ 2 BKAG) hierfür geeignet. Dieses hat immerhin Stellen aufgestockt, um der gescheiterten Meldepflicht gemäß § 3b NetzDG gerecht zu werden.

Zur Sicherstellung eines effektiven Zeug*innenschutzes sollte sowohl in der Onlinewache, als auch bei der analogen Anzeigeerstattung eine verpflichtende Belehrung über die Angabe einer Erreichbarkeitsanschrift (c/o Adresse) erfolgen, § 68 Abs. 2 S. 1 StPO. Bisher hält die vermeintliche Pflicht zur Angabe einer Privatanschrift Betroffene digitaler Gewalt häufig von der Erstattung einer Anzeige ab.

2. Bildbasierte digitale Gewalt

Immer häufiger erreichen qualifizierte Beratungsstellen Fälle bildbasierter digitaler Gewalt. Vor allem sexualisierte Gewalt gegen weiblich gelesene Personen steht hierbei im Vordergrund. Wir betrachten bildbasierte digitale Gewalt als gefährlichste aktuelle Entwicklung im Bereich der digitalen Gewalt. Durch neue Mittel, wie z. B. sog. [FaceSwap-Apps](#)⁷ oder einschlägige Internetseiten sind der Allgemeinheit Technologien zur einfachen, schnellen und professionellen Herstellung sog. Deepfakes zugänglich gemacht worden. Anhand der Inhalte, die in den Beratungsstellen vorgetragen werden, ist längst erkennbar, dass Täter*innen nicht länger intime Bilder stehlen müssen, um diese zu veröffentlichen und Frauen bloßzustellen. Intime Bilder, vor allem pornografische Videos, können jetzt durch die Nutzung entsprechender Apps einfach selbst produziert werden. Dies bringt es mit sich, dass sich die Verbreitung pornographischer Deepfakes zu einem Massenphänomen entwickelt, das sich gegen weiblich gelesene Personen richtet. Es wird gezielt genutzt, um sie öffentlich zu beschämen, zu erniedrigen und mundtot zu machen. So wird entsprechend manipulierte Hardcorepornografie von weiblich gelesenen Personen an ihre Arbeitgeber geschickt, im Kolleg*innenkreis verbreitet oder auf Pornoplattformen zum Download angeboten. Vor allem politisch oder aktivistisch tätige Frauen werden auf diese Weise in Kampagnen und Wahlkämpfen öffentlich unter Druck gesetzt. Drohungen entsprechend manipulierte Videos an

⁷ Mehr Informationen unter: <https://hateaid.org/petition/porno-manipulation/>

Familienangehörige und Kinder zu versenden, sind nicht selten. Die Gefahr, dass die Familie in der Schule oder im Bekanntenkreis mit entsprechenden Bildern konfrontiert wird, ist groß.

Gleichzeitig beobachten wir in diesen Fällen die größten Schutzlücken. In der überwiegenden Zahl der Fälle handelt es sich bei derartigen Vorfällen nämlich in der juristischen Bewertung lediglich um eine Verletzung des Rechts am eigenen Bild gemäß § 33 KunstUrhG. Hierbei handelt es sich nicht nur um ein absolutes Antragsdelikt, sondern auch um ein Privatklagedelikt. Darüber hinaus kommt allenfalls eine Strafbarkeit gemäß § 187 StGB in Betracht, selten auch gemäß § 201a Abs.1, 2 StG, wobei umstritten ist, ob dieser auch die Verbreitung manipulierter Aufnahmen umfasst. Faktisch werden diese Delikte kaum verfolgt und stattdessen auf den Privatklageweg verwiesen. Dies steht außer Verhältnis zu den gravierenden und lebensverändernden Folgen für die Betroffenen.

Um einer massenhaften Einstellung von Ermittlungsverfahren bei Beleidigungsdelikten und der Verletzung des Rechts am eigenen Bild unter Verweis auf den Privatklageweg (§§ 374 ff. StPO) vorzubeugen, empfehlen wir diese Delikte, wenn sie öffentlich oder durch Verbreiten von Schriften (§ 11 Abs. 3 StPO) begangen werden, aus dem Katalog der Privatklagedelikte herauszunehmen. Die Einstellung unter Verweis auf § 374 StPO geschieht oftmals reflexhaft und ist für Anzeigersteller*innen auch bei persönlicher Betroffenheit nicht anfechtbar.

Praktisch bedeutet das, dass Betroffene selbst dann, wenn intime Bilder von ihnen ohne ihre Einwilligung im Internet kursieren oder sie von unter Pseudonym agierenden unbekanntem Täter*innen beleidigt und verleumdet werden, auf den Privatklageweg verwiesen werden. Dieser ist mit hohen Kostenrisiken behaftet und in der Praxis faktisch bedeutungslos. Durch eine solche Praxis wird Betroffenen signalisiert, dass Strafverfolgung in diesen Fällen ihre Privatsache sei. Damit werden die gesamtgesellschaftlichen Folgen von Hasskriminalität im Netz verkannt. Schließlich sind die Ermittlungsbehörden noch immer maßgeblich auf Hinweise aus der Bevölkerung angewiesen, um Hasskriminalität überhaupt zu verfolgen.

3. Gerichte zugänglich machen

Persönlichkeitsrechtsverletzungen können im Zeitalter sozialer Netzwerke jede*n treffen – und dies viel und oft. Während presserechtliche Verfahren mit einer entsprechenden wirtschaftlichen Incentivierung der Parteien seit Jahrzehnten die Gerichte beschäftigen, kommen Persönlichkeitsrechtsverletzungen von Normalbürger*innen, Aktivist*innen, Journalist*innen und anderen in sozialen Netzwerken dort jedoch kaum an. Laut einer europaweiten Umfrage von HateAid

haben lediglich ca. 14 % der Nutzenden einmal darüber nachgedacht, die Gerichte mit digitaler Gewalt zu befassen und lediglich 3 % geben an, es versucht zu haben.⁸

Die Hürden sind vielfältig. Während ein zivilrechtliches Vorgehen gegen Täter*innen allzu häufig daran scheitert, dass diese nicht identifiziert werden können, schrecken Nutzende - obwohl es wie oben beschrieben bereits wirkungsvolle Ansprüche gibt - vor einer Inanspruchnahme der Diensteanbietenden wegen der ungleichen Machtverhältnisse zurück. In beiden Konstellationen gehen die Betroffenen Kostenrisiken von mehreren tausend Euro ein. Hinzu kommen lange Verfahrenslaufzeiten von mehreren Monaten oder Jahren.

Der Koalitionsvertrag hat sich zum Ziel gesetzt: „Kleinforderungen sollen in bürgerfreundlichen digitalen Verfahren einfacher gerichtlich durchgesetzt werden können.“ (S. 84 Zeile 10 des Unterkapitels „Justiz“).

Nach unserem Dafürhalten sollten derartige Verfahren, welche den Zugang zum Recht verbessern sollen, Persönlichkeitsrechtsverletzungen in elektronischen Informations- und Kommunikationsdiensten (Wortlaut: TMG; DSA; Vermittlungsdienste) umfassen.

4. Impressumspflicht, § 5 TMG

Eine weitere Schutzlücke offenbart sich im Bereich der Impressumspflicht. Diese gefährdet vor allem diejenigen, die als Aktivist*innen oder freischaffende Journalist*innen Webseiten und Blogs betreiben und hierfür – mangels Büroräumlichkeiten – ihre Privatanschrift als „ladungsfähige Anschrift“ angeben müssen. Dadurch sind sie gezwungen, sich auf eine Weise im Privatbereich verwundbar zu machen, die unmittelbare Folgen für sie selbst und ihre Familien hat. Denn gerade bei konzertierten und massiven Angriffen von digitaler Gewalt wird durch Täter*innen versucht, private Daten über Betroffene zu erlangen und diese im Internet zu veröffentlichen. Gelingt dies, beobachten wir in der Folge regelmäßig analoge Gewaltübergriffe vor der eigenen Haustür oder dem Arbeitgeber. Die Privatanschrift als „ladungsfähige Anschrift“ angeben zu müssen, stellt daher für viele Menschen eine unnötige Exponierung ihres Privatbereiches und eine unnötige Gefährdung ihrer privaten Sicherheit dar. Hier bedarf es dringend einer Klarstellung, denn sogar die Auslegung des Begriffs „ladungsfähige Anschrift“ ist umstritten. Es ist bisher nicht einmal höchstrichterlich geklärt, ob bspw. die Vertretung durch Rechtsanwält*innen im Impressum zulässig ist. Personen, die die Vorgaben bewusst umgehen wollen, melden ihre Webseite als Briefkastenfirma im Ausland an.

Wir empfehlen daher, Abhilfe für diejenigen zu schaffen, die sich gesetzeskonform verhalten wollen. Es wurden bereits vielfach Vorschläge vorgebracht, die z. B. die

⁸ HateAid-Report „Unsatisfied and helpless – how social media platforms are failing users“
<https://hateaid.org/wp-content/uploads/2022/05/hateaid-eu-report-redress-social-media-platforms.pdf>

Einführung eines behördlich geführten Registers vorsehen. Diese sind diskussionswürdig. Denkbar wäre jedoch auch eine Aufweichung, bzw. Konkretisierung des Begriffs „ladungsfähige Anschrift“, der verdeutlicht, dass es vor allem auf die Erreichbarkeit unter dieser Anschrift ankommt und so Rechtsanwält*innen oder Co-Working-Spaces genutzt werden könnten.

5. Melderegistersperre, § 51 BMG

Die Verbesserung von Auskunftssperren im Melderegister hat ebenfalls Eingang in den Koalitionsvertrag gefunden. Unklar ist, was damit gemeint ist. § 51 BMG wurde zuletzt zu Gunsten der Betroffenen digitaler Gewalt nachgebessert. Weitere Maßnahmen, welche Melderegistersperren für sie niedrighschwelliger machen oder diese beschleunigen, sind selbstverständlich wünschenswert. Zudem ist es erforderlich, dass die Neuregelung des § 51 BMG auch bundesweit einheitlich Anwendung findet.

Dabei müssen vor allem die Voraussetzungen zur Erlangung einer Melderegistersperre immer im Zusammenhang mit denen zur Erlangung einer einfachen Auskunft gemäß § 44 BMG gesehen werden. Angesichts dessen, dass § 51 BMG bereits die Darlegung von Tatsachen erfordert, welche die Annahme einer Gefahr rechtfertigen, sind erstmals und manchmal aus heiterem Himmel Betroffene hier schutzlos gestellt. Nach unserem Dafürhalten sollte daher jede Abfrage im Melderegister, also auch die einfache Abfrage gemäß § 44 BMG, die Glaubhaftmachung von berechtigten Interessen erfordern. Dies würde die Schwelle der Beantragung einer solchen zum Zweck der Einschüchterung erhöhen und wäre zugleich dem Zweck der Vorschrift unschädlich. Diejenigen, die eine solche Abfrage berechtigt durchführen, werden in der Regel ein solches Interesse problemlos darlegen können. An dieser Stelle möchten wir deutlich machen, dass die Veröffentlichung der Privatanschrift im Netz für Betroffene beinahe immer im Wohnungswechsel mündet, da die langfristige analoge Gefahr zu hoch ist. Noch nach Jahren kann es zu analogen Übergriffen kommen, ist die Adresse erst einmal bekannt. Eine zuverlässige Entfernung der Privatadresse in sozialen Netzwerken ist zudem unter den jetzigen Bedingungen nicht möglich.

Dies ist eine gemeinsame Stellungnahme zu den Eckpunkten für ein Gesetz gegen Digitale Gewalt des Bundesministeriums der Justiz vom 25. April 2023 von:

Bundesverband Trans* e.V. (info@bv-trans.de)

Deutscher Juristinnenbund e.V. (djb) (geschaefsstelle@djb.de)

ichbinhier e.V. (info@ichbinhier.online)

HateAid gGmbH (kontakt@hateaid.org)

Lesben- und Schwulenverband (LSVD) e.V. (lsvd@lsvd.de)

Rechtsanwalt Chan-jo Jun (info@kanzlei-jun.de)