Berlin, 26. Mai 2023

STELLUNGNAHME

Deutscher Juristinnenbund e.V.
Vereinigung der Juristinnen,
Volkswirtinnen und Betriebswirtinnen
Geschäftsstelle / Office:
Kronenstraße 73 ● D-10117 Berlin
Telefon: +49 30 4432700
geschaeftsstelle@djb.de ● https://www.djb.de

zu den Eckpunkten des Bundesministeriums der Justiz zum Gesetz gegen digitale Gewalt. *Drei kleine Schritte in die richtige Richtung – mehr aber auch nicht*

I. Vorbemerkung

Der Deutsche Juristinnenbund e.V. (djb) begrüßt ausdrücklich die Neuerungen, die die Bundesregierung im Eckpunktepapier für ein Gesetz gegen digitale Gewalt jetzt bereits vorsieht:

- Die **Ausweitung des bereits existierenden Auskunftsanspruchs** bei anonym getätigten Rechtsverletzungen im Internet,
- die **Neueinführung richterlich angeordneter Accountsperren** in Fällen wiederholter Rechtsverletzungen und
- die Beibehaltung und Ausweitung der Zuständigkeit des „**inländischen Zustellungsbevollmächtigten“**, zu dessen Benennung alle, auch im Ausland ansässige Betreiber*innen von sozialen Netzwerken, verpflichtet werden sollen.

Genauso ausdrücklich weist der djb aber darauf hin, dass diese drei Einzelmaßnahmen weit hinter dem zurückbleiben, was im Kampf gegen digitale Gewalt erforderlich, von der Bundesregierung im Koalitionsvertrag angekündigt und von dieser zu erwarten gewesen wäre. Seit Jahren betonen zahlreiche (Betroffenen-)Organisationen und Verbände, Gruppen aus der Zivilgesellschaft und nicht zuletzt der djb[1] regelmäßig, dass und welche Maßnahmen getroffen werden müssen, um von digitaler Gewalt Betroffene endlich effektiv bei der Rechtsverfolgung und -durchsetzung zu unterstützen, vor weiteren Rechtsverletzungen zu schützen und die Täter*innen sowie Plattformbetreiber (zivil- und strafrechtlich) haftbar zu machen.

Bei der Bekämpfung digitaler Gewalt geht es nicht nur um den Schutz Einzelner, sondern vor allem um den Erhalt einer wehrhaften Demokratie und die Sicherung der Teilhabe am öffentlichen Diskurs – gerade von Frauen und Mitgliedern der LGBTQ* Community. Digitale Gewalt hat eine Geschlechterdimension. Antifeminismus, Hass gegen Frauen und Menschen der LGBTQ* Community finden im Netz Bedingungen, die sich verstärkend auswirken und das Entstehen extremistischer Strömungen begünstigen. Das Netz ist kein neutraler Raum. Für viele Menschen erweist sich das Netz vielmehr als ein Ort der Ausgrenzung, in dem sie beschämt und bedroht werden. Wenn Frauen sich im Netz öffentlich oder gar politisch

[1] https://www.djb.de/fileadmin/user_upload/st21-18_Antifeminismus_im_Netz.pdf; https://www.djb.de/wahlforderungen

äußern, sind sie besonders von Hatespeech, Beleidigungen, aber auch Verletzungen des Rechts am eigenen Bild und/oder der sexuellen Selbstbestimmung betroffen – also von digitaler Gewalt.

Der Kampf gegen digitale Gewalt ist eine zentrale Aufgabe für unsere Gesellschaft. Dieser werden die Eckpunkte zum Gesetz gegen digitale Gewalt (noch) nicht gerecht, die sich mit der Geschlechterdimension gar nicht beschäftigen. Sie bleiben auch dann unzureichend, wenn man die Regelungen des Digital Services Act (DSA) bzw. des geplanten Digitale Dienste Gesetzes (DDG) mitberücksichtigt. Denn digitale Gewalt wirkt in verschiedenste Bereiche des Lebens und des Rechts hinein und muss entsprechend umfassend betrachtet und bekämpft werden. Dazu gehören Neuerungen und Nachschärfungen im Zivil- und Strafrecht und dem jeweiligen Prozessrecht, der Ausbau von Opferschutz und -beratung, Bildung (insb. Medienkompetenz) junger Menschen und Fortbildungen für Justiz, Staatsanwaltschaft und Polizei – um nur einige Maßnahmen zu nennen. Dem wird das Eckpunktepapier nicht gerecht, es ist lediglich als erster (zögerlicher) Schritt zu einem „echten Gewaltschutzgesetz“ zu werten. Weil der Kampf gegen digitale Gewalt besonders dringlich ist, brauchen wir weit mehr als die im Eckpunktepapier genannten Maßnahmen: Ein Gewaltschutzgesetz, das all die genannten Bereiche vernetzt, die verschiedenen Ebenen der Digitalisierung und mit ihr einhergehende Gefahren berücksichtigt und digitaler Gewalt schlagkräftig entgegentritt.

II. Was in den Eckpunkten fehlt – aber im Gesetz enthalten sein sollte

Die Eckpunkte bleiben weit hinter dem zurück, was zum Kampf gegen digitale Gewalt erforderlich ist. Bevor zu den drei geplanten Regelungen unter III. im Einzelnen Stellung genommen wird, ist es deshalb erforderlich, den Fokus darauf zu richten, welche wichtigen Maßnahmen die Bundesregierung in das geplante digitale Gewaltschutzgesetz noch aufnehmen bzw. welche Bereiche sie berücksichtigen sollte. Die folgende Auflistung widmet sich den wesentlichen Lücken im derzeit geplanten digitalen Gewaltschutzgesetz. Ergänzend verweisen wir auf unsere zu der Problematik der digitalen Gewalt bereits veröffentlichten Papiere und Stellungnahmen.

- Wir benötigen **flächendeckende Schwerpunktstaatsanwaltschaften** für Straftaten im Zusammenhang mit digitaler Gewalt. Dies würde die in den Eckpunkten bereits angelegte Bündelung der gerichtlichen Zuständigkeit spiegeln und ergänzen. Dabei ist sicherzustellen, dass sich die Ermittlungen der vorhandenen Schwerpunktstaatsanwaltschaften zu Cybercrime und Computerkriminalität nicht auf wirtschaftsstrafrechtliche Fragestellungen beschränken.
- Es bedarf eines elektronischen Verfahrens zum Stellen von Strafanträgen wegen Straftaten im Zusammenhang mit digitaler Gewalt. Dabei sollten auch Beweismittel wie Screenshots rechtssicher hochgeladen werden können. Darüber hinaus bedarf es für Opfer digitaler Gewalt **umfassender (Online-)Beratungsangebote**, deren „Aufsetzen“ sogar im Koalitionsvertrag ausdrücklich festgeschrieben ist. Es ist zu hoffen, dass diese lediglich deshalb nicht Teil des Eckpunktepapiers sind, weil derartige Beratungsangebote in die Zuständigkeit anderer Ministerien fallen könnten. Und mehr noch: Die bestehenden **Entschädigungsregelungen** müssen auf Opfer psychischer, auch digitaler Gewalt mit schweren Folgen ausgeweitet werden.
- Auch die zivilrechtliche Verfolgung von digitaler Gewalt sollte digital möglich sein. Zumindest den geplanten erweiterten Auskunftsanspruch sollten Betroffene

elektronisch geltend machen können. So würde einerseits ein niedrigschwelliger Zugang zu den Gerichten gewährleistet und andererseits sichergestellt, dass die Rechtsverletzung auch technisch optimal „gesichert“ und belegt werden kann. Hierzu gehört die (etwa im Rahmen der Eingabemaske eines solchen Antrags bei Gericht bereitgestellte) Möglichkeit, rechtssichere Screenshots oder andere Belege zu erstellen und direkt bei Gericht (ohne Medienbruch) hochzuladen und zu sichern. Das entspricht auch einem weiteren Ziel der Bundesregierung: der **Digitalisierung der Justiz**.

- Längst überfällig ist die Möglichkeit für zivilgesellschaftliche (ggf. staatlich anerkannte) Organisationen, Betroffene bei der Rechtsdurchsetzung zu unterstützen und/oder Verfahren eigeninitiativ zu führen (**Prozessstandschaft/Verbandsantragsrecht**). Das Eckpunktepapier verkennt das Gefahrenpotential digitaler Gewalt für den demokratischen Diskurs, wenn es den Fokus nur bzw. jedenfalls zu stark auf die Eigenverantwortung der Betroffenen legt, die „*es selbst in der Hand haben [müssen], effektiv gegen Rechtsverletzungen vorzugehen*“. Die erleichterte Individualrechtsverteidigung genügt jedoch bei weitem nicht, um digitale Gewalt effektiv zu bekämpfen. Der starke Fokus auf Individualrechtschutz wird zudem der Lage der Betroffenen und den Folgen für unsere demokratische Gesellschaft nicht gerecht. Damit Betroffene ihre Rechte gegen digitale Gewalt durchsetzen und verteidigen können, müssen sie in unserem heutigen System über erhebliche emotionale und finanzielle Ressourcen verfügen und diese einsetzen. Nicht nur müssen sie es aushalten, sich immer wieder der Rechtsverletzung und den Täter*innen zu stellen. Auch finanziell müssen die Betroffenen erheblich in Vorleistung gehen und erhalten ihre Rechtsverfolgungskosten regelmäßig nicht erstattet, weil die Täter*innen nicht identifiziert werden können oder mittellos sind. Das ist nicht hinnehmbar, verteidigen die Betroffenen mit der Geltendmachung ihrer Rechte doch zugleich auch den demokratischen Diskurs. Es muss möglich sein, dass sie dabei von Verbänden und Organisationen unterstützt werden, und zwar bis hin zu einer (einvernehmlichen) Übernahme der Rechtsdurchsetzung durch diese. Letztere ist dann sogar entscheidend, wenn es keine in ihren Individualrechten verletzten Personen gibt (etwa bei volksverhetzenden Inhalten). Durch Art. 86 DSA wird eine Verbandsklagemöglichkeit in Bezug auf in sozialen Netzwerken verbreitete rechtswidrige Inhalte erstmals eingeführt. Danach haben „Nutzer von Vermittlungsdiensten das Recht, eine Einrichtung, Organisation oder Vereinigung mit der Wahrnehmung der mit dem DSA übertragenen Rechte in ihrem Namen zu beauftragen“. Dem sollten national weitere Instrumente an die Seite gestellt werden. Da diese Forderung schon so lange und von so vielen Seiten erhoben wird, müssen wir jedoch davon ausgehen, dass die Einführung entsprechender Instrumente ganz bewusst nicht erfolgt.
- Problematisch ist auch, dass es Betroffenen bis heute nicht oder kaum möglich ist, **anonym** oder jedenfalls ohne Angabe weiterer Daten, wie etwa ihrer Anschrift, gegen Rechtsverletzungen vorzugehen. Zivilgerichte verlangen selbst bei anwaltlich vertretenen Betroffenen stets die Angabe ihres Wohnsitzes. Dass Betroffene dies allzu oft von einer Rechtsdurchsetzung abschreckt, ist nur zu verständlich: **Digitale Gewalt kann sich offline fortsetzen**. Übergriffe werden dann nicht nur verbal digital angedroht, etwa unter Offenlegung der privaten Wohnanschrift und der Arbeits- und

Familienverhältnisse der Betroffenen, sondern es kommt tatsächlich zu solchen Taten. Das kann durch die Kombination von Prozessstandschaft, eines Verbandsantragsrechts und der Möglichkeit, anonym, jedenfalls ohne Angabe der Wohnanschrift (etwa mit c/o Adresse), gerichtlich tätig zu werden, wirksam verhindert werden.

- Die Praxis zeigt überdies: Ohne **verpflichtende Fortbildungen für Justiz, Staatsanwaltschaft und Polizei**, im Rahmen derer diese Personen auch für die geschlechtsspezifische Dimension digitaler Gewalt sensibilisiert werden, werden wir der Bedeutung der effektiven Verfolgung digitaler Gewalt und dem Schutz der Betroffenen auch in Zukunft nicht gerecht.
- Bestehende **Strafbarkeitslücken im Bereich digitale Gewalt sind zu schließen**. Welche Lücken im Kampf gegen bildbasierte digitale Gewalt bestehen, wird der djb in einem gesonderten Policy Paper ausführen. Hier sollte ein einheitlicher Komplex von Straftatbeständen innerhalb des Sexualstrafrechts geschaffen werden, der das Herstellen, Gebrauchen und Verbreiten von Bildaufnahmen unter Strafe stellt, die eine andere erwachsene Person sexualbezogen wiedergeben, ohne dass diese wirksam eingewilligt hat. Das Adhäsionsverfahren, mit dem zivilrechtliche Ansprüche unmittelbar im Strafprozess mit geltend gemacht werden, könnte ausgeweitet werden. Und auch Maßnahmen, direkt gerichtet gegen von solchem Bildmaterial profitierende (Porno-)Plattformen, sind wünschenswert.
- Die bestehenden (wenigen) Bildungskampagnen (z.B. an Schulen, im TV und in Sozialen Medien), mithilfe derer Nutzer*innen von Sozialen Netzwerken über deren Gefahren aufgeklärt werden, sind dringend auszuweiten. Es gehört zu den Kernaufgaben einer demokratischen Gesellschaft, jungen Menschen schon in frühen Jahren die heute erforderliche **Medienkompetenz** zu vermitteln.

Erst die Kombination dieser genannten Maßnahmen mit denjenigen, die das Eckpunktepapier vorsieht, bilden aus Sicht des djb ein überzeugendes Konzept gegen digitale Gewalt. Deshalb kann der djb die aktuell veröffentlichten Eckpunkte für ein digitales Gewaltschutzgesetz als nicht mehr als einen ersten – zwar völlig unzureichenden – aber gleichwohl dringlichen Aufschlag werten.

Daher begrüßt der djb die drei geplanten Maßnahmen (Ausweitung des bereits existierenden Auskunftsanspruchs, Neueinführung richterlich angeordneter Accountsperren und Beibehaltung und Ausweitung der Zuständigkeit des „inländischen Zustellungsbevollmächtigten“) und nimmt zu diesen im Einzelnen wie folgt Stellung:

III. Zu den geplanten Maßnahmen im Einzelnen

1. Die Erweiterung des Auskunftsanspruchs (§ 21 Abs. 2 TTDSG)

a) Bisheriger Auskunftsanspruch ungenügend

Der in § 21 Abs. 2 TTDSG bisher geregelte Auskunftsanspruch zur Durchsetzung zivilrechtlicher Ansprüche führt ein Schattendasein. In der anwaltlichen Praxis kommt er aus mehreren Gründen kaum vor. Der Anspruch ist bis dato begrenzt auf die Auskunft über bei dem Anbieter von Telemedien vorhandenen sog. Bestandsdaten, also personenbezogenen Daten, deren Verarbeitung zum Zweck der Begründung, inhaltlichen Ausgestaltung oder Änderung eines

Vertragsverhältnisses zwischen dem Anbieter von Telemedien und dem Nutzer erforderlich ist (§ 2 Abs. 2 Nr. 2 TTDSG). Das sind regelmäßig nur der (meist falsch angegebene) Name oder eine E-Mail-Adresse. Die IP-Adresse hingegen gehört nicht zu den Bestands- sondern zu den sog. Nutzungsdaten. Der Auskunftsanspruch umfasst zwar schon jetzt die Verletzung absoluter Rechte, nach § 21 Abs. 2 TTDSG aber nur, wenn gleichzeitig einer oder mehrere der in § 1 Abs. 3 des Netzwerkdurchsetzungsgesetzes (NetzDG) aufgeführten Straftatbestände erfüllt ist bzw. sind. Zuständig ist gemäß § 21 Abs. 3 TTDSG das Landgericht ohne Rücksicht auf den Streitwert. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend, also insb. der Amtsermittlungsgrundsatz. Die Kosten der richterlichen Anordnung trägt nach dem Wortlaut des § 21 Abs. 3 Satz 7 TTDSG (stets) die verletzte Person (auch wenn § 81 FamFG andere Kostenentscheidungen in das Ermessen des Gerichts legt). Bleibt es bei der Kostentragung der antragstellenden Person, so kann diese erst im Rahmen der Durchsetzung zivilrechtlicher Ansprüche ihre Kosten gegenüber dem oder der Verletzer*in geltend machen (trägt aber stets das Risiko, dass diese Person die Kosten am Ende nicht begleichen kann). Der*die Anbieter*in des Telemediums ist lediglich als sog. Beteiligter hinzuzuziehen.

Hauptgrund dieses Schattendaseins (das nur von wenigen prominenten Entscheidungen, wie etwa der zu *Renate Künast*[2] durchbrochen wird) ist der hohe Aufwand, den Betroffene betreiben müssen, um ihren Auskunftsanspruch durchzusetzen. Dieser hohe Aufwand steht in keinem Verhältnis zu den regelmäßig dürftigen Erkenntnissen, die das Auskunftsverfahren in seiner bisherigen Ausgestaltung hervorbringt. Eine herausgegebene E-Mail-Adresse bringt die Betroffenen nicht zu dem*r Verletzer*in, der*die den Account führt. Denn üblicherweise müssen Nutzer*innen gegenüber den Anbietern Sozialen Medien nicht ihre Wohnanschrift angeben, um einen Account zu eröffnen. Schon gar nicht werden solche Angaben verifiziert. Häufig hinterlegen Nutzer*innen falsche Namen oder Pseudonyme. Selbst wenn es einmal der „echte“ Name ist, führt dieser ohne weitere Angaben etwa zum Wohnort, dem Geburtstag, -ort und/oder Familienstand regelmäßig nicht zu Erkenntnissen, die die Betroffenen in die Lage versetzen, zivilrechtliche Ansprüche gegen den*die Verletzer*in durchzusetzen. Die wenigen durch die Auskunft erlangten Angaben genügen meist nicht einmal für eine erfolgreiche Einwohnermeldeamtsanfrage. Hinzu kommt, dass diesen dürftigen Erkenntnismöglichkeiten erhebliche Kosten entgegenstehen, die die Betroffenen treffen: Denn ausweislich des Wortlauts trägt die Kosten der richterlichen Anordnung die verletzte Person – selbst im Fall des Obsiegens. Über die Erhebung von Gerichtsgebühren kann zwar das Gericht entscheiden, aber auch wenn angesichts der Geltung des FamFG auch vor dem Landgericht kein

[2] LG Berlin, Beschluss vom 9.9.2019 – 27 AR 17/19, KG Beschluss vom 31.10.2022 – 10 W 13/20, BVerfG, Beschluss vom 19.12.2021 – 1 BvR 1073/20

Anwaltszwang besteht: Wenn sich Parteien anwaltlich vertreten lassen, müssen die Betroffenen diese Kosten zunächst selbst tragen. Da zudem der*die jeweilige Anbieter*in von Telemedien gem. § 21 Abs. 4 TTDSG als Beteiligter zu dem Verfahren hinzugezogen werden soll, entstehen den verletzten Personen im Fall deren anwaltlicher Vertretung weitere Kosten. Die Feststellung in den Eckpunkten des Bundesministeriums der Justiz zum Gesetz gegen digitale Gewalt, wonach das *„Verfahren (…) bislang jedoch nicht den Ansprüchen an eine effektive Möglichkeit zur privaten Rechtsdurchsetzung*“ genügt (dort unter II. 1.), ist mithin korrekt.

Der djb unterstützt deshalb ausdrücklich die Stärkung des privaten Auskunftsverfahrens. Je niedrigschwelliger Personen, deren Rechte nachweislich verletzt wurden, auf richterliche Anordnung hin Kenntnis von der Identität der Verletzer*innen erlangen können, desto erfolgsversprechender ist die sich anschließende, insb. zivilrechtliche Rechtsdurchsetzung.

b) Eckpunktepapier irreführend: Auskunftsanspruch erfasst bereits jetzt „absolute Rechte“

Anders als in den Eckpunkten des Bundesministeriums der Justiz zum Gesetz gegen digitale Gewalt angedeutet und von den Medien kolportiert, erstreckt sich der Anwendungsbereich des Auskunftsverfahrens gemäß § 21 Abs. 2 Satz 1 TTDSG schon jetzt auf die Verletzung absolut geschützter Rechte. Dies schließt auch das Recht am eingerichteten und ausgeübten Gewerbebetrieb ein. So gibt es schon jetzt (vereinzelt) Entscheidungen, die neben einer Verletzung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb als absolutes Recht auch eine (in § 1 Abs. 3 NetzDG enthaltene) Kreditgefährdung i.S.d. § 187 Alt. 3 StGB und damit den Auskunftsanspruch bejahten.[3] Der nun in den Eckpunkten enthaltene Hinweis darauf, dass Auskunftsansprüche etwa auch in Fällen einer *„Restaurantkritik: Schädigung durch wahrheitswidrige Nutzerkommentare*“ eröffnet sein können, wirft daher – ohne Not – die Frage auf, ob solche Rechtsverletzungen mit Fällen digitaler Gewalt gegen natürliche Personen vergleichbar sind. Dies hat in den Medien zu viel Kritik geführt. Es bleibt zu hoffen, dass dies das BMJ an der Umsetzung der geplanten Regelungen nicht hindert.

Denn auch im Fall der Verletzung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb besteht der Auskunftsanspruch nur dann, wenn eine rechtswidrige Verletzung dessen durch ein Gericht festgestellt wird. Dafür ist auch im Fall der Verletzung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb stets eine Abwägung der widerstreitenden Interessen erforderlich. Die Meinungsfreiheit wird dadurch nicht verkürzt, sondern ausreichend gewichtet. Zudem trifft gegen juristische Personen gerichtete digitale Gewalt nicht nur die Unternehmen und Vereine selbst, sondern es werden

[3] OLG Celle, Beschluss vom 23.09.2021 – 5 W 39/21

regelmäßig auch einzelne, teils namentlich benannte Mitarbeitende angegriffen, die ebenfalls schutzbedürftig sind.

c) Auskunftsanspruch auch unterhalb der Strafbarkeitsschwelle

Der djb begrüßt nachdrücklich, dass der Auskunftsanspruch künftig neben einer Verletzung absoluter Rechte (einschließlich des Rechts am eingerichteten und ausgeübten Gewerbebetrieb) keine weiteren Anforderungen an die begangene Rechtsverletzung vorsieht.

Die bisher in § 21 Abs. 2 TTDSG enthaltene Einschränkung, wonach der Auskunftsanspruch nur dann bestehen kann, wenn die Verletzung absolut geschützter Rechte durch rechtswidrige Inhalte erfolgt, die (abschließend) in § 1 Abs. 3 NetzDG genannt sind, soll ersatzlos gestrichen werden. Das ist richtig. Bisher war es erforderlich, dass die rechtswidrigen Inhalte die Strafbarkeitsschwelle überschritten, insb. den Tatbestand jedenfalls eines der dort genannten Straftatbestände (§§ 86, 86a, 89a, 91, 100a, 111, 126, 129 – 129b, 130, 131, 140, 166, 184e, 185 – 187, 189, 201a, 241 oder 269 StGB) erfüllen und nicht gerechtfertigt sind. In der Praxis beschränkte sich die Anwendbarkeit des § 21 Abs. 2 TTDSG auf strafbare Inhalte in Form der Beleidung (§ 185 StGB), Verleumdung (§ 187 StGB) oder Bedrohung (§ 241 StGB). Dafür, dass nur im Fall strafbarer Inhalte, und nicht im Fall „bloßer“ Persönlichkeitsrechtsverletzungen (einschließlich der Verletzung des Rechts am eigenen Bild) oder auch Verletzungen des Rechts am eingerichteten und ausgeübten Gewerbebetrieb Auskunftsansprüche bestehen sollen, gibt es keinen sachlichen Grund. Insbesondere nicht, weil der Auskunftsanspruch der Vorbereitung und Durchsetzung zivilrechtlicher Ansprüche dient und die – wie das Beispiel *Renate Künast* zeigt – zuständigen Landgerichte der Zivilgerichtsbarkeit sich mit der Anwendung und Auslegung strafrechtlicher Normen häufig schwertun.

Wenn der Auskunftsanspruch künftig auch unterhalb der Strafbarkeitsschwelle greift, wird die bestehende Schutzlücke bei Rechtsverletzungen unterhalb der Strafbarkeitsschwelle (§ 1 Abs. 3 NetzDG) endlich geschlossen.

Wichtig erscheint dem djb hier eine deutliche Klarstellung: Die Verletzung des allgemeinen Persönlichkeitsrechts als absolutes Recht schließt die Verletzung des Rechts am eigenen Bild und generell Persönlichkeitsverletzungen durch bildbasierte digitale Gewalt ein. Dieser Bereich ist für die Betroffenen von digitaler Gewalt bisher nur sehr unzureichend geregelt. Zwar bezieht § 21 Abs. 2 TTDSG das Recht am eigenen Bild als spezielle Ausprägung des allgemeinen Persönlichkeitsrechts[4] (also eines absoluten Rechts) ein; durch die Bezugnahme auf § 1 Abs. 3 NetzDG besteht der Auskunftsanspruch derzeit aber nur, wenn die Strafbarkeitsschwelle auch in diesem Bereich des Bildnisrechts überschritten ist. Dies ist nur im Rahmen von Aufnahmen, die den höchstpersönlichen Lebensbereich verletzen (§§ 1 Abs. 3 NetzDG i.V.m. 201a StGB) oder dann der Fall, wenn ein Bildnis (isoliert oder im konkreten Kontext) eine Beleidigung darstellt. Mit dem Verzicht auf diese Bezugnahme und das damit verbundene Erfordernis der

[4] Vgl. nur BeckOK BGB/Förster BGB § 12 Rn. 130

Strafbarkeit, können Betroffene künftig auch dann einen Auskunftsanspruch geltend machen, wenn „nur“ ihr Recht am eigenen Bild gem. §§ 22, 23 KUG (wegen der Verbreitung oder öffentlichen Zurschaustellung von Bildnissen) oder ihr allgemeines Persönlichkeitsrecht durch die Erstellung oder Manipulation von Bildnissen (etwa wenn es um die heimliche Erstellung von Bildnissen oder Deepfakes geht) verletzt wurde. Das Recht am eigenen Bild als besondere Ausprägung des allgemeinen Persönlichkeitsrechts und der Bildnisschutz, soweit er direkt dem allgemeinen Persönlichkeitsrecht entspringt, erfahren mit der geplanten Regelung zum Auskunftsanspruch also eine sehr begrüßenswerte, längst überfällige Aufwertung im Rahmen der Vorbereitung und Verfolgung zivilrechtlicher Ansprüche. Allerdings: an den in Bezug auf bildbasierte digitale Gewalt aktuell bestehenden Strafbarkeitslücken würden die angedachten Änderungen gleichwohl nichts ändern. Welche Lücken hier bestehen und wie diese geschlossen werden können, wird der djb in einem gesonderten Policy Paper zum Thema bildbasierte digitale Gewalt ausführen.

Die Aufgabe der Beschränkung auf die in § 1 Abs. 3 NetzDG genannten Straftatbestände ist nicht nur sinnvoll, sondern dringend angezeigt. Die Regelungen des DSA werden das NetzDG bald ersetzen, sodass auch insofern eine Lücke zu schließen sein wird. Aber auch aus Rechtsschutzgesichtspunkten bedarf es neben der Beschränkung auf absolute Rechte keiner weiteren Einschränkung als Voraussetzung für einen Auskunftsanspruch. Die Person, die die – gerichtlich festgestellte – Rechtsverletzung begangen hat, erscheint nicht schutzwürdig, zumal sie sich durch die Angabe eines Pseudonyms dem unmittelbaren Zugriff und der Haftung entzieht oder jedenfalls entziehen will.

d) Erweiterung des Inhalts des Auskunftsanspruchs auch auf Nutzungsdaten

Der djb unterstützt die Ausweitung des Auskunftsverfahrens auf die Herausgabe von Nutzungsdaten. Nutzungsdaten sind personenbezogenen Daten, deren Verarbeitung erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Dazu gehören insbesondere Merkmale zur Identifikation von Nutzer*innen, Angaben über Beginn und Ende sowie Umfang der jeweiligen Nutzung und Angaben über die von den Nutzer*innen in Anspruch genommenen Telemedien (§ 2 Abs. 2 Nr. 3 TTDSG). Diese Angaben sind entscheidend für die Identifikation von Verletzer*innen: In aller Regel ermöglichen es allein die Nutzungsdaten, die Identität des oder der Verantwortlichen zu bestimmen und so die Täter*innen in Haftung – auch zivilrechtlicher Natur – zu nehmen.

Gleichzeitig korrespondiert der erweiterte Auskunftsanspruch mit dem weiter aufrechterhaltenen Grundsatz, dass es keine Pflicht zur Nutzung digitaler Dienste nur mit Klarnamen gibt. Diese Möglichkeit der anonymen oder pseudonymen Nutzung digitaler Dienste bleibt erhalten, was gerade mit Blick auf Personen, die sonst ihre Meinung nicht offen sagen können oder wollen, richtig ist. Dann muss aber gleichzeitig ein effektiv ausgestalteter Auskunftsanspruch den von digitaler Gewalt Betroffenen endlich die damit einhergehenden Schwierigkeiten bei der effektiven Rechtsdurchsetzung nehmen.

e) Erstreckung auf Anbieter*innen von Messenger- und Internetzugangsdiensten

Die angedachte Klarstellung, dass auch Anbieter*innen von Messenger- und Internetzugangsdiensten (Telekommunikationsunternehmen) zur Herausgabe von Daten durch ein Gericht verpflichtet werden können, ist sinnvoll. Denn die Herausgabe etwa der IP-Adresse ist nur der erste Schritt der Täter*innenidentifizierung: nur Internetzugangsanbieter*innen können Auskunft geben, welcher Person eine bestimmte IP-Adresse bei der Rechtsverletzung zugeordnet war. Unter den Kreis der zur Auskunft Verpflichteten würden durch die Ausweitung auch Messenger-Anbieter wie WhatsApp, Signal und Telegram fallen. Dies hat zu Unrecht viel Kritik ausgelöst, gar von der Einführung einer „Vorratsdatenspeicherung durch die Hintertür" ist zu lesen[5].

Denn die Geltendmachung und Durchsetzung der Auskunft erfolgt in einem rechtsstaatlichen Verfahren, das die Rechte aller Beteiligten berücksichtigt und sichert: Zwingende Voraussetzung des Auskunftsanspruchs ist eine Verletzung absoluter Rechte. Erst und allein diese veranlasst die Verpflichtung zur Herausgabe und begründet die Pflicht zur Speicherung bereits erhobener verletzungsbezogener Daten. Was nicht gespeichert ist, muss nicht herausgegeben werden. Private Kommunikation bleibt weiter geschützt. Aber im Fall von gerichtlich festgestellten Rechtsverletzungen darf es keinen Unterschied machen, ob diese in Sozialen Medien oder etwa großen Gruppen in Messengerdiensten geäußert werden. Darüber hinaus bleibt es beim Richtervorbehalt, es ist stets der Grundsatz der Verhältnismäßigkeit zu wahren und die Übermittlung der Information erfolgt zunächst nur an das Gericht (siehe unten). Die an der Ausweitung des Anspruchs geäußerte Kritik ist deshalb aus Sicht des djb nicht begründet. Wenig wahrscheinlich erscheint zudem die teilweise geäußerte Befürchtung, dass gespeicherte Daten auch zu nicht vorgesehenen Zwecken verwendet würden (etwa der Erleichterung möglicher Profilbildung). Auskunftsverfahren werden auch weiterhin nur im Einzelfall stattfinden, sodass diese Gefahr wenig realitätsnah erscheint.

Der djb gibt an dieser Stelle zu bedenken, dass sich der Auskunftsanspruch zur Schließung von Schutzlücken auch gegen die Anbieter*innen sog. virtueller privater Netzwerke (VPN) richten muss. Solche VPN-Anbieter*innen verhindern die direkte Verbindung zum Server einer Webseite, sodass an Dritte ausschließlich die IP-Adresse des VPN-Servers übertragen wird. Die Identität von VPN-Nutzer*innen bleibt daher verborgen. Wenn Betroffene den Anspruch nicht auch gegen VPN-Anbieter*innen richten können, bliebe eine erhebliche Schutzlücke, wenn Verfasser*innen rechtswidriger Inhalte einen VPN nutzen. Eine weitere Herausforderung im Kampf gegen digitale Gewalt ist der Umgang mit VPN-Anbieter*innen, die keine Logs speichern und deshalb auch bei erweiterter Auskunftspflicht keine Nutzungsdaten herausgeben können, wie zum Beispiel die beliebte Anbieterin Proton.

Offen ist noch die Frage, welche Folgen es hat, dass die Diensteanbieter*innen im Wege des Auskunftsverfahrens Kenntnis von rechtsverletzenden Inhalten

[5] https://www.ccc.de/de/updates/2023/digitale-gewalt-vorratsdaten

erlangen. Diese positive Kenntnis begründet die Störerhaftung und löst (zumutbare) Prüf- und ggf. Löschpflichten aus.

f) Prozessuale Änderungen

Die geplante Beweissicherungsanordnung, durch die Diensteanbieter*innen bereits in einem frühen Verfahrensstadium verpflichtet werden können, die Bestands- und Nutzungsdaten von Verletzer*innen offenzulegen, ist sinnvoll und dient der Effektivität der Rechtsdurchsetzung, der Rechtssicherheit und -klarheit. Missbrauch oder erhebliche Gefahren für die Verfasser*innen der potentiell rechtsverletzenden Inhalte bestehen nicht, da die gezielte Sicherung und Offenlegung der Bestands- und Nutzungsdaten bis zur Feststellung der Rechtswidrigkeit nur gegenüber dem Gericht erfolgt.

Die gleichzeitig angedachte Anordnung zur Sicherung des zu überprüfenden Inhalts selbst (also unabhängig von den Bestands- und Nutzungsdaten) nimmt Betroffenen das Risiko, etwa durch einen unzureichend erstellten Screenshot und/oder die Behauptung der Verfasser*innen, der erstellte, dann ausgedruckte Screenshot sei womöglich nachträglich gefälscht bzw. manipuliert worden, den Beweis der Rechtsverletzung am Ende nicht zur vollen Überzeugung des Gerichts führen zu können. Denn die Rechtsprechung sieht in dem Ausdruck eines Screenshots auf Papier nicht mehr als ein Augenscheinsobjekt, dessen Beweiskraft sich daher allein nach § 286 ZPO beurteilt[6].

Derartige Beweisanordnungen sind auch deshalb sinnvoll, weil einige Gerichte in der Vergangenheit den Auskunftsanspruch nach Löschung des rechtsverletzenden Inhalts durch den*die Diensteanbieter*in zu Unrecht verneinten. Zur Begründung erklärten sie, aufgrund der Löschung bestehe kein Rechtsverhältnis zwischen verletzter Person und Diensteanbieter*inmehr [7]. Diese zu kritisierende Rechtsauffassung hat dazu geführt, dass Betroffene die ihnen gegen die Verletzer*innen zustehenden Ansprüche wie Unterlassung, Geldentschädigung oder Ersatz von Rechtsanwaltskosten nicht durchsetzen konnten. Sie wäre im Fall der Umsetzung der geplanten Eckpunkte nicht aufrechtzuerhalten.

In der Praxis kaum sinnvoll durchführ- und erst recht nicht überprüfbar scheint dem djb die angedachte Unterscheidung zwischen „normaler“ Beweissicherungsanordnung und einstweiliger Beweissicherungsanordnung. Mit der „normalen“ Beweissicherungsanordnung verpflichtet das Gericht Dienste- bzw. Internetzugangsanbieter*innen zur gezielten Sicherung und Offenlegung von Bestands- und Nutzungsdaten von Inhalteverfasser*innen. Durch eine einstweilige Beweissicherungsanordnung soll das Gericht dieselbe Entscheidung ausnahmsweise bereits innerhalb „weniger Tage“ treffen. Schon begrifflich ist die Unterscheidung zwischen Beweissicherungsanordnung und einstweiliger Beweissicherungsanordnung schwer nachzuvollziehen, entscheidend aber ist: die zentrale Voraussetzung, unter der eine einstweilige Beweisanordnung möglich und angezeigt sein soll, ist – das lehrt die Erfahrung mit dem NetzDG – weitestgehend willkürlich, jedenfalls in keiner Weise präzise oder überprüfbar. Einstweilige

[6] OLG Jena, Urt. v. 28.11.2018 – 2 U 524/17

[7] OLG Frankfurt am Main, Beschluss vom 6.9.2018 – 16 W 27/18, nachfolgend (nicht jedoch zu diesem Aspekt): BGH, Beschl. v. 24.9.2019 – VI ZB 39/18; OLG Köln, Beschluss vom 11.03.2021 – 15 W 10/21, Rz. 50

Anordnungen sollen bei „*offensichtlich rechtswidrigen Inhalten*“ möglich sein. Das erinnert an § 3 Abs. 2 Nr. 2 bzw. 3 NetzDG, der (noch) vorsieht, „*offensichtlich rechtswidrige Inhalte*“ innerhalb von 24 Stunden, und im Vergleich dazu „*jeden anderen rechtswidrigen Inhalt*“ unverzüglich, in der Regel innerhalb von 7 Tagen zu löschen bzw. den Zugang zu sperren. Eine klare Abgrenzung, wann ein Inhalt „*offensichtlich rechtswidrig*“ ist und wann nicht, ist seit Einführung des NetzDG nicht gelungen. Dies mag bei der geplanten Regelung anders, weniger willkürlich sein, weil im Rahmen des Auskunftsanspruchs stets Richter*innen (und nicht wie im Rahmen von § 3 Abs. 2 Nr. 2 bzw. 3 NetzDG ein/e Anbieter*in eines Sozialen Netzwerks) diese Unterscheidung zwischen rechtswidrigen und offensichtlich rechtswidrigen Inhalten treffen würden. Eine klare Unterscheidung dürfte aber auch hier schwierig werden. Ggf. wäre es deshalb sinnvoller, die Unterscheidung nicht an der „Offensichtlichkeit“ der Rechtsverletzung, sondern an der Frage der Dringlichkeit festzumachen, angelehnt an das Verfahren auf Erlass einer einstweiligen Verfügung. Die Möglichkeit einer einstweiligen Beweissicherungsanordnung wäre dann davon abhängig, ob die Angelegenheit für die betroffene Person besonders dringlich erscheint, etwa weil diese gerade erst von einem rechtswidrigen Inhalt erfahren hat, und durch zügiges Vorgehen zeigt, dass ihr die Verfolgung der Rechtsverletzung besonders dringlich ist. Zeit ist ohnehin der entscheidende Faktor, weil IP-Adressen je nach Anbietendem nur wenige Tage gespeichert werden.

Die Unterscheidung zwischen „normaler“ Beweissicherungsanordnung und einstweiliger Beweissicherungsanordnung hat auch Folgen für die Beweis- bzw. Glaubhaftmachungslast: Die bloße Glaubhaftmachung i.S. des § 31 FamFG genügt auch im Verfahren der freiwilligen Gerichtsbarkeit nur in Ausnahmefällen, beispielsweise einem einstweiligen Anordnungsverfahren. In allen anderen Fällen wird gem. § 37 FamFG die „volle Überzeugung“ vorausgesetzt, also ein für das praktische Leben brauchbarer Grad von Gewissheit, der vernünftigen Zweifeln Schweigen gebietet. Hier ist klar zu regeln, wann welche Anforderungen gelten.

Zu begrüßen ist, dass die Durchführung des Erörterungstermins, soweit vom Gericht für erforderlich erachtet, durch einen Verweis auf § 128 a der ZPO im Wege der Bild- und Tonübertragung sicher ermöglicht werden soll. Dies hat sich im Rahmen äußerungsrechtlicher Verfahren in den letzten Jahren als sinnvoll, weil ressourcensparend herausgestellt. Im Einzelfall kann davon, wenn die Bedeutung der Angelegenheit es erfordert, natürlich abgesehen werden. Die Durchführung der Erörterungstermine im Wege der Bild- und Tonübertragung erfordert jedoch die Einrichtung einer ausreichenden Anzahl entsprechend ausgestatteter Sitzungssäle in den Gerichten. Bislang ist dies nicht der Fall. Die wenigen entsprechend ausgestatten Sitzungssäle werden häufig von einer ganzen Reihe von Richter*innen, Kammern oder Senaten oder sogar einem ganzen Gericht geteilt. Eine Bündelung der Zuständigkeit des Auskunftsverfahrens bei einigen wenigen oder einem speziellen Gericht, könnte eine rasche technische Ausstattung vereinfachen.

Wie bisher sollen die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit gelten. Die geplante Regelung ist insofern nicht neu, auch wenn die Eckpunkte zum

digitalen Gewaltschutzgesetz mit dem Hinweis auf den Amtsermittlungsgrundsatz diesen Eindruck erwecken.

Sinnvoll ist nach Auffassung des djb die geplante Bündelung der gerichtlichen Zuständigkeit, dass etwa durch Rechtsverordnung ein Gericht zentral als zuständig für das Auskunftsverfahren bestimmt werden kann. Für die Zuständigkeit näher zu bestimmender Landgerichte spricht die Expertise der dort angesiedelten Pressekammern, die sehr erfahren sind im Umgang mit Persönlichkeitsrechtsverletzungen und der erforderlichen Abwägung der widerstreitenden Interessen. Welches Landgericht örtlich zuständig sein soll, ist zu klären, insb. ob der „fliegende" Gerichtsstand des § 32 ZPO, oder die Bestimmung des Gerichtsstands nach dem FamFG Anwendung finden.

Vor diesem Hintergrund wäre nach Auffassung des djb im Zuge echter Verfahrensbeschleunigung und der Umsetzung des Ziels einer Digitalisierung der Justiz[8] nicht nur eine Bündelung der Zuständigkeit der Gerichte möglich und sinnvoll. Folgerichtig wäre es, das Verfahren gänzlich digital auszugestalten: von einer digitalen Eingabemaske zur Einreichung des Antrags, der Möglichkeit der unmittelbaren digitalen Beweissicherung beim Gericht selbst (ohne etwa Screenshots ausdrucken zu müssen) und durch direkte Kommunikation zwischen Antragsteller*in, dem Gericht und den Plattformbetreiber*innen auf elektronischem Wege. Eine komplett digitale Ausgestaltung trägt dem Verfahrensgegenstand – digitaler Gewalt und Rechtsverletzungen – am besten und unmittelbarsten Rechnung. Vorbilder könnten etwa die bereits bestehenden Meldestellen einiger Bundesländer sein, die sehr einfach und rein digital eine Möglichkeit bieten, strafbare Hasskommentare aus dem Netz anzuzeigen[9]. Im Zuge dessen müsste auch nach Erlass eines Beschlusses zwingend Sorge dafür getragen werden, dass ein solcher Beschluss dann nicht analog – in Papierform – zugestellt werden muss, gar im Wege der Parteizustellung. Vielmehr sollte das Gericht die Bekanntgabe bzw. Zustellung des Beschlusses ebenfalls elektronisch durchführen können (immerhin muss gem. § 41 Abs. 1 FamFG ein anfechtbarer Beschluss, der dem erklärten Willen der Empfänger*innen widerspricht, zugestellt werden). Das Auskunftsverfahren wäre durch eine rein digitale Ausgestaltung noch niedrigschwelliger, könnte von den Betroffenen also insbesondere ohne die Inanspruchnahme anwaltlicher Unterstützung rein digital betrieben werden – auch wenn diese inhaltlich, was die *Künast*-Beschlüsse zeigen, in vielen Fällen sinnvoll und wünschenswert ist und bleibt. So könnte das BMJ zugleich zusammen mit den Ländern bei der Digitalisierung der Justiz im Bereich digitaler Gewalt eine Vorreiterrolle einnehmen.

Kurzum: Soweit das BMJ plant, das Auskunftsverfahren effektiver auszugestalten, wird dies vom djb als sinnvoll begrüßt. Die derzeitigen Pläne der Bundesregierung gehen nach Auffassung des djb aber noch nicht weit genug. Hier sieht der djb die Chance, eine echte Digitalisierung der Justiz auf den Weg zu bringen, und zwar nicht einhergehend mit einer Beschränkung des Rechtsschutzes für Betroffene, sondern im Gegenteil einer echten Erweiterung und Erleichterung. Gerade bei der

[8] https://www.bmj.de/SharedDocs/Artikel/DE/2022/0927_Pakt_Rechtsstaat.html

[9] https://www.polizei.sachsen.de/onlinewache/meldunghasskriminalitaet.aspx, https://zhin.de/, oder auch https://hessengegenhetze.de/hate-speech-und-extremismus-melden

Bekämpfung digitaler Gewalt drängt es sich auf, die Möglichkeiten einer digitalen Justiz auszuweiten und auszureizen.

2. Die Einführung (vorübergehender) richterlicher Accountsperren

a) Grundsätzliches – auch zur Frage der Effektivität

Schon lange hat sich der djb[10] ebenso wie andere Verbände[11] für die Einführung richterlicher Accountsperren ausgesprochen. Hintergrund ist, dass die Möglichkeit der Nutzung von digitalen Diensten anonym oder unter Nutzung eines Pseudonyms ausdrücklich bestehen bleiben soll, also auf eine Klarnamenpflicht weiterhin verzichtet wird. Dies führt dazu, dass sich überaus häufig nicht herausfinden lässt (es sei denn, man führt das o.g. Auskunftsverfahren durch), wer sich hinter einem Account verbirgt, obwohl von diesem Account eine Rechtsverletzung ausgeübt wurde. Dies kann umso dramatischer sein, wenn es sich um einen Account handelt, von dem aus wiederholt (schwere) Rechtsverletzungen begangen werden. Den Betroffenen blieb bisher keine Möglichkeit, abgesehen von langwierigen und häufig genug ergebnislos eingestellten strafrechtlichen Ermittlungsverfahren, herauszufinden, wer verantwortlich für den Account ist, um gegen die Rechtsverletzer*innen (zivilrechtlich) vorzugehen. Die Einführung der geplanten richterlich angeordneten Accountsperre würde jedenfalls die wiederholten Rechtsverletzungen über einen Account abstellen. Nicht klar – und daher durch das BMJ klarzustellen – ist, ob der Anspruch auch dann bestehen soll, wenn bekannt ist, wer den Account betreibt, von dem „notorische Rechtsverletzungen“ ausgehen. Dies würde der djb begrüßen.

Im öffentlichen Diskurs über die Effektivität von Accountsperren wird oft eingewandt, dass die Einrichtung neuer Accounts durch Personen, deren bisheriger Account oder bisherige Accounts zeitweilig gesperrt werden, innerhalb weniger Minuten möglich sei. Sogenannte Internet-Trolle, die ohnehin über mehrere Accounts/Konten verfügen, würden sich mit vorübergehenden Accountsperren wohl kaum eindämmen lassen. Auch ist zu lesen, dass diejenigen Täter*innen digitaler Gewalt, die nicht selbst über eine hohe Reichweite verfügten, sondern ihre Hassbotschaften und sonstigen rechtsverletzenden Inhalte in Kommentare anderer Seiten, Accounts und Profile mit hoher Reichweite schreiben, von (zeitweiligen) Accountsperren kaum beeinträchtigt würden. Dagegen schränkten (auch nur vorübergehende) Accountsperren die Meinungsäußerungsfreiheit erheblich ein.

Aus Sicht des djb berücksichtigt diese Kritik zu wenig, dass es eine Vielzahl von Accounts, Seiten oder Gruppen „notorischer Rechtsverletzer*innen“ gibt, die gerade durch und aufgrund ihrer verbreiteten rechtsverletzenden Inhalte bei einer entsprechenden Community eine hohe Reichweite, also eine große Anzahl von

[10] Vgl. nur https://www.djb.de/fileadmin/user_upload/st21-18_Antifeminismus_im_Netz.pdf und https://www.djb.de/wahlforderungen

[11] file:///C:/Users/v.haisch/Downloads/2023-05-22-DigGewSchG_GFF.pdf

„Follower*innen“ bzw. „Freund*innen“ haben. Es gibt zahlreiche Accounts, die nichts anderes tun, als beispielsweise Politiker*innen Falschzitate zu unterstellen oder beleidigende Fotos und/oder Äußerungen zu posten, um so ihre Follower*innen/Freund*innen dazu zu bringen, dort entsprechende Hasskommentare zu hinterlassen. Nicht selten finden sich unter solchen Posts von Falschzitaten oder „Memes“ hunderte schwer rechtsverletzender Kommentare. Solche anonym bleibenden Accounts könnten durch (zeitweilige) Accountsperren durchaus erheblich in ihrer Wirkung beschränkt und die Betroffenen umfassend geschützt werden. Zwar gilt auch hier das Argument, dass ein solcher Account sich jederzeit neu gründen kann. Allerdings müssten die Täter*innen erst einmal wieder – immer noch anonym – eine vergleichbar große Anzahl von Followern/Freund*innen generieren, also ihre (erschreckend hohe) Reichweite neu aufbauen. Dies kann dazu führen, dass „notorische Rechtsverletzer*innen“ durch eine (zeitweilige) Sperre ihres Accounts von ihren Umtrieben für eine gewisse Zeit, oder auch dauerhaft, abgebracht werden.

Aus diesem Grund begrüßt der djb die geplante Einführung der Möglichkeit richterlicher Accountsperren. Ein weiterer Grund ist, dass auf diesem Wege die Entscheidung über die Sperrung eines Accounts, und mag sie auch nur zeitweilig sein, nicht länger (nur) in den Händen der betroffenen Anbieter*innen digitaler Dienste liegt. Derartiges sieht – wenngleich als Pflicht zur zeitweiligen Sperre von missbräuchlich genutzten Accounts nach Vorwarnung – Art. 23 DSA vor, der der geplanten Regelung daher auch nicht im Wege stehen dürfte Vielmehr werden angesichts der geplanten Voraussetzungen dieses neuen, bisher nicht gekannten Rechtsinstruments (das sich ja gegen die Anbieter*innen digitaler Dienste richten soll), Richter*innen unter Berücksichtigung aller rechtsstaatlicher Erwägungen hierüber zu bestimmen haben.

b) (Strenge) Tatbestandsvoraussetzungen für die Verhängung (zeitweiliger) Accountsperren

Der Anspruch auf Verhängung (vorübergehender) Accountsperren soll nach den Plänen des BMJ nur unter strengen, bisher gleichwohl nur grob umrissenen Voraussetzungen und nur auf richterliche Anordnung hin bestehen können. Kumulative Tatbestandsvoraussetzungen sind dabei, dass von einem Account wiederholte Verletzungen von Rechten begangen werden, eine Inhaltemoderation als milderes Mittel nicht ausreicht und die Gefahr der Wiederholung schwerwiegender Beeinträchtigungen des allgemeinen Persönlichkeitsrechts besteht. Ferner ist Voraussetzung, dass der*die Dienstanbieter*in den*die betroffene*n Accountinhaber*in vorab auf ein anhängiges Sperrersuchen hingewiesen und ihm*ihr Gelegenheit zur Stellungnahme gegeben hat. In jedem Fall muss die Verhängung einer (zeitweiligen) Accountsperre im konkreten Fall verhältnismäßig sein, gerade auch mit Blick auf ihre Dauer. Insgesamt soll es sich bei diesem neuen Instrument um einen ultima ratio Rechtsbehelf handeln.

Da die angedachten Regelungen, die Tatbestandsvoraussetzungen und auch das prozessuale Vorgehen mit Blick auf dieses neue Rechtsinstrument in dem Eckpunktepapier nur sehr grob umrissen sind, kann auch diese Stellungnahme zur konkreten Ausgestaltung nur entsprechend generell formuliert werden. Bei der Einführung richterlicher Accountsperren wird jedoch Folgendes zwingend zu beachten sein:

Da sich das Verfahren gegen die Diensteanbieter*innen richtet, und nicht gegen die Accountinhaber*innen selbst, ist Letzteren rechtliches Gehör zu gewähren: Es muss sichergestellt und dokumentiert werden, dass die jeweiligen Accountinhaber*innen vor Erlass einer (zeitweiligen) Accountsperre von den Diensteanbieter*innen auf das Sperrersuchen hingewiesen werden und Gelegenheit zur Stellungnahme erhalten. Zur Sicherstellung ausreichenden rechtlichen Gehörs sollte nicht nur die Tatsache, dass eine entsprechende Möglichkeit zur Stellungnahme gegeben sein muss, gesetzlich geregelt werden. Es sollte zugleich konkret ausgestaltet werden, in welcher Form diese erfolgen muss. Dass die Beteiligung ansonsten von unterschiedlichen Diensteanbieter*innen ganz unterschiedlich ausgestaltet wird, zeigt eindrücklich die Erfahrung mit den NetzDG und den dort vorgeschriebenen Meldeverfahren und Transparenzberichten.

Eine Tatbestandsvoraussetzung, auf die es wesentlich ankommen dürfte, bleibt bisher unklar gefasst: In den Eckpunkten für ein Gesetz gegen digitale Gewalt heißt es, dass eine Accountsperre nur angeordnet werden kann, wenn „*die Gefahr der Wiederholung schwerwiegender Beeinträchtigungen des allgemeinen Persönlichkeitsrechts durch von einem spezifischen Account veröffentlichte Inhalte besteht*“. Dem ist zum einen zu entnehmen, dass eine solche Accountsperre nicht bereits (wie der oben skizzierte Auskunftsanspruch) im Fall der Verletzung (irgend)eines absoluten Rechts, sondern nur bei schwerwiegenden Beeinträchtigungen des allgemeinen Persönlichkeitsrechts bestehen soll. Hier stellt sich die Frage, weshalb die Möglichkeit richterlicher Accountsperren auf das allgemeine Persönlichkeitsrecht beschränkt bleiben soll, während das BMJ das Erfordernis des Auskunftsanspruchs auch im Fall der Verletzung des Rechts an eingerichteten und ausgeübten Gewerbebetrieb ausdrücklich betont. Wird durch einen Account wiederholt und schwerwiegend das Recht am allgemeinen und ausgeübten Gewerbebetrieb verletzt, ist nicht ersichtlich, warum nicht auch ein solcher (dann womöglich marktverzerrender) Account bei Vorliegen sämtlicher weiterer Tatbestandsvoraussetzungen zeitweilig und auf richterliche Anordnung hin gesperrt werden sollte.

Klar ist, dass auch im Fall wiederholter schwerwiegender Verletzungen des Rechts am eigenen Bild gem. §§ 22, 23 KUG (wegen der Verbreitung oder öffentlichen Zurschaustellung von Bildnissen) oder des allgemeinen Persönlichkeitsrechts durch die Erstellung oder Manipulation von Bildnissen (etwa wenn es um die heimliche Erstellung von Bildnissen oder Deepfakes geht) ein Anspruch auf richterlich

angeordnete Accountsperren bestehen kann. Das Recht am eigenen Bild als besondere Ausprägung des allgemeinen Persönlichkeitsrechts und der Bildnisschutz, soweit er direkt dem allgemeinen Persönlichkeitsrecht entspringt, dürften auch hier endlich an Bedeutung bei der Rechtsverfolgung gewinnen.

Des Weiteren muss klar geregelt werden, wie in dem Zusammenhang die „Gefahr der Wiederholung" und der Begriff „schwerwiegender Beeinträchtigungen des allgemeinen Persönlichkeitsrechts" zu verstehen sein sollen. Der djb regt an, dies entsprechend der Vermutung des Bestehens der Wiederholungsgefahr im Fall bereits erfolgter Rechtsverletzungen im Presse- und Äußerungsrecht auszugestalten. Nach ständiger Rechtsprechung u.a. des BGH wird die für den Unterlassungsanspruch aus § 1004 Abs. 1 Satz 2 BGB erforderliche Wiederholungsgefahr aufgrund einer erfolgten Rechtsverletzung vermutet. Diese Vermutung für das Vorliegen der Wiederholungsgefahr kann zwar entkräftet werden, aber an die Entkräftung sind strenge Anforderungen zu stellen. Hierzu bedarf es im Regelfall der Abgabe einer strafbewehrten Unterlassungsverpflichtungserklärung gegenüber dem*der Gläubiger*in des Unterlassungsanspruchs oder beispielsweise einer gegenüber einer anderen Person abgegebene Unterlassungsverpflichtungserklärung, wenn diese geeignet scheint, den*die Verletzer*in wirklich und ernsthaft von weiteren Verstößen abzuhalten. Die Widerlegung der tatsächlichen Vermutung für das Vorliegen der Wiederholungsgefahr kann (ausnahmsweise) auch dann angenommen werden, wenn der Eingriff durch eine einmalige Sondersituation veranlasst war[12].

Die Übernahme der Vermutung der Wiederholungsgefahr erscheint im Zusammenhang mit richterlichen Accountsperren erforderlich, da die Gefahr, dass weitere schwerwiegende Beeinträchtigungen von dem spezifischen Account ausgehen werden, von der betroffenen Person ansonsten kaum nachgewiesen werden können. Ein Nachweis von in der Zukunft liegenden Handlungen kann nicht gelingen. Es muss also eine Vermutungsregelung mit Blick auf eine oder mehrere bereits erfolgte Rechtsverletzung(en) eingeführt werden.

Unklar ist zudem, ob das auf Seite 5 der Eckpunkte für ein Gesetz gegen digitale Gewalt erwähnte Merkmal „schwerwiegender" Beeinträchtigungen synonym für „wiederholte Rechtsverletzungen" stehen soll, oder zusätzlich Voraussetzung sein soll, dass die Rechtsverletzung(en) entsprechend jeweils und für sich genommen „schwerwiegend" sein müssen. Sicherlich gibt es auch hier Rechtsprechung zum Presse- und Äußerungsrecht, insb. im Zusammenhang mit der Zuerkennung eines Anspruchs auf Zahlung einer Geldentschädigung, die hier herangezogen werden kann. So kann eine besondere Schwere der Rechtsverletzung dort sowohl mit Blick auf die Qualität einzelner, also einmaliger Rechtsverletzungen, als auch aufgrund der hartnäckigen Wiederholung von (für sich genommen jeweils nicht

[12] BGH, Urteil vom 4.6.2019 – VI ZR 440/18

schwerwiegenden) Rechtsverletzungen bejaht werden. In beiden Fällen (besondere Qualität aber auch Quantität der Rechtsverletzung(en)) sollte nach Auffassung des djb eine zeitweilige Accountsperre möglich sein. Allerdings bedarf es sehr klarer Tatbestandsvoraussetzungen und Erläuterungen.

Der djb merkt kritisch an, dass Accountsperren derzeit nur für Fälle geplant sind, in denen wiederholte Rechtsverletzungen über „den gleichen Account verbreitet werden". Eine richterliche Accountsperre müsste darüber hinaus auch dann greifen können, wenn eine Person für ihre rechtsverletzenden Inhalte mehrere Accounts verwendet. Im Zuge der geplanten Ausweitung des Auskunftsanspruchs könnte dies offengelegt werden. Das setzt aber voraus, dass – so versteht der djb die Eckpunkte für ein Gesetz gegen digitale Gewalt derzeit – auch dann richterliche Accountsperren angeordnet werden können, wenn bekannt ist, wer den Account – oder eben die Accounts – betreibt.

Der djb regt zudem an, richterliche Accountsperren auch für zwei weitere Fälle vorzusehen: Wenn es von einem speziellen Account nicht nur zu Verletzungen des allgemeinen Persönlichkeitsrechts einer erkennbaren Person, sondern mehrerer Betroffener kommt. Und auch in Fällen, in denen es zu (ggf. wiederholten) volksverhetzenden Inhalten kommt, es also keine individuell Betroffenen im Sinne des Äußerungsrechts gibt. Rechtsverletzungen, die über solche Accounts begangen werden, und die verschiedene Opfer oder ganze Gruppen verunglimpfen (Letzteresohne dass eine individuell betroffene Person auszumachen ist), sollten von den vorgesehenen Sperren ebenfalls erreicht werden. Bisher sind nur individuell in ihrem allgemeinen Persönlichkeitsrecht verletzte Personen im Blick der Regelung. Das genügt im Kampf gegen digitale Gewalt nicht.

Auch hier gilt: In Anlehnung an Art. 86 DSA sollte auch mit Blick auf die Anordnung richterlicher Accountsperren eine Verbandsklagemöglichkeit eingeführt, so dass nicht nur Individuen, sondern auch Einrichtungen, Organisationen oder Vereinigungen die Wahrnehmung der Rechte Betroffener übernehmen können.

Zu klären bleiben zwei weitere Fragen: Welche Folgen hat die Tatsache, dass die Diensteanbieter*innen im Wege der Durchsetzung richterlicher Accountsperren Kenntnis von rechtsverletzenden Inhalten erlangen? Und wie stellt man sicher, dass rechtswidrige Inhalte, die ja zur Sperrung eines Accounts geführt haben, nach dessen „Freischaltung" nicht wieder wahrnehmbar sind?

Und schließlich muss das BMJ die Frage beantworten, ob nicht auch die Verhängung zeitlich unbegrenzter Accountsperren in besonderen Härtefällen möglich sein muss, etwa wenn wiederholt zeitweilige richterliche Accountsperren verhängt wurden, das Verhalten des Accountinhabers sich aber nicht ändert.

3. Die Beibehaltung und Kompetenzerweiterung des inländischen Zustellungsbevollmächtigten

a) Grundsätzliches

Die Beibehaltung und Kompetenzerweiterung des „inländischen Zustellungsbevollmächtigten“ ist aus Sicht des djb für die Praxis der Rechtsdurchsetzung gänzlich unverzichtbar. Gerade in Ansehung der strengen Zustellungsregelungen insbesondere im einstweiligen Rechtsschutz im Rahmen der ZPO, die zum Teil sogar die Zustellung im Parteiwege vorsehen, muss den Betroffenen eine einfache und praktikable Zustellung insb. gerichtlicher Beschlüsse möglich sein. Gerade bei Zustellungen an in der Regel im Ausland ansässige Dienste werden Betroffenen erhebliche Hürden in den Weg gelegt. Hier braucht es inländische Zustellungsbevollmächtigte. Es ist daher uneingeschränkt zu begrüßen, dass Anbieter*innen digitaler Dienste (auch) zukünftig verpflichtet sein sollen, inländische Zustellungsbevollmächtigte zu benennen.

Dabei ist kritisch anzumerken, dass in den Eckpunkten nicht von Anbieter*innen digitaler Dienste, sondern ausschließlich von „Sozialen Netzwerken“ die Rede ist. Die Benennung von inländischen Zustellungsbevollmächtigten soll nach dem bisherigen Wortlaut begrenzt sein auf Soziale Netzwerke, nicht aber beispielsweise Messenger-Dienste, Porno-Plattformen, Internetzugangsdienste oder auch VPN-Dienste. Sachliche Gründe für eine entsprechende Ungleichbehandlung bzw. Privilegierung sind nicht ersichtlich. Die Ausführungen in den Eckpunkten zum Gewaltschutzgesetz (dort insbesondere unter 3. a) gelten hier wie dort: In beiden Fällen ist Betroffenen von Rechtsverletzungen im digitalen Raum die Durchsetzung ihrer Rechte zu erleichtern. In beiden Fällen sind förmliche Auslandszustellungen mit einem besonderen Zeit- und Kostenaufwand verbunden. Dies gilt umso mehr, als ein Großteil dieser Anbieter*innen im Ausland ansässig ist.

Wie wichtig die Möglichkeit einer wirksamen Zustellung auf einfachem Wege im Inland für die Betroffenen ist, zeigt nicht zuletzt eine Entscheidung des Bundesgerichtshofs vom 10.11.2022 (I ZB 10/22). Danach gilt: Gläubiger*innen (im Falle digitaler Gewalt also die verletzten Personen) sind auch für die wirksame Zustellung einer Beschlussverfügung nach den allgemeinen Regeln darlegungs- und beweisbelastet.

b) Erweiterung der Zuständigkeit

Uneingeschränkt zu begrüßen ist die Ausweitung der Zuständigkeit inländischer Zustellungsbevollmächtigter auf außergerichtliche Schreiben, etwa Aufforderungen zur Löschung rechtswidriger Inhalte. Die bisherige Situation, dass Betroffene zwar die Möglichkeit haben, über Meldeformulare oder auch per E-Mail Anbieter*innen digitaler Dienste auf Rechtsverletzungen hinzuweisen, ist unzureichend. Trotz automatisch generierter Eingangsbestätigung können die Betroffenen nie wissen, ob ihre Hinweise tatsächlich zugegangen sind und geprüft werden (können). Zurecht weisen die Eckpunkte für ein Gesetz gegen digitale Gewalt mehrfach und ausdrücklich auf die Bedeutung hin, die die Kenntniserlangung der Anbieter*in von einem rechtswidrigen Inhalt hat, da erst diese Handlungspflichten auslöst. Aber auch für die Einleitung gerichtlicher

Verfahren im Rahmen der privaten Rechtsverfolgung, etwa der Geltendmachung von Unterlassungsansprüchen, würde es für die Betroffenen ein hohes Maß an Rechtssicherheit bedeuten, wenn inländische Zustellungsbevollmächtigte benannt werden müssten.

Die Frage, ob die Pflicht zur Benennung von inländischen Zustellungsbevollmächtigten mit dem Herkunftslandprinzip des Artikel 3 Abs. 2 RL 2000/31 EG vereinbar ist, wird in der Literatur unterschiedlich beantwortet. Inhaltliche Gründe, die gegen eine (nationale) Pflicht zur Benennung von inländischen Zustellungsbevollmächtigten sprechen könnten, sind nicht ersichtlich. Insbesondere gilt dies mit Blick auf den DSA, der gerade keinen „inländischen Zustellungsbevollmächtigten“ vorsieht, sondern lediglich einen „gesetzlichen Vertreter“ für den Fall, dass Anbieter*innen von Vermittlungsdiensten, die keine Niederlassung in der Europäischen Union haben, ihre Dienste in der EU anbieten. Ohne nationale Regelung würde eine erhebliche Schutzlücke bleiben.

Prof. Dr. Maria Wersig
Präsidentin

Anke Stelkens und Verena Haisch
Vorsitzende der nichtständigen Kommission Digitales