LEIBNIZ-INSTITUT
FÜR MEDIENFORSCHUNG
HANS-BREDOW-INSTITUT

Sünje Andresen, Stephan Dreyer, Matthias C. Kettemann,
Tobias Mast, Katharina Mosene, Jan Rau, Valerie Rhein,
Wolfgang Schulz, Neda Wysocki

Eckpunkte des BMJ zum Gesetz gegen digitale Gewalt

Stellungnahme

Hamburg, Mai 2023

Inhalt

1. Zur Einordnung

Der aktuelle Haftungsrahmen, die pseudonyme Nutzungsmöglichkeit von Social Media-Plattformen und die vermeintlich weniger strikten sozialen Normen unterliegenden Kommunikationsräume dort führen zu einem Anwachsen beleidigender, verunglimpfender und herabwürdigender Äußerungen und Darstellungen.[1] Betroffene sind persönlichen Angriffen und Anfeindungen ausgesetzt, die sie massiv in ihren Allgemeinen Persönlichkeitsrechten – und dort insbesondere in ihrem sozialen Geltungsanspruch – verletzen. Daneben haben sich weitere Formen digital vermittelter persönlichkeitsrechtsverletzender Handlungen entwickelt (z.B. sexuelle Grenzverletzungen; digitales Stalking; bildbasierte sexualisierte Gewalt wie non-konsensuales Sexting, Deepfakes oder die Weitergabe von intimen Aufnahmen; Erpressung mit digitalen Bildern; Doxing), durch die Betroffene nicht nur unmittelbar in ihren Rechten und ihrer persönlichen Integrität geschädigt werden, sondern die auch das Potenzial aufweisen, die kommunikative Teilhabemöglichkeiten und ihre Ausübung zu schmälern oder ganz zu verhindern. Bei digitalem Gewaltschutz geht es insoweit nicht ausschließlich um die Gewährleistung individueller Freiheitsrechte der Betroffenen, auch gesellschaftliche Interessen wie Sicherheit und Ordnung, demokratische Teilhabe, kommunikative Chancengerechtigkeit und vielfältige gesellschaftliche Diskurse sind durch das Phänomen berührt. Gleichzeitig ist seit vielen Jahren erkannt, dass die Möglichkeiten Betroffener, sich gegen Angriffe auf ihre Persönlichkeitsrechte zur Wehr zu setzen, nicht nur begrenzt sind, sondern insbesondere in der straf- und zivilrechtlichen Praxis auf Anforderungen und Hürden treffen, die die Wirksamkeit der bereits existierenden Instrumente schmälern.

Vor diesem Hintergrund kann das Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI) das Vorhaben des BMJ, ein Gesetz gegen digitale Gewalt vorzulegen, nachvollziehen. Als unabhängige Forschungsinstitution, die sich der Erforschung der Transformation der öffentlichen Kommunikation verschrieben hat, weisen die Fragen des Eckpunktepapiers viele Überlappungen zu dem Fokus des Instituts auf, darunter wissenschaftliche Aktivitäten im Bereich Plattform-Governance, gesellschaftlicher Zusammenhalt, Kommunikationsregulierung wie durch das NetzDG- und das Äußerungs(straf)recht, Kommunikations- und Interaktionsrisiken im Kinder- und Jugendmedienschutz und aktuelle Arbeiten zum Digital Services Act. Das HBI nimmt die Gelegenheit der Stellungnahme gerne wahr, um auf einzelne Aspekte des Eckpunktepapiers hinzuweisen, aber auch, um auf grundsätzlichere Regulierungsaspekte im Rahmen der Einführung eines Gesetzes gegen digitale Gewalt hinzuweisen.

[1] Vgl. Hoven, Hass im Netz, Leipzig 2022, abrufbar unter https://www.uni-leipzig.de/fileadmin/prins_import/dokumente/dok_20220829123452_ae0b27c451.pdf.

2. Anwendungsbereich eines Digitalen Gewaltschutzgesetzes

Der Zuschnitt des Anwendungsbereichs eines Gesetzes zum Schutz vor digitaler Gewalt ist zu sehen mit Blick auf die Instrumente, die Betroffenen zur Rechtsdurchsetzung zur Verfügung stehen. Je eingriffsintensiver die Instrumente (und Sanktionen), desto klarer muss der sachliche Anwendungsbereich des Normenwerks sein. Bei einem zu weiten Anwendungsbereich besteht ansonsten die Gefahr eines regulativen Spillovers, d.h. die rechtlichen Instrumente könnten dann auch auf Sachverhalte Anwendung finden, die entweder vorab noch nicht klar absehbar waren, oder die Situationen betreffen, bei denen der Einsatz der Instrumente angesichts marginaler Rechtsberührungen unverhältnismäßig erschiene. Gerade im Äußerungsrecht besteht eine verfassungsrechtliche Rechtsprechung, die immer wieder auf die fundamentale Wichtigkeit der Ausübbarkeit des Rechts auf freie Meinungsäußerung verweist und relativ hohe Anforderungen an gesetzliche Eingriffe in dieses Recht legt. Entsteht etwa durch einen nicht vollkommen klaren Anwendungsbereich Unsicherheit darüber, ob die Vorschrift auf eine bestimmte Äußerung oder Darstellung Anwendung findet oder nicht, können empfindliche Instrumente und Sanktionen dazu führen, dass bestimmte Meinungen gar nicht erst geäußert werden. Derartige Auswirkungen von Rechtsnormen auf den öffentlichen Diskurs (Chilling Effects) sieht das BVerfG als klaren verfassungswidrigen Eingriff in die Meinungsfreiheit.[2]

Vor diesem Hintergrund wird es von zentraler Relevanz sein, den sachlichen Anwendungsbereich eines digitalen Gewaltschutzgesetzes auf klare und schwere Verstöße gegen das Allgemeine Persönlichkeitsrecht (inkl. seiner Ausprägungen wie Ehrschutz, Recht am eigenen Bild, Recht auf sexuelle Selbstbestimmung, Recht auf Privatheit, Recht auf informationelle Selbstbestimmung) zu beschränken. Der Begriff der „digitalen Gewalt" und der Gewaltbegriff insgesamt knüpfen an stark belastende kommunikative Handlungen an, die schwere geistig-seelische und physische Auswirkungen auf die betroffenen Personen haben. Der vom BMJ vorgeschlagene, sehr weite Anwendungsbereich, der sich auf alle Verletzungen absolut geschützter Rechte bezieht und dabei auch juristische Personen einbezieht, erscheint insoweit als Abweichung von dem im gesellschaftlichen wie im wissenschaftlichen Diskurs vorherrschenden Verständnis von digitaler Gewalt. Daneben erscheint der sehr weite Anwendungsbereich auch mit Blick auf die rechtlichen Instrumente und Sanktionsmöglichkeiten, die das Eckpunktepapier vorsieht, als ein Ansatz mit signifikantem Risikopotenzial für die Meinungsfreiheit und den freien öffentlichen Diskurs.

Das dem Eckpunktepapier beiliegende Beispiel einer Restaurantkritik, bei der der in seinen Rechten verletzte Gewerbebetrieb nach Herausgabe der Anschlussinhaberdaten gegen den vermeintlichen Verletzter mit strafbewehrten Unterlassungsaufforderungen, einstweiligen Verfügungen und Schadensersatzklagen sowie mit möglichen temporären Accountsperren vorgeht, kann als gutes Beispiel dafür dienen, wie groß die Inkohärenz von geplantem

[2] BVerfGE 42, 143 (158 f.); BVerfGE 43, 130 (133, 136).

Anwendungsbereich und dem allgemeinen Verständnis von „digitaler Gewalt" ist – und welche Risiken durch einen zu weiten Anwendungsbereich für die öffentliche Kommunikation entstehen. Wie das Beispiel zeigt, würde mit einem entsprechenden Gesetz ein Rechtsrahmen geschaffen, der signifikante Auswirkungen auf die öffentliche Kommunikation und das, was gesagt werden darf, haben kann. Darüber hinaus würde in der faktischen Gleichsetzung einer überschießenden Restaurantkritik mit einem aggressiven sprachlichen Akt gegen z.B. eine einer besonders vulnerablen Gruppe angehörigen Person einer unzulässigen Gleichsetzung unterschiedlicher Rechtsverletzungsintensitäten der Boden bereitet.

Das HBI empfiehlt vor diesem Hintergrund einen klaren und begrenzten Zuschnitt des Anwendungsbereichs auf Rechtsverletzungen des Allgemeinen Persönlichkeitsrechts von natürlichen Personen. Sollte es einen politischen Wunsch zur gesetzlichen Rahmung von äußerungsrechtlichen Handlungen gegenüber Gewerbebetrieben oder juristischen Personen über die bestehenden strafrechtlichen und lauterkeitsrechtlichen Instrumente hinaus geben, wären entsprechende Regeln ggf. in einem anderen Gesetz besser aufgehoben, da die Äußerungsformen und Schutzgüter bei digitaler Gewalt einer- und bei wettbewerbsrelevanten Kritiken andererseits voneinander abweichen. Eine Beschränkung des gesetzlichen Anwendungsbereichs auf Verletzungen des Allgemeinen Persönlichkeitsrechts natürlicher Personen hielte einer verfassungsrechtlichen Prüfung, insbesondere am Maßstab des allgemeinen Gleichbehandlungsgebots des Art. 3 Abs. 1 GG Stand. Nach diesem ist der Gesetzgeber gehalten, wesentlich gleiche Personengruppen gleich zu behandeln, wenn für eine Differenzierung keine sachlichen Gründe vorliegen. Im Hinblick auf „digitale Gewalt" ist eine Differenzierung zwischen natürlichen und juristischen Personen allerdings jedenfalls gut begründbar. Zwar kommt auch Unternehmen ein Schutz ihres sozialen Achtungsanspruchs und ihrer informationellen Selbstbestimmung zu, der teils über Art. 2 Abs. 1 i.V.m. Art. 19 Abs. 3 GG[3], teils über Art. 14 Abs. 1 i.V.m. Art. 19 Abs. 3 GG konstruiert wird.[4] Das unternehmenseigene Persönlichkeitsrecht ist allerdings nach vorherrschender Ansicht nicht in der Menschenwürde des Art. 1 GG verankert und hat dementsprechend nicht an dessen besonderer Rangstufe Teil.[5] Dementsprechend ist das über Art .2 Abs. 1 oder Art. 14 Abs. 1 vermittelte Schutzniveau, das sich regelmäßig lediglich auf wirtschaftliche Interessen beschränkt, im Vergleich zu betroffenen natürlichen Personen abgesenkt.[6] Eine entsprechend differenzierte Schutzintensität hat auch das BVerfG bereits an verschiedenen Stellen anklingen lassen: „Jedenfalls dort, wo der Grundrechtsschutz an Eigenschaften, Äußerungsformen oder Beziehungen anknüpft, die nur natürlichen Personen wesenseigen sind, kommt eine Erstreckung auf juristische Personen als bloße Zweckgebilde der Rechtsordnung nicht in Betracht. Das wird umso eher der Fall sein, als

[3] BVerfGE 10, 89 (99); 20, 323 (329); 23, 12 (30); 66, 116 (130); 70, 1 (25 f.).
[4] BVerfGE 67, 100 (142 f.).
[5] Vgl. Rixen in Sachs, GG, 9. Aufl. 2021, Art. 2 Rn 77.
[6] Di Fabio in Dürig/Herzog/Scholz, GG, Lfg. 39 (2001), Art. 2 Abs. 1 Rn. 224.

der Grundrechtsschutz im Interesse der Menschenwürde gewährt wird, die nur natürliche Personen für sich in Anspruch nehmen können".[7]

Das Eckpunktepapier sieht zudem einen Anwendungsbereich vor, der sowohl über Telemedien – d. h. etwa über Websites, Soziale Netzwerke oder Video-Sharing-Plattformen vorgenommene Handlungen umfasst, als auch solche, die über interpersonale Kommunikationsdienste wie etwa Instant Messenger begangen werden. Zudem sollen sich die Ansprüche auch auf Internetzugangsdienste erstrecken. Dies erscheint angesichts der „Tatorte" digitaler Gewalt nachvollziehbar. Die Ausweitung auf Messengerdienste (als Tatort) und Internet Service Provider (als Quelle der Zuordnung einer IP-Adresse zu einem Anschlussinhaber) ermöglicht Betroffenen in deutlich mehr Fällen eine erfolgreiche Aussicht auf die Identifikation des Anschlusses, von dem aus eine Handlung vorgenommen wurde; als Ausgangspunkt für einen besseren digitalen Gewaltschutz ist die Erweiterung insoweit anzuraten. Andererseits erhöht ein weiter Anwendungsbereich zivilrechtlicher (Folge-)Ansprüche theoretisch auch das Missbrauchspotenzial der geplanten Rechtsinstrumente (s. dazu unten Punkt 3.1); hier wird das Missbrauchsrisiko und dessen Auswirkungen auf den Einzelnen wie auf die öffentliche Kommunikation insgesamt ebenfalls von der Begriffsweite bzw. einer konkret gefassten Definition der digitalen Gewalt abhängen.

Dem Bundesgesetzgeber muss daneben klar sein, dass mit einem rein äußerungsrechtlichen Ansatz eine Vielzahl von beeinträchtigenden und gefährdenden Ausprägungen digitaler Gewalt gerade nicht umfasst ist. Die teils prekäre Lage von Betroffenen digitaler Gewalt würde sich insoweit nicht verbessern, so etwa in Fällen von Formen digitalen Stalkings, dem heimlichen Einsatz von Überwachungsgeräten und -software, von Formen bildbasierter sexualisierter Gewalt wie Deepfakes, nicht-konsensualem Sexting oder dem Verbreiten intimer Aufnahmen, der Erpressung mit digitalen Bildern, persönlichkeitsrechtsverletzenden Formen des Identitätsdiebstahls und des Doxing, d.h. der Veröffentlichung personenbezogener Daten wie der Privatadresse einer Person. Wenn der Bund Betroffene digitaler Gewalt mit mehr Rechtsschutzmöglichkeiten ausstatten will, dann spiegelt der Anwendungsbereich des jetzigen Eckpunktepapiers nur einen kleinen Teil der relevanten Phänomene wider.

3. Vorgesehene Instrumente

Die im Eckpunktepapier vorgesehenen Rechtsinstrumente beschränken sich im Kern auf verbesserte Auskunftsrechte von Betroffenen zur Ermittlung von Täterinnen und Tätern (3.1), die Mög-

[7] BVerfGE 95, 220 (242); vgl. auch BVerfGE 38, 312 (320).

lichkeit der Anordnung zeitlich begrenzter Sperrungen von Accounts, von denen Rechtsverletzungen ausgehen (3.2.) sowie die Pflicht von Anbietern zur Benennung eines Zustellungsbevollmächtigten im Inland (3.3).

3.1. Stärkung der Auskunftsrechte

Die Stärkung von Betroffenenrechten erfolgt im Eckpunktepapier in einem ersten Schritt durch die Erweiterung von Auskunftsansprüchen gegenüber Diensteanbietern. Anders als derzeit (s. § 21 Abs. 2, 3 TDDSG) soll eine Rechtsgrundlage geschaffen werden, die es Betroffenen ermöglicht, neben den Bestandsdaten auch die Nutzungsdaten von einem Diensteanbieter herausgegeben zu bekommen. Durch die Einbeziehung von Telekommunikationsdiensten wäre es Betroffenen dann möglich, zunächst die Bestands- und Nutzungsdaten vom hostenden Anbieter zu erhalten, und dort, wo die Bestandsdaten sich als unrichtig herausstellen, über eine Anfrage zu der übermittelten IP-Adresse beim relevanten Internet Service Provider die Bestandsdaten des Anschlussinhabers zu erhalten. Ausgestattet mit diesen Informationen können Betroffene dann strafrechtlich oder bzw. und zivilrechtlich gegen den Anschlussinhaber vorgehen. Die Herausgabe auf Antrag unterliegt dem Eckpunktepapier nach einem Richtervorbehalt, so dass grundrechtlichen Anforderungen grundsätzlich Genüge getan ist; insbesondere ist auf diese Weise eine Kontrolle der Zulässigkeit des Anspruchs durch das Gericht gewährleistet, was Missbrauchspotenziale verringert.

Mit Blick auf die aktuelle Praxis der Herausgabeansprüche begegnet der Ansatz aber strukturellen Bedenken: Wie gezeigt handelt es sich bis zu Ermittlung des Anschlussinhabers um ein für die betroffene Person mehrstufiges Verfahren, dessen Erfolg davon abhängt,

- ob die verletzende Person bei dem Telemediendienst oder dem interpersonalen Kommunikationsdienst wahre Bestandsdaten hinterlegt hat, oder – wenn nicht – der Anbieter die IP-Adresse (a) überhaupt speichert oder (b) so lange vorhält, bis die gerichtliche Anordnung den Anbieter erreicht,[8]
- ob die IP-Adresse dann tatsächlich geeignet ist, den Anschlussinhaber zu ermitteln (dies ist etwa schwierig bei Nutzung von VPN-Diensten oder Overlay-Netzwerken wie Tor);
- und schließlich, ob die Identifizierung des Anschlussinhabers zu der Ermittlung der verletzenden Person führt, oder ob ggf. auch ein Rechtsanspruch gegen den Anschlussinhaber direkt in Frage kommt.

[8] Die Frage des Zeitverlaufs bei zweistufigen Herausgabeverfahren ist zentral. In der Regel liegt die Speicherung von Nutzungsdaten bei Internet Service Providern bei 0 bis sieben Tagen, nur in seltenen Fällen bei bis zu 90 Tagen. Der Erfolg eines Auskunftsverfahrens ist damit zentral abhängig von Geschwindigkeit der IP-Herausgabe und dem ISP-bezogenen Beschlusses des zuständigen Landgerichts. In der Regel wird man davon ausgehen können, dass die IP-Adresszuordnung nicht mehr gelingt.

Bei jeder dieser Stufen besteht die Möglichkeit, dass die Betroffenenrechte leerlaufen. Das erscheint insbesondere im Zivilrecht, bei dem die betroffene Person diesen mehrstufigen Aufwand hat, nicht als großer Anreiz zur Wahrnehmung dieser Rechte. Angesichts der hohen Anzahl von Persönlichkeitsrechtsverletzungen stellt sich bei der Delegierung der Rechtsdurchsetzung an Landgerichte zudem die Machbarkeitsfrage angesichts knapper personeller und finanzieller Ressourcen der Gerichte. Dass das Eckpunktepapier an dieser Stelle Eilverfahren und zügige Beweissicherungsverfahren vorsieht, wie sie aus der Durchsetzung bei Urheberrechtsverletzungen gängig sind, kann zu einer zügigeren Rechtsdurchsetzung beitragen. Dabei übersieht das Papier aber den kategorialen Unterschied bei der gerichtlichen Bewertung von technisch dokumentierten, gleichförmigen und eindeutigen Urheberrechtsverletzungen und der äußerungsrechtlichen Prüfung im Einzelfall, ob eine Aussage oder Darstellung tatsächlich eine Persönlichkeitsrechtsverletzung darstellt. Letztere sind oft abhängig vom jeweiligen Kontext, von der Art der betroffenen Person und von ihrem vorausgegangenen Verhalten, und nicht selten unterschiedlichen Interpretationen zugänglich, was ihren Aussagegehalt angeht. Insbesondere bei massenhaften Anträgen zur Herausgabe von Bestands- und Nutzungsdaten in Fällen von vielen vermeintlichen Verletzungshandlungen, die nicht gleichförmig sind, muss das Gericht jeden Einzelfall einer Abwägung zwischen Meinungsfreiheit und Persönlichkeitsrechten zuführen. Hinzu tritt, dass die Spruchpraxis eines Landgerichts keine verbindlichen Auswirkungen auf die anderer Landgerichte hat: Die Aussicht auf Erfolg eines Antrags auf Herausgabe von Bestands- und Nutzungsdaten hängt insoweit auch von der Rechtsansicht des jeweils zuständigen Gerichts ab.

Insgesamt erscheint die Erweiterung der Auskunftsansprüche wie vorgeschlagen aus Betroffenensicht als strukturell lediglich schwache Verbesserung.

3.2. Temporäre Accountsperren nach gerichtlicher Anordnung

Als weiteres Instrument sieht das Eckpunktepapier die temporäre Sperrung von Verletzendenaccounts auf Online-Plattformen vor – insbesondere dann, wenn der Auskunftsanspruch nicht zur Ermittlung der verletzenden Person geführt hat. Die Accountsperre funktioniert in diesen Fällen wie ein technisch durchgesetzter Unterlassungsanspruch: Die verletzende Person soll dadurch von der fortlaufenden Verletzung der betroffenen Person abgehalten werden. An dieses Instrument stellt das Papier starke rechtsstaatliche Anforderungen (ausschließlich bei Rechtsverletzungen mit Wiederholungsgefahr; nur sukzessorisch nach einer eingeleiteten Plattformbeschwerde; erst nach Hinweis an Accountinhaber mit Gelegenheit zur Stellungnahme; zeitliche Begrenzung auf angemessenen Zeitraum). Zudem soll es beschränkt sein auf wiederholte, schwerwiegende Verletzungen von dem gleichen Account.

Bereits die sehr grobe Darstellung des Instruments im Eckpunktepapier begegnet größeren rechtlichen Bedenken:

- Accountsperren stellen keinen wirksamen Schutz vor digitaler Gewalt dar. Sie folgen eher einem Sanktionsgedanken als einem Schutzansatz zur Verhinderung von wiederholten Verletzungen. Die verletzenden Personen haben insbesondere jederzeit die Möglichkeit, die Verletzungen über neu eingerichtete Accounts zu wiederholen bzw. fortzusetzen. Bei der Umgehung der Accountsperren durch Anlegen eines neuen Accounts sehen sich die Accountinhaber zudem keinen unmittelbaren weiteren rechtlichen Sanktionen ausgesetzt (abgesehen von der Löschung des Accounts durch die Plattform selbst wegen Umgehung von AGB-Recht, wenn der Anbieter die Person identifizieren kann), da etwaige Sperranordnungen accountbezogen sind und sich nicht auf die dahinterstehende Person beziehen. Insgesamt steht damit die Eignung des Instruments grundsätzlich in Frage; nicht ausgeschlossen ist aber, das Instrument der Accountsperre als (straf-)rechtliche Sanktion zu nutzen.
- Accountsperren sollen verhältnismäßig sein; als schwerwiegender Eingriff in die Kommunikationsrechte der Accountinhaber darf es insbesondere keine gleichwirksamen Mittel geben, die geringere Eingriffe darstellen. Dies führt notwendigerweise dazu, dass Betroffene zunächst über Auskunftsverfahren in Erfahrung bringen müssten, ob die verletzende Person ermittelbar ist. Eine direkte Inanspruchnahme auf Unterlassung und ggf. Schadenersatz kann insoweit ein wirksameres Mittel darstellen. Insgesamt führt dies aber zu einer deutlichen Verzögerung bei der Stellung des Anspruchs auf Accountsperrung.
- Die unbestimmten Rechtsbegriffe der „wiederholten" und „schwerwiegenden" Persönlichkeitsrechtsverletzungen stellen Einfallstore für unterschiedliche Interpretationen dar und können in der Praxis dazu führen, dass Gerichte unterschiedliche Voraussetzungen für Sperranordnungen sehen.
- Die Anforderung, dass diese Verletzungen vom gleichen Account aus ausgehen müssen, lässt die teils dezentralen und angebotsübergreifenden Formen von Persönlichkeitsverletzungen außer Betracht. Ein Sachverhalt, bei dem Accountsperren helfen könnten, wären Sperren bei sich verstärkenden Hasswellen und kampagnenartigen und plattformübergreifenden Angriffen auf Einzelpersonen; hier könnte das kurzfristige Offline-Nehmen von steuernden und teilnehmenden Accounts als „Wellenbrecher" agieren. Auf diese Fälle findet der Vorschlag im Eckpunktepapier aber keine Anwendung bzw. wären Betroffene dazu gezwungen, gegen jeden einzelnen Account auf jeder Plattform einen eigenen Antrag zu stellen.
- Schließlich stellt sich mit Blick auf das Instrument der Accountsperre die Frage nach der Notwendigkeit und der rechtlichen Zulässigkeit angesichts der Vorgaben in Art. 23 Abs. 1 Digital Services Act. Letztlich würden durch ein digitales Gewaltschutzgesetz Vorgaben

(auch) für Vermittlungsdienste und Online-Plattformen gemacht, die die Sperrung von Accounts beinhalten. Damit würde die nationalen Normen einen Anwendungsbereich betreffen, der durch Art. 23 DSA grundsätzlich vollharmonisiert ist. Daneben bestehen im Zivilrecht bereits Möglichkeiten der Durchsetzung von Unterlassungstiteln gegen Accountinhaber und ggf. Plattformen (etwa über §§ 1004 iVm 823 BGB).

Insgesamt erscheint das Instrument der Accountsperren noch nicht ausgereift und bedarf weiterer rechtlicher Prüfung und – wo möglich – Konkretisierung.

3.3. Ansprechpartner im Inland

Als drittes Instrument sieht das Eckpunktepapier die erleichterte Kontaktaufnahme der Anbieter durch Betroffene in Fällen von Persönlichkeitsrechtsverletzungen vor, wo Betroffene ihre Rechte gegenüber dem Anbieter geltend machen möchten. Die niedrigschwellige Adressierbarkeit und nachweisbare Inkenntnissetzung eines Anbieters ist eine wichtige Voraussetzung der Geltendmachung von Ansprüchen Betroffener. Das HBI unterstützt dieses Instrument ausdrücklich, weist aber auf Fragen der europarechtlichen Zulässigkeit einer solchen Vorgabe hin, da dies als Durchbrechung des Herkunftslandsprinzip aus Art. 3 der E-Commerce-Richtlinie gesehen werden kann. Zwar kann die zivilrechtliche Durchsetzung von Betroffenenrechten unter Umständen in den Bereich der Ausnahmen von Art. 3 Abs. 4 E-Commerce-Richtlinie fallen, doch gelten die Ausnahmen ausschließlich für behördliche Einzelverfahren gegen einen konkreten Diensteanbieter. Allgemeine Vorgaben, wie die Pflicht zur Einsetzung eines nationalen Ansprechpartners, der für die Entgegennahme behördlicher, gerichtlicher und privater Rechtskorrespondenz ermächtigt ist, fallen gemäß Art. 3 Abs. 4 lit. a) ii) der Richtlinie gerade nicht unter die Ausnahme vom Grundsatz des Herkunftslandprinzips.

4. Herausforderungen in der Praxis

Neben den instrumentenbezogenen Überlegungen lässt das Eckpunktepapier zu diesem Zeitpunkt noch weitere Fragen offen, die sich insbesondere auf die praktische Umsetzung der Betroffenenansprüche beziehen:

- Die Durchsetzung über das zuständige Landgericht führt zu Kosten (Anwaltskosten, Gerichtskosten, Kosten auf Seiten des Diensteanbieters). Wer für diese Kosten in welchen Fällen – insbesondere dort, wo die verletzende Person nicht ermittelbar ist - aufkommt, bleibt angesichts der im Papier versprochenen Kostenfreiheit für die betroffene Person unklar.

- Die Zusicherung, dass die Verfahren für die Betroffenen kostenfrei bleiben, werden in vielen Fällen in der Praxis nicht zu einem niedrigschwelligeren Zugang von Betroffenen führen. Die Geltendmachung von rechtlichen Ansprüchen bei einem Landgericht setzt eine Reihe von Anforderungen auf Seiten von Betroffenen voraus, die diese leicht einschüchtern oder überfordern kann. Dadurch entstehen insbesondere für prekäre und marginalisierte Gruppen hohe praktische Hürden beim Zugang zu den geplanten Rechtsinstrumenten. Dazu kann auch insgesamt die schwere Absehbarkeit des weiteren Verfahrens, die Sorgen vor ungeplanten Folgen und vor möglichen Kosten gehören. Dass der Entwurf das Thema der Förderung von analogen wie digitalen Beratungsangeboten für Betroffene bzw. Opfer digitaler Gewalt nicht vorsieht, die diese Zugangshürden senken könnten, ist bedauerlich. Auch die bereits im Diskurs vorgeschlagene Einführung von Verbandsklagerechten kann einzelnen Betroffenen Kostenrisiken bzw. -ängste nehmen und parallel dazu vor einer möglichen Retraumatisierung im Rahmen des gerichtlichen Verfahren schützen.
- Eine Personengruppe, die das Eckpunktepapier bislang ausspart, sind Minderjährige. Auch diese Gruppe kommt immer wieder in Berührung mit verletzenden Äußerungen, hat aber angesichts des Gerichtszwangs keine Möglichkeit, die ihnen zustehenden Rechte selbst durchzusetzen. Der Zugang zu Rechtsmitteln bleibt auch mit den geplanten neun Instrumenten nur über die Erziehungsberechtigen möglich. Die gerade bei Minderjährigen bestehenden erhöhten Anonymitäts- bzw. Geheimhaltungsinteressen sowohl bzgl. der eigenen Kommunikation als auch der Offenbarung im Rahmen zivilrechtlicher Verfahren werden so außer Acht gelassen.
- Schließlich unterstellt das Eckpunktepapier implizit die Kooperation durch die angeschriebenen Telemedien- und Telekommunikationsdienste. Die Erfahrungen der letzten Jahre mit diesen Anbietern haben aber gezeigt, dass es einzelne Diensteanbieter gibt, die sich kategorisch nicht an nationale Vorgaben halten. Das geplante Gesetz läuft hier leer; zudem kann sich dadurch das systematische Risiko einer Verlagerung von Rechtsverletzungen auf just diese Dienste ergeben.

5. Zusammenfassende Beurteilung

Das Eckpunktepapier adressiert ein wichtiges Thema und zielt mit der Einführung von drei Maßnahmen (erweiterte Auskunftsansprüche; temporäre Accountsperrungsansprüche; bessere Ansprechbarkeit von Anbietern) auf die Verbesserung der Durchsetzung rechtlicher Ansprüche Betroffener ab. In der jetzigen Fassung begegnen allerdings alle drei Instrumenten rechtlichen Bedenken und Fragen der Effektivität in der Praxis.

Deutlich geworden ist insbesondere, wie eng der Zusammenhang zwischen der Breite des genutzten Verletzungs- oder Gewaltbegriffs und der Gefahr von Chilling Effects für die öffentliche Kommunikation sein wird: Je breiter und vager der sachliche Anwendungsbereich, desto unklarer ist die Möglichkeit der rechtlichen Einschätzung des eigenen Handelns, und desto eher sehen Kommunizierende ggf. von einer (auch zulässigen) Äußerung ab. Die geplante Einbeziehung juristischer Personen als Anspruchsberechtigte droht bei einem weiten Gewaltbegriff bestehende Machtungleichgewichte zu verstärken, insbesondere mit Blick auf die Möglichkeit, aus Unternehmenssicht unliebsame Äußerungen und selbst sachliche Kritik aus dem Netz entfernen zu wollen. Es erscheint angeraten, den Gewaltbegriff auf Rechtsverletzungen von natürlichen Personen zu begrenzen.

Insgesamt stellt sich angesichts der Rechts-, der Wirksamkeits- und der Praktikabilitätsprobleme die Frage, ob die Übergabe der Durchsetzung von Betroffenenrechten an das Zivilrecht sinnvoll ist. Bei vielfachen und schweren Persönlichkeitsrechtsverletzungen geht es zentral um den staatlichen Gewährleistungsauftrag, eine Rechtsordnung zu schaffen, die einzelne Personen vor Persönlichkeitsrechtsverletzungen zu schützen in der Lage ist. Das vorgesehene Konzept, bei Persönlichkeitsrechtsverletzungen in erster Linie der betroffenen Person Mittel zur Rechtsdurchsetzung an die Hand zu geben, erscheint angesichts der auch betroffenen gesellschaftlichen und staatlichen Interessen einer nicht-toxischen öffentlichen Kommunikation, die zur kommunikativen Teilhabe aller Bürgerinnen und Bürger einlädt, jedenfalls suboptimal.

Angesichts der Verletzungshandlungen erscheint angezeigt, jedenfalls auch über Möglichkeiten des Ordnungsrechts für die Gewährleistung von Schutz vor Persönlichkeitsrechtsverletzungen zu diskutieren – angesichts der auch berührten überindividuellen, gemeinschaftlichen Interessen kann dies auch eine Thematik der Kommunikationsregulierung sein. Ein medienaufsichtsrechtliches Vorgehen gegen signifikante Persönlichkeitsrechtsverletzungen könnte zumindest einige der aufgezeigten Problematiken schmälern.

Letztlich aber muss festgestellt werden, dass jeder staatliche Ansatz angesichts der Vielzahl der begangenen Verletzungen schlecht skaliert. Die Bearbeitung von Einzelfällen ist personaleinsatz- und kostenintensiv und kostet Zeit. Alternative Governanceansätze, die statt einzelner behördlicher oder gerichtlicher Stellen Formen der Netzwerkverantwortung mit prozeduralen Vorgaben hinsichtlich der einzuhaltenden Verfahrensgestaltungen und Entscheidungsmaßstäbe machen, können das Problem der Skalierbarkeit ggf. besser lösen. Plattformen verfügen über ausdifferenzierte Governanceinstrumente von Informationsflüssen und können gerade kampagnenhafte Kommunikationsakte gut erfassen und etwa dort, wo eine entsprechende Sensibilisierung im Austausch mit Politik und Wissenschaft erfolgt ist, effektiv steuern bzw. unterbinden. Hier zeigt der Digital Services Act, dass es auch Formen hybrider

Governance und regulierter Selbstregulierung gibt, bei denen gesetzliche Vorschriften Vorgaben für die Gestaltung von Verfahren auf der Seite der Plattformanbieter machen, die diese dann in skalierbare, gelebte Moderations- und Sperrpraktiken umsetzen. Das Eckpunktepapier verharrt hier noch in eher klassischen Regulierungsansätzen.

Hamburg, im Mai 2023