Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
19(23)123

Prof. Dr. Dirk Heckmann

Gutachterliche Stellungnahme

für den Ausschuss Digitale Agenda des Deutschen Bundestages

Sachverständigen-Anhörung vom 24. März 2021 zu den Themen

a) Digitale Gewalt gegen Frauen und Mädchen (Selbstbefassung);

b) Antrag der Abgeordneten Anke Domscheit-Berg, Cornelia Möhring, Doris Achelwilm, weiterer Abgeordneter und der Fraktion DIE LINKE: Digitale Gewalt gegen Frauen BT-Drucksache 19/25351

24. März 2021

Univ.-Prof. Dr. Dirk Heckmann

Lehrstuhl für Recht und Sicherheit der Digitalisierung

Ass. jur. Valentin Vogel, wiss. Mitarbeiter

TUM Center for Digital Public Services
Munich Center for Technology in Society
Technische Universität München

Direktor:
Univ.-Prof. Dr. jur.
Dirk Heckmann
dirk.heckmann@tum.de

Geschäftsführerin:
Assessorin jur.
Sarah Rachut
sarah.rachut@tum.de

Tel. +49 89 90 77 93 300
www.tum-cdps.de
www.gov.tum.de/elaw

I. Zusammenfassung und Handlungsempfehlungen

1. Es gibt zahlreiche **Erscheinungsformen digitaler Gewalt (insbesondere) gegen Frauen und Mädchen**: sowohl solche, die sich – wie etwa tiefgehende Beleidigungen oder Verleumdungen (sog. Cybermobbing) – weitgehend im Internet abspielen, als auch solche, bei denen Hard- und Software (Smartphones, Miniaufzeichnungsgeräte in Alltagsgegenständen, GPS Tracker etc.) genutzt werden, um unerwünschte Audio-, Bild- oder Videoaufnahmen anzufertigen, mit denen Opfer bloßgestellt werden bzw. ihnen nachgestellt wird. Die Liste lässt sich „dank" technischer Innovationen zunehmend verlängern.

2. Die Rechtsordnung reagiert auf solche Sachverhalte bereits in vielfältiger Weise, insbesondere durch **Straftatbestände** wie die §§ 201, 202a ff., 238 StGB. Deren Abschreckungspotential erscheint angesichts der berichteten Häufigkeit solcher Übergriffe unterdessen gering. Es ist deshalb naheliegend, nach besseren Schutzmechanismen zu suchen.

3. Was hierbei Fälle des Cybermobbings betrifft, könnte ein **Gesetz zur Verbesserung des Persönlichkeitsrechtsschutzes im Internet** (Persönlichkeitsrechtsschutzgesetz – PRG) weiterhelfen. Ein solches haben die Rechtswissenschaftler Prof. Dr. Dirk Heckmann und Dr. Anne Paschke bereits 2018 entworfen und zur Diskussion gestellt. Darin wird die Schaffung eines neuen **Straftatbestandes für erhebliche Persönlichkeitsverletzungen** (in der Qualifikation: mit Todesfolge) – sog. Cybermobbing – vorgeschlagen, verbunden mit **Maßnahmen zum Opferschutz** (die Pflicht zur Verfolgung von Amts wegen, effizientere – auch elektronische – Anzeigemöglichkeiten, das Recht auf einen Prozessbeistand und psychosoziale Prozessbegleitung für Cybermobbingopfer). Darüber hinaus sollen Plattformbetreiber, die mit ihren Diensten ja eine gewisse Gefährdungslage schaffen, ihr technologisches KnowHow für einen besseren Rechtsschutz zur Verfügung stellen, in dem sie ein **System zur Kennzeichnung, Sperrung und Löschung** rechtswidriger Inhalte entwickeln und zur Beweissicherung beitragen.

4. Eine **Änderung der gesetzlichen Pflicht zur Anbieterkennzeichnung** kann verhindern, dass die Impressumspflicht für Diensteanbieter vielfach gerade Frauen zur Veröffentlichung ihrer Privatanschrift zwingt, was sie der Bedrohung etwa durch Stalking aussetzt. In Betracht kommt insbesondere die Zulassung von „Impressumsintermediären", die eine Anschrift nur bei berechtigtem Anlass (etwa zur Geltendmachung rechtlicher Ansprüche) herausgeben müssen.

5. Innovationen im Smart Home oder dem Internet der Dinge können oftmals auch missbraucht werden, sei es zur **unbemerkten Aufzeichnung oder Überwachung, Nachstellung oder Nötigung.** Ein Verbot solcher Produkte ist nur in Ausnahmefällen möglich. In Betracht kommen aber gesetzliche Regelungen, die die Hersteller verpflichten, Produkte so zu gestalten, dass ihre Funktionen für Dritte offensichtlich werden. Dies stärkt die Möglichkeiten eines Eigenschutzes und vermag Täter und Täterinnen zu enttarnen.

II. Allgemeines

Der Ausschuss befasst sich mit einem Themenkomplex, der auch aus meiner Sicht eine besondere parlamentarische Aufmerksamkeit und Befassung verdient. Digitale Gewalt, insbesondere gegenüber Frauen und Mädchen (aber auch allen anderen Menschen), kennt verschiedene Erscheinungsformen, denen auch deshalb weder rechtlich noch tatsächlich ausreichend begegnet wird, weil die Mechanismen der Tatbegehung (anders als in „klassischen" Fällen von Körperverletzung, Nötigung oder Sexualdelikten) nicht jedem Akteur in der Gesetzgebung, bei den Gefahrenabwehrbehörden oder anderen, zuständigen bzw. relevanten Stellen verständlich sind; das Gleiche gilt wiederum für adäquate, IT-bezogene Abwehr-, Schutz- und Hilfemaßnahmen. Die allenthalben an vielen Stellen bemerkbaren Defizite bei den Digitalkompetenzen wirken sich auch insofern aus. Zu Recht adressieren die Fragen in den Ausschuss-Vorlagen aus unterschiedlichen Perspektiven, von den Sozialwissenschaften über die Kriminologie bis hin zu Strafrecht, Strafprozessrecht und IT-Recht. Angesprochen sind neben den genannten wissenschaftlichen Disziplinen auch die Ermittlungspraxis und der gesamte, bereits bestehende Schutzkomplex gegenüber den adressierten Fällen digitaler Gewalt.

Als Sachverständiger kann und möchte ich mich hier nur zu den rechtlichen Fragen äußern und auch nur soweit ich aus meiner Forschung eine hilfreiche Perspektive beisteuern kann. So befasse ich mich seit mittlerweile fast 10 Jahren mit dem Phänomen des Cybermobbings, also der erheblichen Persönlichkeitsrechtsverletzung im Internet. Weil ich insofern bis heute Defizite im rechtlichen Schutz von Opfern sehe, habe ich mit meiner Kollegin, Frau Dr. Anne Paschke, 2018 den wissenschaftlichen Entwurf eines Gesetzes zur Verbesserung des Persönlichkeitsrechtsschutzes im Internet (PRG), verfasst und veröffentlicht. Der Gesetzentwurf ist dieser Stellungnahme als Anhang beigefügt. Er befasst sich zwar nur mit einem Teil der im Ausschuss behandelten Thematik, dies aber wiederum in besonderer Vertiefung. Daneben werden im Folgenden einige Fragen aus dem Fragenkatalog aufgegriffen, die etwas mehr in die Breite der Thematik gehen.

III. Zu einzelnen Fragen

Aufgrund der Komplexität der Thematik und der Kurzfristigkeit der Stellungnahme soll hier nur auf einzelne Fragen eingegangen werden, die in meinem Forschungsschwerpunkt liegen. Dabei fasse ich die Fragen 17 und 23 zusammen und äußere mich anschließend separat zu Frage 24.

1. Verbesserung des Persönlichkeitsrechtsschutzes im Internet: Regelungsdefizite und Handlungsbedarf

Die vielfach als Cybermobbing bezeichnete digitale Gewalt betrifft Persönlichkeitsrechtsverletzungen auch und besonders gegenüber Frauen und Mädchen. Maßnahmen zur Verbesserung des Persönlichkeitsrechtsschutzes im Internet bilden zwar nur einen kleinen, aber doch wichtigen Ausschnitt der staatlichen Reaktionsmöglichkeiten auf Äußerungsformen digitaler Gewalt.

Der im Anhang beigefügte wissenschaftliche Entwurf eines Gesetzes zur Verbesserung des Persönlichkeitsrechtsschutzes (PRG) setzt an drei Stellen an:

- erstens durch Einfügung eines Straftatbestandes der besonders schweren Persönlichkeitsverletzung („Cybermobbing“) im Strafgesetzbuch,
- zweitens durch Regelungen des Opferschutzes (Opferanwalt, psychosoziale Prozessbegleitung) im Strafprozessrecht und
- drittens durch ein System der Kennzeichnung, Sperrung und Löschung von rechtswidrigen, insbesondere persönlichkeitsrechtsverletzenden Inhalten auf Plattformen oder ähnlichen Speicherorten im Internet.

Der gesamte Gesetzentwurf erfasst in den Grenzen seiner intendierten Schutzwirkungen auch Fälle digitaler Gewalt gegen Frauen und Mädchen, richtet sich aber nicht speziell an diese Adressaten.

a) Straftatbestand des „Cybermobbing“

Begehungsformen des sog. Cybermobbing (international: Cyberbullying) sollen durch einen neuen § 190 StGB-E einen eigenen Straftatbestand der schweren Ehrverletzung im Internet erhalten.[1] Die bisherige Strafbarkeit ist so vielfältig wie die unterschiedlichen Erscheinungsformen des Cybermobbings. Für beleidigende Äußerungen ergibt sich eine Strafbarkeit nach den Ehrverletzungsdelikten der §§ 185 ff. StGB, im Einzelfall auch nach § 130 StGB wegen Volksverhetzung[2] oder nach § 140 StGB wegen der Billigung von Straftaten[3]. Andere Arten des Cybermobbings im weiten Sinne wie das Cyberstalking, Sextortion, Bildaufnahmen etc. fallen unter die jeweils einschlägigen allgemeinen Delikte im

[1] Wissenschaftlicher Entwurf eines Gesetzes zur Verbesserung des Persönlichkeitsrechtsschutzes im Internet, hier zitiert als: PRG Heckmann/Paschke, S. 21.
[2] OLG Köln v. 09.06.2020, 1 RVs 77/20, openJur 2020, 6552, Rn. 89, 91.
[3] *Heckmann* in: Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021 (im Erscheinen), Kap. 8, Rn. 435.

Strafrecht. So kommt eine Strafbarkeit wegen Nötigung[4] (§ 240 StGB), Bedrohung[5] (§ 241 StGB), Erpressung (§ 253 StGB), Nachstellung/„Stalking"[6] (§ 238 StGB), aber auch wegen der Herstellung und Zugänglichmachung von Bildaufnahmen im höchstpersönlichen Lebensbereich (§ 201a StGB), Upskirting[7] (§184k StGB) oder anderen Straftatbeständen in Betracht. Die Bestrafung der unterschiedlichen Varianten des Cybermobbings ist nach dem materiellen Strafrecht also in vielen Fällen möglich.

Aktuelle Bestrebungen zu Gesetzesänderungen und Anpassungen wie beim Upskirting (§ 184k StGB), dem Cyberstalking[8] (§ 238 StGB), der erhöhten Strafbarkeit der Beleidigung (§ 185 StGB) durch Verbreiten von Inhalten (§ 11 Abs. 3 StGB)[9], der Versuchsstrafbarkeit des Cybergroomings[10] (§ 176 Abs. 4 Nr. 3 StGB) oder der Modernisierung des Schriftenbegriffs in § 11 Abs. 3 StGB zu einem Inhaltebegriff sind grundsätzlich zu begrüßen. Sie zeigen, dass die punktuellen Regelungen weiter an den Fortschritt der Digitalisierung und damit zusammenhängendes Verhalten in der Gesellschaft angepasst werden müssen, um konsequent Strafbarkeitslücken zu schließen und der Heterogenität der möglichen Delikte gerecht zu werden. Sie zeigen aber auch die mosaikartige Regelung der einzelnen Erscheinungsformen von Cybermobbing, die jeweils für sich genommen zwar eine Strafbarkeit begründen können, aber nicht dem Gesamtunrechtsgehalt der digitalen Gewalt gerecht werden. Ein eigener Straftatbestand lenkt die Aufmerksamkeit auf dieses Phänomen, wirkt einer (nicht angemessenen) Bagatellisierung solcher Grenzüberschreitungen entgegen und hat überdies Vorteile im System des Strafrechts und Strafprozessrechts, weil dadurch eine bessere Verweisung in der Strafprozessordnung gelingt, die sich im Hinblick auf besondere Verfahrensvorschriften an Deliktsgruppen oder bestimmten Straftatbeständen orientiert. Dies wäre nicht möglich, wenn man das Cybermobbing als bloße Anwendung des § 185 StGB begreift.

Gleichwohl ist für die effektive Strafverfolgungspraxis nicht nur die Möglichkeit der Strafbarkeit nach materiellem Recht erforderlich, sondern es kommen weitere Faktoren hinzu, die fachübergreifend in einem Gesamtkonzept berücksichtigt werden müssen. Die Sensibilisierung und Umsetzung in der Praxis erfordert eine Lösung, die für eine rechtspolitische Klarstellung sorgt, den Unrechtsgehalt des Cybermobbings in seiner Gesamtheit erfasst und ergänzende Regelungen aus Strafprozess- und Zivilrecht setzt, um dem Opferschutz gerecht zu werden. Hier setzt der Gesetzesentwurf für ein Gesetz zur Verbesserung des Persönlichkeitsrechtschutzes im Internet (Persönlichkeitsrechtsschutzgesetz – PRG)

---

[4] *Heckmann* in: Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021 (im Erscheinen), Kap. 8, Rn. 427.
[5] PRG Heckmann/Paschke, S. 21.
[6] *Heckmann* in: Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021 (im Erscheinen), Kap. 8, Rn. 421.
[7] Ziegler in: BeckOK StGB, § 184k Rn. 4.
[8] Entwurf vom 24.03.2021: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_Cyberstalking.pdf;jsessionid=476E482F2DC54D128D112D010F1E6632.1_cid334?__blob=publicationFile&v=3 (abgerufen am 24.03.2021).
[9] BT-Drs. 19/17741, S. 3, 7, 18.
[10] BGBl I S. 431.

mit der Entwicklung eines Cybermobbing-Straftatbestandes nach § 190 StGB-E an, der neben den bereits vorhandenen Teilregelungen ergänzend normiert werden soll.[11]

Der Straftatbestand des § 190 StGB-E stellt eine ehrverletzende Tat nach den Beleidigungsdelikten der §§ 185 ff. StGB[12] unter Strafe, wenn sie dergestalt im Internet zugänglich gemacht wird, dass der gegenständliche Inhalt von einer erheblichen Anzahl von Personen wahrgenommen werden kann und geeignet ist, das Opfer in seiner Lebensgestaltung schwerwiegend zu beeinträchtigen. Dies soll für eine Angleichung mit dem Tatbestand der Nachstellung nach § 238 StGB und so auch für eine qualitative Abhebung von den §§ 185 ff. StGB sorgen, die im Unrechtsgehalt unter Berücksichtigung der erheblichen Folgen für die Opfer mit Fällen des Cybermobbing nicht vergleichbar sind.[13] Dadurch bleibt eine Differenzierung zu solchen Fällen möglich, die in § 190 StGB-E einer großen Zahl an Personen zugänglich gemacht wird und schwerwiegende Folgen hat oder in der Tatbestandsvariante nach § 190 Abs. 2 StGB-E sogar zum Tod führt, wobei auch die Kompatibilität mit aktuellen Gesetzgebungsvorhaben gewahrt ist.

Sollte § 185 StGB wie im Gesetzesentwurf gegen Hasskriminalität vorgesehen, an die §§ 186 ff. StGB angepasst werden, indem das Strafmaß für die Begehung durch Verbreitung eines Inhaltes erhöht wird[14], so bliebe die weitergehende und spezifischere Qualifikation nach § 190 StGB-E für einschlägige Fälle der schweren Ehrverletzung im Internet davon unberührt erhalten. Eine Qualifikation des § 190 StGB-E wird nach dessen Abs. 2 verwirklicht, wenn dadurch leichtfertig der Tod der Person verursacht wird.[15]Denkbar ist auch eine abstufende Erfolgsqualifikation im Sinne des § 226 StGB aufzunehmen, die das Strafmaß anpasst, wenn durch die Tat typische Folgeerkrankungen wie Angststörungen, Depressionen o.ä. ausgelöst werden.

Ergänzend wird § 194 StGB dahingehend angepasst, dass ein Strafantragserfordernis für Opfer einer Tat nach § 190 StGB-E nicht erforderlich ist.[16] Die einschlägigen Delikte der §§ 185 ff. StGB sind Antragsdelikte, deren Verfolgung nur auf förmlichen Strafantrag erfolgt, sodass viele Opfer, sei es aus Scham, wegen des Aufwandes oder des fehlenden Bewusstseins für die Schwere der Tat oder der verpassten Antragsfrist (§ 77b StGB) einen solchen Strafantrag oftmals nicht in Betracht ziehen.[17] Dazu soll § 158 StPO dergestalt angepasst werden, dass Strafanträge und Strafanzeigen auch auf elektronischem Wege möglich sein sollen, um etwaige Hemmnisse weiter zu vermeiden (falls ein Antrag noch erforderlich ist).[18] Beispielhaft ist hier auch an eine Erweiterung der Onlinewachen zu

[11] *Heckmann* in: Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021 (im Erscheinen), Kap. 8, Rn. 397.
[12] PRG Heckmann/Paschke, S. 23.
[13] PRG Heckmann/Paschke, S. 7.
[14] BT-Drs. 19/17741.
[15] PRG Heckmann/Paschke, S. 7.
[16] PRG Heckmann/Paschke, S. 7.
[17] PRG Heckmann/Paschke, S. 26.
[18] PRG Heckmann/Paschke, S. 7.

denken, die bisher je nach Bundesland nur einige wenige Delikte zur Online-Anzeige zulassen.[19]

Mit einer dedizierten Regelung des Cybermobbings wäre Deutschland nicht allein. Dies ist in einigen anderen Ländern bereits umgesetzt.[20] So hat z.B. Österreich schon seit 01.01.2016 trotz der bestehenden Delikte der Beleidigung u.a. einen eigenständigen Cybermobbing-Straftatbestand in § 107c StGB[21]; auch in den USA haben viele Staaten eigene „Cyberbullying-Laws".[22]

b) Erweiterung des Opferschutzes

Neben der Änderung des materiellen Strafrechts und der Regelungen zum Strafantrag ist für eine effektive Rechtsverfolgung und konsequente Durchsetzung unter Mithilfe der Opfer auch die Erweiterung des Opferschutzes notwendig. Die kaum vorhandenen Strafurteile und Verfahren zu diesem Thema bei gleichbleibend hohen Zahlen empirisch erhobener Häufigkeit solcher Verletzungen[23] rühren neben den formalen Hemmnissen auch von der Belastung, die mit einem potentiellen Verfahren einhergehen. Im Jahr 2020 offenbarte eine Studie des Kinderhilfswerks Plan International, dass insbesondere Frauen und Mädchen häufig durch digitale Gewalt betroffen sind. Rund 70 Prozent der Befragten aus Deutschland gaben an, im Netz Bedrohungen, Beleidigungen und Diskriminierungen erlitten zu haben, z.B. durch Beleidigungen, Body Shaming, sexuelle Belästigungen, Bedrohungen oder anderen Ausdrucksformen, die häufig in den großen sozialen Medien wie Facebook, Instagram, Youtube, Snapchat und TikTok auftreten.[24] Spezifisch bei den befragten Mädchen gaben 58 Prozent an, schon Belästigungen erlebt zu haben. Hieraus folgen auch psychische und physische Folgen in Form von körperlich spürbarer Angst (23 %), Stress (32 %) oder einer Herabsetzung des Selbstwertgefühls (30 %)[25], die es für die Opfer nur umso schwerer machen, gegen solche Inhalte vorzugehen und ein kräftezehrendes Verfahren durchzustehen. Dabei bietet sich bei diesen Formen der (geschlechterspezifischen) digitalen Gewalt besonders im Hinblick auf Frauen und Mädchen ein Vergleich zum Sexualstrafrecht an, bei dem viele Opfer die persönlichen Folgen eines

---

[19] So z.B. für Bayern: https://online-strafanzeige.de/bayern (abgerufen am 22.03.2021).
[20] *Jülicher*: Cybermobbing in der Schule, NJW 2019, 2801.
[21] *Jülicher*: Cybermobbing in der Schule, NJW 2019, 2801.
[22] so u.a. Kalifornien, Florida, Missouri, https://www.findlaw.com/criminal/criminal-charges/cyber-bullying.html (abgerufen am 22.03.2021); Übersicht der Staaten: https://cyberbullying.org/bullying-laws (abgerufen am 22.03.2021).
[23] Vgl. etwa die Studie des Bündnisses gegen Cybermobbing – Cyberlife III, abrufbar unter: https://www.tk.de/resource/blob/2095298/e576a0e34a8731c50c60d9edbb661ca7/studie-cybermobbing-2020-data.pdf.
[24] Zum Weltmädchenbericht 2020: https://www.sueddeutsche.de/medien/studie-digitale-gewalt-vertreibt-maedchen-aus-sozialen-medien-1.5055546 (abgerufen am 22.03.2021); https://www.vorwaerts.de/artikel/digitale-gewalt-gegen-frauen-uns-alle-angeht (abgerufen am 22.03.2021); https://www.plan.de/presse/pressemitteilungen/detail/welt-maedchenbericht-2020-digitale-gewalt-vertreibt-maedchen-und-junge-frauen-aus-den-sozialen-medien.html (abgerufen am 22.03.2021).
[25] Weltmedienbericht 2020: https://www.plan.de/presse/pressemitteilungen/detail/welt-maedchenbericht-2020-digitale-gewalt-vertreibt-maedchen-und-junge-frauen-aus-den-sozialen-medien.html (abgerufen am 22.03.2021).

Prozesses scheuen und so zumindest Gegenmaßnahmen getroffen werden müssen.[26] Auch hier setzt das PRG an und bietet den Opfern stärkeren rechtlichen und psychologischen Schutz.[27] Dabei soll § 395 StPO dahingehend abgeändert werden, dass Opfer von Cybermobbing als Nebenkläger auftreten können, bei ihrem Tod durch Suizid (§ 190 Abs. 2 StGB-E) die Kinder, Eltern, Geschwister oder Ehepartner/Lebenspartner.[28] Flankierend soll eine Ergänzung von § 397a Abs. 1 Nr. 5 StPO die Entlastung der Nebenkläger durch die Möglichkeit der Bestellung eines Prozessbeistandes festsetzen, wobei auch die Möglichkeit einer psychosozialen Prozessbegleitung für Minderjährige nach § 406g Abs. 3 S. 1 StPO eröffnet wird, um das Opfer bei der Durchführung des seelisch belastenden Strafverfahrens kompetent und einfühlsam begleiten zu können.[29]

c) Kennzeichnung, Sperrung und Löschung rechtswidriger Inhalte

Das PRG sieht nicht nur strafrechtliche, sondern auch zivilrechtliche Anpassungen und Alternativlösungen zum NetzDG vor. Dieses wird neben verfassungs- und europarechtlichen Bedenken in weiten Teilen der Literatur[30] in Bezug auf das Cybermobbing auch als unzureichend angesehen[31], da es keine wesentliche Verbesserung des Persönlichkeitsrechtschutzes mit sich bringt, die Täter und Täterinnen weitgehend schont[32] und dem Dilemma potentiell rechtswidrig weiterbestehender Inhalte im Netz bei Abwägung der ebenfalls zu schützenden Meinungsfreiheit nicht gerecht wird.[33] Die Regelungen begünstigen Overblocking[34], da die Plattformbetreiber im Zweifel eher zu viel als zu wenig löschen, um möglichen Sanktionen zu entgehen. Dabei übernehmen die Plattformen „quasirichterliche“ Aufgaben, indem sie die Rechtswidrigkeit der Inhalte beurteilen, wohingegen die technischen Möglichkeiten nicht ausgeschöpft werden.[35]

Bei Aufhebung des NetzDG sollten dennoch in anderer Form Pflichten zur Kennzeichnung, Sperrung und Löschung von rechtswidrigen Inhalten geregelt werden. Durch Neuregelung eines § 13c TMG-E soll ausdrücklich ein Auskunftsanspruch gegen die Diensteanbieter sozialer Telemedien nach § 13a TMG-E festgesetzt werden, um gegen die oft pseudonymisierten Täter und Täterinnen auch zivilrechtlich vorgehen zu können. Bisher war regelmäßig unklar, ob sich der Auskunftsanspruch seit den Neuregelungen des NetzDG weiter aus § 242 BGB oder ggfs. auch aus § 14 Abs. 3 TMG direkt ergibt. Dieser regelt

[26] *Heckmann/Paschke*, DRiZ 2018, 144, 147.
[27] PRG Heckmann/Paschke, S. 28.
[28] PRG Heckmann/Paschke, S. 7.
[29] PRG Heckmann/Paschke, S. 28.
[30] Stellungnahme der Deutschen Gesellschaft für Recht und Informatik DGRI e.V. https://www.dgri.de/index.php/fuseaction/download/lrn_file/dgri-stellungnahme-netzdg.pdf (abgerufen am 22.03.2021); *Gersdorf*, Hate Speech in sozialen netzwerken, MMR 2017, 439; *Hoven/Gersdorf* in: BeckOK Informations- und Medienrecht, § 1 NetzDG Rn. 5ff, 9ff; *Liesching* in: Spindler/Schmitz, Telemediengesetz, § 1 NetzDG Rn. 21; *Liesching* in: Hamburger Kommentar Gesamtes Medienrecht, § 1 NetzDG, Rn. 3, 5.
[31] *Heckmann* in: Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021 (im Erscheinen), Kap. 8, Rn. 396.; *Heckmann/Paschke*, DRiZ 2018, 144.
[32] PRG Heckmann/Paschke, S. 2.
[33] *Heckmann* in: Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021 (im Erscheinen), Kap. 8, Rn. 396.
[34] *Heckmann/Paschke*, DRiZ 2018, 144, 145.
[35] PRG Heckmann/Paschke, S. 2.

ausdrücklich nur eine datenschutzrechtliche Erlaubnis zur Erteilung der Bestandsdaten.[36] Mit der Neuregelung soll ausdrücklich eine Rechtsgrundlage für die Auskunftserteilung geschaffen werden[37], sodass nicht mehr auf § 242 BGB zurückgegriffen werden muss und Rechtssicherheit geschaffen wird. Daneben sieht auch das PRG die Benennung von inländischen Zustellungsbevollmächtigten als Pflicht nach § 13d TMG-E vor, um Ermittlungs- und Gerichtsverfahren zu beschleunigen.[38] Die Neuregelung des Auskunftsanspruchs ist auch mit Art. 15 Abs. 2 E-Commerce-RL vereinbar, der eine Verpflichtung zur Herausgabe von Daten zur Ermittlung der Nutzer an die Behörden ermöglicht, wobei Auskunftspflichten in § 13c TMG-E und Bestandsdaten nach § 14 Abs. 3 TMG-E erfasst werden.

Abweichend von den Regelungen des NetzDG soll in § 13b TMG-E eine Meldefunktion für rechtswidrige bzw. verdächtigte Inhalte geschaffen werden. Danach müssen Diensteanbieter sozialer Telemedien geeignete technische Maßnahmen zur Meldung persönlichkeitsrechtsverletzender Inhalte vorhalten, so z.B. durch die Bereitstellung einer Meldeschaltfläche. Dabei sind die Diensteanbieter nach § 13b Abs. 2 TMG-E dazu verpflichtet, solche persönlichkeitsrechtsverletzenden Inhalte nach einer Meldung deutlich sichtbar zu kennzeichnen und eine Dokumentation des Posts und der Verbreitung zu erstellen. Der Inhalt ist zusätzlich mit dem Warnhinweis zu versehen, dass eine solche Dokumentation erfolgt und die Weiterverbreitung des Inhalts rechtliche Konsequenzen nach sich ziehen kann. Der Verfasser des Inhalts erhält währenddessen eine Frist von einer Woche zur Abgabe einer Stellungnahme gegenüber dem Diensteanbieter. Um ein übermäßiges oder ungerechtfertigtes Markieren von Inhalten zu vermeiden, sind die Kennzeichnungen unverzüglich zu entfernen, wenn sich die Meldung als offensichtlich unberechtigt erweist, die Meldung zurückgenommen wird oder ein Gericht die Rechtmäßigkeit feststellt.[39] Die letztliche Löschung nach gerichtlichem Beschluss stellt sicher, dass nur die Gerichte konsequent über die Einschätzung der Tatbestandsverwirklichung der Straftatdelikte entscheiden und die sozialen Netzwerke keine quasi-richterlichen Funktionen übernehmen.[40] Gleichzeitig tragen die Plattformbetreiber und Provider mit ihrer Technologiekompetenz zu einem gesamtheitlichen Ansatz des Persönlichkeitsrechtsschutzes bei. Denn sie müssen die technischen Voraussetzungen und das Gerüst bereitstellen[41], das eine rechtliche Durchsetzung für die Gerichte und Staatsanwaltschaften ermöglicht, sie sollen die Verstöße aber nicht selbst durchsetzen. Zur weiteren Unterstützung bei der Durchführung und Strafverfolgung dienen die Dokumentationspflichten, sodass das Gesamtkonzept auch an die Digitalisierung der Rechtspflege (E-Justice) anschlussfähig ist.[42] Die Rechtfertigung dieser Pflichten folgt auch aus dem Gesichtspunkt der Ingerenz. Mit der Schaffung und Bereitstellung sozialer Medien, die darauf ausgerichtet sind, dass die

[36] *Schmitz* in: Spindler/Schmitz, Telemediengesetz, § 14 TMG Rn. 51, 52.
[37] PRG Heckmann/Paschke, S. 32f.
[38] PRG Heckmann/Paschke, S. 34.
[39] *Heckmann/Paschke*, DRiZ 2018, 144, 148.
[40] *Heckmann* in: Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021 (im Erscheinen), Kap. 8, Rn. 399.
[41] *Heckmann/Paschke*, DRiZ 2018, 144, 148.
[42] *Heckmann/Paschke*, DRiZ 2018, 144, 148.

Nutzer untereinander unabhängig kommunizieren und interagieren können, entstehen auch Pflichten zum aktiven Vorgehen gegen rechtswidrige Inhalte entsprechend den Grundsätzen des Urheberrechts zur Störerhaftung bei Sharehostern, wenn Plattformen den illegalen Austausch urheberrechtlich geschützter Werke fördern.[43] Diese Lösung ist auch mit Art. 14 Abs. 3 E-Commerce-RL vereinbar, da die Richtlinie die Möglichkeit gibt, dass Gerichte von Diensteanbietern das Abstellen oder Verhindern der Rechteverletzung verlangen oder Verfahren dafür regeln. Es werden gerade keine eigenen rechtlichen Entscheidungen von den Diensteanbietern gefordert, sondern eben solche technischen Verfahren, wie sie von Art. 14 Abs. 3 E-Commerce-RL erfasst sind. [44] Alternativ zum NetzDG soll hierbei auf starre Fristen verzichtet werden, die in Art. 13 Abs. 1 lit. b) E-Commerce-RL nicht vorgesehen sind. [45] Im Ergebnis können mit diesem alternativen Lösungsansatz die europa- und verfassungsrechtlichen Probleme des NetzDG umgangen werden, sodass sich die Frage der Unionsrechtskonformität nicht weiter stellt.

2. Exkurs: Alternativen zur Anbieterkennzeichnung für Telemediendienste

Nach § 5 Abs. 1 Nr. 1 TMG haben Diensteanbieter für geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien den Namen und die Anschrift, unter der sie niedergelassen sind, leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten. Das bedeutet, dass zum Beispiel Frauen, die einen Online-Shop, eine Internetdienstleistung oder auch einen Blog anbieten, ihre „Geschäftsadresse“ auf der entsprechenden Internetseite veröffentlichen müssen – eine Adresse, die nicht selten mit ihrer privaten Wohnanschrift identisch ist. Durch diesen Umstand sind sie allerdings möglicherweise Angriffen von Stalkern ausgesetzt. Dies gilt insbesondere mit Blick darauf, dass die Grenze rein privater Seiten und dem Erfordernis einer Impressumspflicht schnell überschritten sein kann.[46] Eine gegen Entgelt angebotene Seite im Sinne des § 5 TMG ist regelmäßig schon dann anzunehmen, wenn Privatpersonen Blogs betreiben, auf denen Werbung geschaltet wird oder Affiliate-Links gesetzt werden, die zur Monetarisierung einzelner Inhalte führen.[47] Eine private Blogbetreiberin, die z.B. einen Finanzblog veröffentlicht und für einen kleinen Nebenverdienst Affiliate-Links zu rezensierten Büchern oder benutzten Applikationen setzt, die sie selbst genutzt hat, könnte nach diesen Grundsätzen bereits der Impressumspflicht unterliegen.

Hier besteht offenbar ein Interessenkonflikt: Die Angabe der Adressdaten im Rahmen der Anbieterkennzeichnung soll berechtigte Interessen des Rechts- und Geschäftsverkehrs schützen, nicht zuletzt durch die leichte Zugänglichkeit der ladungsfähigen Anschrift.

---

[43] *Heckmann/Paschke*, DRiZ 2018, 144, 148; vgl. dazu *Heckmann* in: Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021 (im Erscheinen), Kap. 3, Rn. 171 ff.
[44] PRG Heckmann/Paschke, S. 16.
[45] PRG Heckmann/Paschke, S. 16.
[46] *Micklitz/Schirmbacher* in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, § 5 TMG, Rn. 15.
[47] Spindler/Schmitz/Spindler, 2. Aufl. 2018, TMG § 5 Rn. 12.

Umgekehrt zwingt diese (gesetzlich angeordnete) Publizität zur Veröffentlichung sensibler personenbezogener Informationen. Dies mag wegen der gesetzlichen Grundlage der sog. Impressumspflicht datenschutzrechtlich gerechtfertigt sein. Im Sinne eines Schutzes von Frauen gegenüber Übergriffen durch Stalking ist diese Form der Anbieterkennzeichnung allerdings kritisch zu hinterfragen. So stellt sich insbesondere die Frage, ob man dem Schutzinteresse von potentiellen Klägern oder Verwaltungsbehörden (etwa der Gewerbeaufsicht) auch ohne Preisgabe der (persönlichen) Wohnanschrift gerecht werden kann.

Dabei kommen mehrere Möglichkeiten in Betracht, um eine Impressumspflicht für bestimmte Personengruppen so zu regulieren, dass sie besser geschützt werden. Zunächst könnte die gesetzliche Regelung in § 5 TMG so angepasst werden, dass private Blog- oder Webseitenbetreiber ausdrücklich nicht mehr erfasst sind, selbst wenn sie in geringem Umfang durch Werbung oder Affiliate-Links Einnahmen generieren. Hierdurch würde aber das Interesse potentieller Kläger oder Verwaltungsbehörden nicht ausreichend gewürdigt, das ab dem Zeitpunkt besteht, in dem Werbe-, Kooperations- oder andere Verträge geschlossen werden und Einnahmen generiert werden.

Die Zwischenschaltung von Agenturen oder Netzwerken als offizielle Betreiber der Seite kann für erfolgreiche Betreiber eine Lösung sein, gerade schützenswerte Kleinstbetreiber können auf solche Möglichkeiten im Regelfall jedoch nicht zurückgreifen. Gleiches gilt für die Gründung und das Betreiben von eigenen Unternehmen mit (von der Privatadresse) abweichender Geschäftsadresse.

In Betracht kommt eine Regelung durch Intermediäre, die sich für private Kleinbetreiber zwischenschalten können. Die richtigen Adress- und Kontaktdaten der Privatpersonen werden sicher bei Impressumsintermediären hinterlegt und verwaltet. Beim Auftreten von Rechtsproblemen kann sich der Betroffene sodann an den Intermediär wenden, der die Daten bei einem berechtigten Interesse herausgeben muss. So bleibt die Pflicht zur Angabe der Daten erhalten, gleichzeitig werden die veröffentlichten Daten aber minimiert und solange pseudonymisiert, bis ein berechtigtes Interesse zur Herausgabe an den einzelnen Interessenten geltend gemacht wird. Selbst wenn die Anforderungen an die Geltendmachung eines berechtigten Interesses minimal gehalten werden oder eine Auskunft immer gegeben werden muss, werden schon Risiken dadurch minimiert, dass die Adressdaten nicht mehr frei einsehbar auf der Website und über Suchmaschinen zu finden sind und ggfs. ein gewisses Hemmnis für potentielle Täter besteht. Dass ein Bedürfnis für solche Intermediäre besteht, zeigt beispielhaft eine Anwaltskanzlei, die für Kleinstbetreiber als Zustellungsbevollmächtigter agiert, damit diese ihre Adressdaten nicht preisgeben müssen.[48] Hier bietet sich eine zentrale Regulierung der Möglichkeiten und Angebote für Kleinstbetreiber an.

[48] https://matutis.com (abgerufen am 22.03.2021).

3. Verbot schwer erkennbarer Hard- und Software zu Überwachungs-, Aufzeichnungs- und Verfolgungszwecken in Haushaltsgeräten oder Smartphones

Technische Innovationen, die Entwicklung von Smart Home, dem Internet der Dinge und eine zunehmende Miniaturisierung von IT-Komponenten bilden die Ausgangslage für ein neues Überwachungspotential, das sich vielfach auch als digitale Gewalt gegen schutzbedürftige Menschen äußern kann. Die Rede ist von Video-, Audio- und Bewegungsaufzeichnungen, die durch sehr kleine, weitgehend unmerkliche IT-Komponenten in solchen Geräten ermöglicht werden, bei denen man diese Funktionen entweder gar nicht vermutet (wie etwa Kameralinsen in Haushaltsgegenständen) oder deren aktiver Betrieb unmerklich ferngesteuert werden kann (etwa eine Tracking-Funktion im Smartphone des Ehepartners). Obwohl der bewusste und zielgerichtete Einsatz solcher Komponenten bereits jetzt strafbar ist (zum Beispiel durch §§ 201, 201a StGB), sind die Opfer diesem Gebaren oft schutzlos ausgeliefert, weil dieses strafbare Verhalten sich eben im Geheimen abspielt. Selbst wenn die Hersteller der inkriminierten Hard- oder Software diese Einsatzszenarien nicht intendiert haben mögen, nehmen sie doch billigend einen solchen Missbrauch in Kauf. Fraglich ist, wie man dem rechtlich begegnen kann. In Betracht käme ein vollständiges Verbot der Herstellung und des Vertriebs solcher Komponenten, aber auch – als milderes Mittel – die Verpflichtung zur ausdrücklichen Kennzeichnung, Kenntlichmachung oder anderer Maßnahmen, die einen unmerklichen Einsatz verhindern, um das Opfer quasi zu warnen.

Die Strafbarkeit hängt maßgeblich von den eingesetzten Mitteln ab. So ist zwischen dem Einsatz von Video-, Foto- und Audioaufnahmegeräten in haushaltsüblichen Geräten („smart voyeur home“), dem Verstecken von Video- und Aufnahmegeräten in Alltagsgegenständen und dem Einsatz von Software oder Apps, die z.B. heimlich auf Mobiltelefonen installiert werden („Stalkerware“), zu differenzieren.

a) Stalking-Hardware und smart-voyeur-home Geräte

aa) Benutzung von Stalking-Hardware und smart-voyeur-Geräten

So können in der Wohnung des Opfers beispielsweise Abhörwanzen und kleine Kameralinsen bzw. Videokameras in Alltagsgegenständen versteckt werden oder „Smart Voyeur Home“-Geräte platziert oder geschenkt werden, die mit solchen Funktionen ausgestattet sind und Video- und Tonmaterial aufzeichnen können wie z.B. in Kugelschreibern oder Puppen.[49] Für den Einsatz damit aufgezeichneter heimlicher Ton- und Bildaufnahmen bietet zunächst das Strafrecht Instrumente mit den §§ 201ff. StGB. Für das heimliche Aufnehmen des gesprochenen Wortes gilt der Tatbestand des § 201 Abs. 1 Nr. 1 StGB, für das bloße Abhören mit einem Abhörgerät den des § 201 Abs. 2 S. 1 Nr. 1 StGB. Abhörgeräte sind dabei technische (Hardware)-Vorrichtungen, die das gesprochene Wort über den normalen Klangbereich durch Verstärkung wahrnehmbar machen, so z.B. drahtlose

[49] https://www.zeit.de/digital/datenschutz/2017-02/my-friend-cayla-puppe-spion-bundesnetzagentur (abgerufen am 23.03.2021); *Hermmann*/*Heilmann* in: BeckOK IT-Recht, 1. Edition, § 90 TKG Rn. 2.

Kleinsender („Minispione“), Webcams mit Tonaufzeichnungen oder kleine Mikrofone.[50] Noch belastender sind für die Opfer voyeuristische Bild- und Videoaufnahmen, die sie in intimen Situationen zeigen. Diese stellen eine besondere Form der sexualisierten bzw. geschlechterspezifischen Gewalt dar. Dabei folgt die Strafbarkeit von heimlichen Bild- oder Videoaufnahmen in der Wohnung oder einem geschützten Raum aus § 201a Abs. 1 Nr. 1 StGB, bei Mädchen unter 18 Jahren, soweit sie nackt gezeigt werden, nach § 201 Abs. 3 Nr. 1 StGB.

> Für die ggfs. erfolgende Verbreitung kann flankierend eine Strafbarkeit nach §§ 33 Abs. 1 KUG in Betracht kommen, wenn die Bildnisse ohne Einwilligung des Abgebildeten (§ 22 KUG) verbreitet oder öffentlich zur Schau gestellt werden, ohne dass ein Ausnahmetatbestand nach § 23 KUG vorliegt.[51] Sollten die Aufnahmen, die durch die Integration in solche Geräte ermöglicht werden, zu Aufnahmen von Genitalien, der weiblichen Brust oder der bedeckenden Unterwäsche führen, kommt eine Strafbarkeit nach § 184k Abs. 1 Nr. 1 StGB in Betracht, wenn diese Bereiche gesondert gegen Anblick geschützt sind. Dabei muss für einen außenstehenden Dritten erkennbar sein, dass das Opfer sie gegen Anblick schützen will, so dass z.B. Aufnahmen auf dem Strand im Bikini oder Badehose nicht erfasst sind.[52] Dies kann in der Wohnung bezweifelt werden, da das Opfer hier erkennbar nicht davon ausgeht, aufgenommen zu werden und sich so ein gesondert geschützter Anblick nach außen hin nicht manifestiert. Insofern verbleibt es bei § 201a StGB.

bb) Rechtliche Einordnung eines möglichen Verbots

Die Rechtsgrundlage für ein mögliches Verbot durch die Bundesnetzagentur ergibt sich zunächst aus § 90 TKG. Nach § 90 Abs. 1 TKG ist es verboten, Sendeanlagen oder sonstige Telekommunikationsanlagen zu besitzen, herzustellen, etc., die ihrer Form nach einen anderen Gegenstand vortäuschen oder die mit Gegenständen des täglichen Gebrauchs verkleidet sind, auf Grund dieser Umstände oder auf Grund ihrer Funktionsweise in besonderer Weise geeignet und dazu bestimmt sind, das nicht öffentlich gesprochene Wort eines anderen von diesem unbemerkt abzuhören oder das Bild eines anderen von diesem unbemerkt aufzunehmen. Im Jahr 2017 forderte die Bundesnetzagentur beispielsweise Verkaufsstellen zur Rücknahme einer Spielzeugpuppe „My Friend Carla“ auf. Die Puppe ist als „Smart Toy“ ausgestaltet, kann sich mit dem Internet verbinden, hat Bluetooth und Lautsprecher und die Kinder können ihr Fragen stellen, die die Puppe beantworten kann. Die Puppe leuchtet sodann – ähnlich wie bei Alexa – wenn sie mit dem Internet verbunden ist oder zuhört.[53] Dabei wurde aber festgestellt, dass auch ohne das Leuchten auf das Mikrofon zugegriffen werden kann und es für Dritte nicht mehr ohne weiteres erkennbar war, ob hier eine Sendeanlage vorliegt, da nach außen hin der Eindruck eines normalen Spielzeuges erweckt wurde.[54] In Betracht kommt z.B. auch das Versteck in Kugelschreibern

---

[50] *Eisele* in: Schönke/Schröder/Eisele, Strafgesetzbuch, § 201 StGB Rn. 19.
[51] *Heckmann/Paschke*, DRiZ 2018, 144, 148; vgl. dazu *Heckmann* in: Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021 (im Erscheinen), Kap. 3, Rn. 329f..
[52] Ziegler in: BeckOK StGB § 184 Rn. 4.
[53] https://www.zeit.de/digital/datenschutz/2017-02/my-friend-cayla-puppe-spion-bundesnetzagentur (abgerufen am 23.03.2021).
[54] https://www.zeit.de/digital/datenschutz/2017-02/my-friend-cayla-puppe-spion-bundesnetzagentur (abgerufen am 23.03.2021).

oder anderen alltäglichen Gegenständen.[55] Ein ähnliches Verbot sprach die Bundesnetzagentur für Kinderuhren mit Abhörfunktion aus.[56] § 90 TKG ist aber nur dann anwendbar, wenn die Gegenstände (zur Tarnung) in die Alltagsgegenstände eingebaut sind und nicht einfach nur in diesen versteckt sind wie bei kleinen Kameras oder Wanzen.[57] Für bestimmte Hardwareanlagen besteht also grundsätzlich schon die rechtliche Möglichkeit eines Verbots im Einzelfall, wenn die missbräuchlichen Funktionen entdeckt werden. Sanktionsmöglichkeiten bieten sich gegenüber den Herstellern z.B. auch nach Art. 8, 25, 5, 6 i.V.m. 83 Abs. 4a DSGVO an, wenn nachgewiesen werden kann, dass das Unternehmen selbst Daten erhebt.

Fraglich ist, ob es hier eines grundsätzlichen Verbots bedarf. Dabei ist zu berücksichtigen, dass viele der Funktionen solcher Gegenstände gerade gewünscht sind und diese auszeichnen. So wurde die oben beschriebene „smart-toy"-Puppe regelmäßig auch gerade deshalb gekauft, weil sie dem Kind auf Fragen antworten konnte, gleichzeitig mit dem Internet verbunden war und über Bluetooth Musik abspielen konnte. Insoweit erscheint es problematisch, der technologischen und gesellschaftlichen Entwicklung durch umfassende Verbote auf Entwicklungsebene zu begegnen, um die Risiken des Fortschritts einzudämmen. Aufgabe des Rechts ist es aber diesen Fortschritt zu begleiten und zu regulieren, um eine missbräuchliche Verwendung auszuschließen und gerade nicht, ihn gänzlich verhindern. So kann dem Problem, dass die missbräuchliche Verwendung oder Ausgestaltung eines Produktes aber häufig nicht erkannt wird und es so nicht zu Verboten im Einzelfall kommen kann, aber dadurch begegnet werden, dass verpflichtende Warnhinweise eingeführt werden, die jederzeit sicherstellen, dass dem Benutzer des Gegenstandes klar ist, ob und an wen gerade Daten ausgetauscht werden oder Ton/Video aufgezeichnet wird und ob er damit einverstanden ist. Gleichzeitig müssen solche Produkte ausdrücklich gekennzeichnet und kenntlich gemacht werden, sowohl vorab, als auch im konkreten Einsatz und im Fall der Datenübermittlung.

b) Stalking-Software und Apps – „StalkerWare"

aa) Rechtliche Konsequenzen der Benutzung von Stalkerware

Davon zu unterscheiden ist die rechtliche Beurteilung der Herstellung und des Einsatzes von „Stalkerware". Das ist Software die „Personen direkt zur Verfügung gestellt wird und Remote-Benutzer in die Lage versetzt, die Aktivitäten des Geräts eines anderen Benutzers ohne Einwilligung dieses Benutzers und ohne ausdrückliche, stete Benachrichtigung dieser Benutzer zu manipulieren, um beabsichtigt oder unbeabsichtigt, intime Überwachung, Belästigung, Missbrauch, Stalking und/oder Gewalt zu erleichtern"[58]. Damit können also z.B. Personen die Bewegungsdaten und Nachrichten ihres Partners oder ihre Partnerin tracken und sie verfolgen. Diese Technologie erlaubt es den Tätern, insbesondere gegen

---

[55] *Hermmann/Heilmann* in: BeckOK IT-Recht, 1. Edition, § 90 TKG Rn. 2.
[56] https://netzpolitik.org/2019/warum-es-so-schwer-ist-rechtlich-gegen-spionage-apps-vorzugehen/ (abgerufen am 23.03.2021).
[57] *Hermmann/Heilmann* in: BeckOK IT-Recht, 1. Edition, § 90 TKG Rn. 2.
[58] https://stopstalkerware.org/de/was-ist-stalkerware/ (abgerufen am 23.03.2021).

Frauen und Mädchen gerichtet, private Daten der Opfer zu erhalten, diese zu verfolgen und zu belästigen. Ein Forschungsbericht „Gewalt im Internet gegen Frauen und Mädchen“ aus dem Jahr 2017 kommt zu dem Ergebnis, dass 70 Prozent der befragten Frauen, die von Cyber-Stalking betroffen waren, auch psychische oder sexuelle Gewalt durch den Partner erfahren haben, da die geschlechterspezifische Gewalt durch die missbräuchliche Nutzung der Technologie erleichtert wird. Stalkerware ist also ein geschlechterspezifisches Problem.[59] Für die Benutzung solcher Tools zur Erlangung von Daten kommt eine Strafbarkeit nach §§ 202a ff. StGB in Betracht. § 202b StGB stellt das unbefugte Verschaffen von Daten aus einer nichtöffentlichen Datenübermittlung unter Anwendung von technischen Mitteln unter Strafe. Der Begriff der technischen Mittel ist weit auszulegen und umfasst auch den Einsatz von Software, so z.B. Spionage-Tools, die Signale aufzeichnen (Keylogger) und Netzwerksniffer.[60] Für das „Verschaffen“ im Sinne des § 202b StGB reicht die Kenntnisnahme oder Erlangung der Herrschaftsgewalt über die Daten[61], sodass bei Telefongesprächen das Mithören oder bei E-Mails die Kenntnisnahme[62] den Tatbestand verwirklicht. Eine Strafbarkeit beim Verwenden von Stalkerware ist je nach Ausgestaltung auch nach § 202a StGB möglich. Danach macht sich strafbar, wer sich unbefugt unter Überwindung der Zugangssicherung Zugang zu Daten verschafft, die nicht für ihn bestimmt sind und die gegen unberechtigten Zugang besonders gesichert sind. Bedeutsam dafür ist, dass der Täter oder die Täterin den Zugang zu Daten unter Überwindung der Zugangssicherung erlangt, also ein Zugangsschutz[63] vorliegt, den er zur Erlangung der Daten überwinden muss. Davon umfasst ist auch das Verschaffen des Zugangs durch Hacking wie z.B. beim Einsatz von Trojanischen Pferden, Sniffern oder Backdoorprogrammen.[64] Erwähnt sei ergänzend ein aktueller Gesetzentwurf vom 24. März 2021 zur Erweiterung des „Stalking“-Paragraphen der Nachstellung nach § 238 StGB. Dieser sieht einen erweiterten Tatbestandskatalog für typische Cyberstalkinghandlungen vor. Dabei sieht § 238 Abs. 2 Nr. 5 StGB-E eine Strafbarkeit in Form eines besonders schweren Falles vor, wenn der Täter oder die Täterin durch Stalkingware, Hacking oder auf andere Weise unbefugten Zugang zu Daten des Opfers erlangt, also z.B. in Social-Media-Konten eindringt oder den Standort verfolgt[65], also ein „Computerprogramm einsetzt, dessen Zweck das digitale Ausspähen anderer Personen ist“.[66] Hier soll eine Form des (bisher im Strafrecht nicht

---

[59] https://stopstalkerware.org/de/was-ist-stalkerware/ (abgerufen am 23.03.2021); https://eige.europa.eu/publications/cyber-violence-against-women-and-girls (abgerufen am 23.03.2021).
[60] *Eisele* in: Schönke/Schröder/Eisele, Strafgesetzbuch, § 202b StGB Rn. 8.
[61] *Mansdörfer* in: BeckOK IT-Recht, § 202b StGB Rn. 10.
[62] *Weidemann* in: BeckOK StGB, § 202b StGB Rn. 9.
[63] *Keller* in: Hamburger Kommentar Gesamtes Medienrecht, § 202a StGb Rn. 35.
[64] *Keller* in: Hamburger Kommentar Gesamtes Medienrecht, § 202a StGb Rn. 36.
[65] https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_Cyberstalking.pdf;jsessionid=476E482F2DC54D128D112D010F1E6632.1_cid334?__blob=publicationFile&v=3, S. 11 (abgerufen a, 24.03.2021).
[66] Gesetzesentwurf vom 24.03.2021: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_Cyberstalking.pdf;jsessionid=476E482F2DC54D128D112D010F1E6632.1_cid334?__blob=publicationFile&v=3 (abgerufen am 24.03.2021).

hinreichend erfassten) Doxing erfasst werden, wenn so erlangte Daten nach § 238 Abs. 2 Nr. 6, 7 StGB-E öffentlich gemacht oder breitet werden.[67]

bb) Rechtliche Konsequenzen der Herstellung von Stalkerware

Für Vorbereitungshandlungen, insbesondere also für die Herstellung solcher Tools kann sich eine Strafbarkeit nach § 202c Abs. 1 Nr. 2 StGB ergeben, womit insbesondere Hacker-Tools erfasst werden sollen, die nach Art und Zweck auf illegale Zwecke ausgerichtet sind, leicht und anonym verfügbar sind und leicht angewendet werden können.[68] Dabei muss das Computerprogramm zur Begehung einer Straftat nach den §§ 202a, 202b StGB bestimmt sein.[69] Bei „dual use tools", bei denen nicht ausschließlich illegale Zwecke angelegt sind, sondern erst eine missbräuchliche Anwendung zur Illegalität führt, ist der Tatbestand nicht verwirklicht.[70] Dies führt zu dem praktischen Problem, dass solche Software oft als Diebstahlschutz angepriesen wird oder für Eltern zur Ortung ihres Kindes, sodass nicht nur illegale Zwecke angestrebt werden.[71] Bei der Haftung von Firmen besteht regelmäßig das Problem, dass diese selbst keine Daten verarbeiten, sondern letztlich nur die Personen, die solche Stalkerware einsetzen, sodass nur diese Verantwortlicher im Sinne des Datenschutzrechtes sind. Selbst wenn diese aber selbst Daten erheben, besteht oftmals das Problem, dass sie ihren Sitz außerhalb der EU haben und praktisch schwer zu fassen sind.[72]

cc) Rechtliche Einordnung eines möglichen Verbots

Letztlich ist der Umstand, dass so gut wie keine Verurteilungen wegen der Nutzung von Stalkerware existieren[73] aber nicht allein auf das materielle Strafrecht zurückzuführen, das eine Strafbarkeit dem Grunde nach für die Herstellung und Benutzung der Tools vorsieht. Denn viele der Betroffenen wissen gar nicht und erfahren es auch nie, dass etwa ihr Handy abgehört wird oder ihre Bewegungen getrackt werden, weil Spionage-Apps installiert sind.[74] Insoweit sind Maßnahmen erforderlich, die den Umgang mit Stalkerware regulieren.

Dabei scheitert ein vollständiges Verbot regelmäßig. Zum einen begegnet ein Verbot durch die Bundesnetzagentur analog zu den oben dargestellten „smart-voyeur-Geräten" dem Problem, dass eine entsprechende Rechtsgrundlage nicht bereits vorhanden ist. Oben genannter § 90 TKG bildet nur die Rechtsgrundlage für ein Verbot Sendeanlagen

---

[67] https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_Cyberstalking.pdf;jsessionid=476E482F2DC54D128D112D010F1E6632.1_cid334?__blob=publicationFile&v=3, S. 11 (abgerufen am 24.03.2021).
[68] BT-Drs. 16/3656, S. 12; Weidemann in: BeckOK StGB, § 202c Rn. 6.
[69] BT-Drs. 16/3656, S. 12; Weidemann in: BeckOK StGB, § 202c Rn. 7.
[70] BT-Drs. 16/3656, S. 19.
[71] https://www.spiegel.de/netzwelt/apps/stalkerware-welche-apps-gibt-es-wie-kann-man-sich-schuetzen-a-ae8c77a5-da62-420a-a62f-0729bd8201b0 (abgerufen am 22.03.2021).
[72] https://netzpolitik.org/2019/warum-es-so-schwer-ist-rechtlich-gegen-spionage-apps-vorzugehen/ (abgerufen am 23.03.2021).
[73] https://netzpolitik.org/2019/warum-es-so-schwer-ist-rechtlich-gegen-spionage-apps-vorzugehen/ (abgerufen am 22.03.2021); AG Heilbronn, becklink 2001899.
[74] https://netzpolitik.org/2019/warum-es-so-schwer-ist-rechtlich-gegen-spionage-apps-vorzugehen/ (abgerufen am 22.03.2021).

oder sonstigen Telekommunikationsanlagen, die ihrer Form nach einen anderen Gegenstand vortäuschen oder mit Gegenständen des täglichen Lebens verkleidet sind und deshalb dazu geeignet sind, das nicht öffentlich gesprochene Wort eines anderen unbemerkt abzuhören oder das Bild unbemerkt anzufertigen, also ausdrücklich Hardware und keine Software.[75] Zum anderen bieten solche Softwareangebote und Apps ihre Leistungen regelmäßig unter dem Deckmantel der rechtmäßigen Verwendungsabsicht an. So werden sie regelmäßig als Sicherheits-App für Kinder oder als Diebstahlsicherung mit Einwilligung angeboten, wobei der Nutzer zustimmt, die Software nur gegen Einwilligung zu nutzen (s.o. zur dual-use-Problematik) .[76]

Im Einzelfall sind dabei auch rechtmäßige Einsatzszenarien möglich und denkbar, sodass bezüglich eines umfassenden Verbots zunächst mildere Mittel wie Warnungen oder technische Anforderungen in Betracht kommen. Dabei sollten die Maßnahmen sich nicht auf eine einmalige Zustimmung beschränken, die dadurch umgangen werden kann, dass der Täter oder die Täterin eine Spionage-App auf dem Smartphone in einem unbeobachteten Moment installiert und der Datenweitergabe zustimmt oder ein Smartphone vergibt, auf dem die Stalkerware bereits installiert ist. Vielmehr müsste bei einem fremden Abruf der Daten in regelmäßigen Abständen ein Hinweis durch die App erfolgen, der der betroffenen Person die Möglichkeit gibt, etwaige Stalkingversuche zu identifizieren oder bei rechtmäßiger Nutzung die Einwilligung zu bestätigen. So haben die Opfer erst die Möglichkeit, Stalkingversuche durch Stalkerware zu entdecken und sodann zur Anzeige zu bringen oder Strafantrag zu stellen.

75 https://netzpolitik.org/2019/warum-es-so-schwer-ist-rechtlich-gegen-spionage-apps-vorzugehen/ (abgerufen am 23.03.2021);

76 https://www.lto.de/recht/feuilleton/f/spionage-app-ausspaehen-daten-corona-seitensprung-arbeitnehmer/ (abgerufen am 22.03.2021); https://stopstalkerware.org/de/was-ist-stalkerware/ (abgerufen am 23.03.2021).

IV. Anhang: Entwurf eines „Cybermobbing-Gesetzes“

Der beigefügte wissenschaftliche Entwurf eines Gesetzes zur Verbesserung des Persönlichkeitsrechtsschutzes im Internet wurde im Rahmen eines Drittmittelprojektes der Universität Passau, Forschungsstelle für IT-Recht und Netzpolitik, von Prof. Dr. Dirk Heckmann und Dr. Anne Paschke, im Mai 2018 fertiggestellt und der (Fach-) Öffentlichkeit über die Webseite

https://www.arag.com/de/presse/pressemitteilungen/group/00448/

zur Verfügung gestellt. Er dient hier der Vertiefung der Ausführungen in Abschnitt II.

Auf eines sei dabei hingewiesen:

Der Entwurf des PRG sieht unter anderem eine Angleichung des Cybermobbing an das Cyberstalking vor. Er formulierte 2018 deshalb: „… wenn die Tat geeignet ist, das Opfer in seiner Lebensgestaltung *schwerwiegend* zu beeinträchtigen.“

Im Regierungsentwurf eines „Gesetzes zur Änderung des Strafgesetzbuches – effektivere Bekämpfung von Nachstellungen und bessere Erfassung des Cyberstalkings“ vom 24.3.2021 mit nunmehr – mit guten Gründen – vorgeschlagen, § 238 Abs. 1 StGB dahingehend zu ändern: „…wer einer anderen Person in einer Weise unbefugt nachstellt, die geeignet ist, deren Lebensgestaltung *nicht unerheblich* zu beeinträchtigen.“

Wollte man also unserem Vorschlag eines Cybermobbing-Straftatbestandes folgen, könnte der § 190 Abs. 1StGB-neu so formuliert werden:

„(1) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer einen ehrverletzenden Inhalt (§§ 185 bis 187) dergestalt im Internet zugänglich macht, dass dieser von einer erheblichen Anzahl von Personen wahrgenommen werden kann, wenn die Tat geeignet ist, das Opfer in seiner Lebensgestaltung nicht unerheblich zu beeinträchtigen.“

Damit wäre dann wiederum ein Gleichklang mit § 238 StGB erzielt.

Verbesserung des Persönlichkeitsrechtsschutzes im Internet

Ein rechtspolitischer Diskussionsvorschlag als

Gesetzentwurf mit Begründung

Wissenschaftliches Drittmittelprojekt der Universität Passau
Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht
Forschungsstelle für IT-Recht und Netzpolitik For..Net

auf Initiative und mit Unterstützung der ARAG

Univ.-Prof. Dr. Dirk Heckmann

Dr. Anne Paschke, Akad. Rätin a. Z., Geschäftsführerin For..Net

Vorwort

Im Koalitionsvertrag zwischen CDU/CSU und SPD für die 18. Legislaturperiode aus dem Jahr 2013 heißt es auf Seite 147:

„Wir verbessern den strafrechtlichen Schutz vor Beleidigungen in sozialen Netzwerken und Internetforen (Cybermobbing und Cybergrooming), da die Folgen für die vor einer nahezu unbegrenzten Öffentlichkeit diffamierten Opfer besonders gravierend sind. Cybermobbing und Cybergrooming in sozialen Netzwerken müssen einfacher gemeldet und angezeigt werden können."

Vier Jahre später kann festgestellt werden, dass dieses Versprechen nicht eingelöst worden ist. Die einzigen Reformen, die überhaupt in diesem Kontext erwähnenswert sind, sind eine Verschärfung des § 201a StGB (Schutz des höchstpersönlichen Lebensbereichs vor Weitergabe intimer Bildaufnahmen, insbesondere auf elektronischem Wege) im Jahr 2015 und der Erlass des Netzwerkdurchsetzungsgesetzes (NetzDG), das am 1.10.2017 in Kraft getreten ist. Während der *strafrechtliche* Schutz vor Cybermobbing durch die einzelne Detailregelung zu kurz greift, zielt das hoch umstrittene NetzDG mit seinen *zivilrechtlichen* Instrumenten quasi ins Leere: Es ist nicht nur nach Meinung vieler Experten europarechts- und verfassungswidrig. Auch konzeptionell setzt es falsch an, weil es die Täter weitgehend schont, stattdessen Plattformbetreibern quasi-richterliche Aufgaben auferlegt und die technischen Möglichkeiten für einen besseren Rechtsschutz nicht ausschöpft.

Der aktuelle Koalitionsvertrag von CDU/CSU und SPD vom 12. März 2018 erneuert das Versprechen eines Cybermobbing-Gesetzes nicht. Zum NetzDG heißt es nur: „Das Netzwerkdurchsetzungsgesetz ist ein richtiger und wichtiger Schritt zur Bekämpfung von Hasskriminalität und strafbaren Äußerungen in sozialen Netzwerken. Wir werden auch weiterhin den Schutz der Meinungsfreiheit sowie der Persönlichkeitsrechte der Opfer von Hasskriminalität und strafbaren Äußerungen sicherstellen. Die Berichte, zu denen die Plattformbetreiber verpflichtet sind, werden wir sorgfältig auswerten und zum Anlass nehmen, um das Netzwerkdurchsetzungsgesetz insbesondere im Hinblick auf die freiwillige Selbstregulierung weiterzuentwickeln." (Seite 31)

Hier setzt die Idee einer Verbesserung des Persönlichkeitsschutzes durch eine Kombination von strafrechtlicher Verschärfung, erweitertem Opferschutz und Mitwirkung der Plattformbetreiber in ihrem ureigenen Kompetenzbereich, der Entwicklung und Bereitstellung von Technologien, an.

Diese Idee beruht auf der Auswertung umfangreicher Studien, die von der ARAG SE gemeinsam mit dem Bündnis gegen Cybermobbing und Frau Dr. Katzer von 2013 bis 2016 in diesem Themenfeld durchgeführt wurden. Dabei stellte sich deutlich heraus, dass durch Cybergewalt Handlungsmuster vermittelt, erlernt und angewendet werden, die auf eine systematische Verletzung von Persönlichkeitsrechten abzielen. Mit Blick auf die mehr als 80jährige Expertise des Unternehmens in

nationalen wie internationalen Rechtsfragen ist die ARAG überzeugt, dass dieses wichtige Rechtsgut in Deutschland auch durch das NetzDG nicht wirksam geschützt wird. Daraus entstand die Initiative, eine neue Diskussionsgrundlage zu schaffen, um die gesetzlichen Rahmenbedingungen auch im internationalen Vergleich zu verbessern. Im Rahmen eines Drittmittelprojekts mit der Universität Passau, Forschungsstelle für IT-Recht und Netzpolitik (For..Net), wurde der vorliegende Gesetzentwurf durch Professor Dirk Heckmann und die For..Net-Geschäftsführerin Dr. Anne Paschke als Vorschlag für eine zielführende politische Diskussion zum Persönlichkeitsrechtsschutz im Internet verfasst. Er vereint die konzeptionellen Ideen der Strafverschärfung, des Opferschutzes und der Innovationen eines technischen Rechtsschutzes. Hierbei wurde bewusst das Format eines Gesetzentwurfs gewählt, um dem Eindruck einer rein „akademischen Angelegenheit“ entgegenzuwirken. Mit ihm sollen die Verantwortlichen im Bundestag und den zuständigen Ministerien gleichsam in gewohnter Diktion angesprochen werden.

Gleichwohl bleibt dies natürlich ein Diskussionsvorschlag ohne den Anspruch zu erheben, dass dies genau so umgesetzt werden müsste. Wenn der hierdurch angestoßene Diskussionsprozess ein noch besseres Konzept hervorbringen sollte, wird das Ziel der Projektverantwortlichen, endlich besser vor Cybermobbing zu schützen, ebenso erreicht.

Besonderer Erwähnung bedarf der Umstand, dass die Diskussion um Hass im Netz, Hate Speech und verleumderische „Fake News“ weiter reicht als das Spektrum der rechtspolitischen Ziele, die mit dem hier zur Diskussion gestellten „Gesetz zur Verbesserung des Persönlichkeitsrechtsschutzes im Internet (Persönlichkeitsrechtsschutzgesetz – PRG)“ verfolgt werden und umsetzbar erscheinen. Cybermobbing, so wie es hier verstanden wird, ist ein spezielles Phänomen schwerer und schwerster Ehrverletzungen im bzw. über das Internet, die sich gegen einzelne Personen richten. „Hass im Netz“, der sich gegen Personengruppen, etwa ethnische Minderheiten wendet, wird davon nicht erfasst. Ebenso geht es hier nicht um einfache Falschmeldungen, so schädlich diese auch für Demokratie und politische Kultur sein mögen. Durch die hier vorgelegte politische Initiative kann aber ein Signal gesetzt werden, dass nicht jedes Verhalten im Internet hingenommen wird, nur weil Plattformen wie soziale Netzwerke häufig dem Diktat der normativen Kraft des Faktischen folgen. Damit kann und soll zugleich ein wichtiger gesellschaftlicher Diskurs angestoßen werden. Denkbar ist, dass das System des Persönlichkeitsrechtsschutzes, dem durch das PRG wichtige Bausteine zugefügt werden, durch diesen Diskurs immer weiter ausgebaut und verfeinert wird.

Gesetzentwurf

Entwurf eines

Gesetzes zur Verbesserung des Persönlichkeitsrechtsschutzes im Internet

(Persönlichkeitsrechtsschutzgesetz – PRG)

A. Problem und Ziel

Grobe Beleidigungen und Verleumdungen nehmen in unserer Gesellschaft zu, auch und gerade in sozialen Netzwerken, Online-Foren und interaktiven Portalen. Das Internet ist aber kaum „schuld“ an dieser Entwicklung, es zeigt vielmehr als „Spiegel der Gesellschaft“ deren Zustand in Bezug auf das Werteverständnis, charakterliche Merkmale seiner Nutzer und auch die Diskussionskultur. Zwar sind solche Ehrverletzungen schon nach geltendem Recht strafbar. Dies hindert die Täter aber nicht an ihrem Treiben, vor allem weil eine Strafverfolgung nur in ganz seltenen Fällen stattfindet. Das hat mehrere Ursachen: Zum einen werden Ehrverletzungsdelikte nur auf Antrag verfolgt und selbst dann kaum zur Verurteilung gebracht. Zum anderen scheuen viele Opfer die Strafanzeige, weil sie im Verfahren selbst nur unzureichend geschützt und unterstützt werden. Auch die schiere Masse von Tausenden neuer Straftaten jeden Tag scheint die Ermittlungsbehörden zu erdrücken. Außerdem leidet die Diskussion um das Thema „Cybermobbing“ darunter, dass erhebliche Ehrverletzungen (teilweise mit Suizid-Folgen) mit einfachen Beleidigungen „in einen Topf geworfen werden“ (zumal derzeit § 185 StGB dafür einheitlich gilt) und dabei auch keine rechtssichere Abgrenzung gegenüber grundrechtlich geschützten Meinungsäußerungen erfolgt. Das am 1. Oktober 2017 in Kraft getretene „Netzwerkdurchsetzungsgesetz“ nimmt einseitig die Betreiber von sozialen Netzwerken in die Pflicht und adressiert undifferenziert missliebige Äußerungen und Meldungen (einschließlich sog. „fake news“). Eine echte Verbesserung des Persönlichkeitsrechtsschutzes im Internet ist durch dieses Gesetz weder intendiert noch möglich.

B. Lösung

Um die Nutzer von sozialen Medien besser vor Ehrverletzungen im Internet zu schützen, sieht der Entwurf für ein Persönlichkeitsrechtsschutzgesetz (PRG) die Änderung beziehungsweise Ergänzung des Straf-, Strafprozess- und Telemedienrechts vor. Dies betrifft insbesondere die Neuregelung von Qualifikationsstraftatbeständen bei Ehrverletzungen im Internet, aber auch die Verbesserung des Opferschutzes sowie eine moderate Einbindung der Diensteanbieter in die Rechtsdurchsetzung. Durch diesen breiten Regelungsansatz soll der Bedeutung und Schutzbedürftigkeit des Persönlichkeitsrechts, welches durch die technischen Möglichkeiten des Internets in besonderem Maße betroffen ist, Rechnung getragen werden.

C. Alternativen

Keine.

Die Beibehaltung oder moderate Änderung des am 30. Juni 2017 vom Deutschen Bundestag verabschiedeten Gesetzes zur Verbesserung der Rechtsdurchsetzung in den sozialen Netzwerken (NetzDG) stellt keine taugliche Alternative zu dem hier vorliegenden Gesetzentwurf dar. Trotz der Änderungen, die das Gesetz noch im Rechtsausschuss erfahren hat, wirft es in erheblichem Maße europarechtliche Probleme auf, insbesondere aufgrund der länderübergreifenden Geltung innerhalb der Union in Hinblick auf das Herkunftslandprinzip gemäß Artikel 3 Richtlinie 2000/31/EG (E-Commerce-Richtlinie), und wird vor allem aufgrund seiner starren Löschfristen und der Übertragung einer Löschungskompetenz an die sozialen Netzwerke als europarechtswidrig angesehen.[1]

Im Rahmen von potentiell ehrverletzenden Inhalten ist eine Abgrenzung zwischen einer Persönlichkeitsrechtsverletzung und einem Inhalt, der noch der Meinungsfreiheit unterfällt, meist äußerst komplex und stellt die Gerichte vor große Herausforderungen. Derartige rechtliche Abwägungen können von den Diensteanbietern schon wegen der schieren Masse an beanstandungsfähigen Äußerungen nicht ohne die Gefahr eines „Overblocking“ vorgenommen werden. Ein solches „Overblocking“, also die Löschung oder Sperrung legaler Inhalte, bedeutet zugleich eine erhebliche Einschränkung der Meinungsfreiheit. Nach der Regelungssystematik des NetzDG ist zum einen aufgrund der kurzen Fristen für die Diensteanbieter und zum anderen wegen der Bußgeldbewehrung des Nichtvorhaltens eines effektiven Beschwerdesystems damit zu rechnen, dass die Diensteanbieter in Zweifelsfällen auch legale Inhalte löschen werden.

D. Haushaltsausgaben ohne Erfüllungsaufwand

###

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Keiner.

E.2 Erfüllungsaufwand für die Wirtschaft

###

E.3 Erfüllungsaufwand für die Verwaltung

###

F. Weitere Kosten

###

[1] Zur Europarechtswidrigkeit des NetzDG siehe das Gutachten des Wissenschaftlcihen Dienstes des Deutschen Bundestages (https://www.bundestag.de/blob/510384/c5bdf3939cf1a4529d2f7abf11065ee5/pe-6-032-17-pdf-data.pdf) sowie die Stellungnahme der Deutschen Gesellschaft für Recht und Informatik DGRI e.V. http://dgri.de/index.php/fuseaction/download/lrn_file/dgri-stellungnahme-netzdg.pdf Zur darüber hinausgehenden Verfassungswidrigkeit des NetzDG ausführlich Gersdorf, MMR 2017, 439.

Entwurf eines Gesetzes zur Verbesserung des Persönlichkeitsrechtsschutzes im Internet

(Persönlichkeitsrechtsschutzgesetz – PRG)

Artikel 1

Änderung des Strafgesetzbuches

Das Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 1 des Gesetzes vom 17. August 2017 (BGBl. I S. 3202) geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:
   a. Nach der Angabe zu § 189 werden folgende Angaben eingeführt:
      „§ 190 Schwere Ehrverletzung im Internet“.
   b. § 190 Wahrheitsbeweis durch Strafurteil wird zu § 191.
2. § 185 wird wie folgt geändert:
   a. Der Wortlaut wird Satz 1.
   b. Folgender Satz 2 wird ergänzt:
      „Wird ein ehrverletzender Inhalt über das Internet einer erheblichen Anzahl von Personen zugänglich gemacht, wird die Tat mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.“
3. § 190 Wahrheitsbeweis durch Strafurteil wird zu § 191.
4. § 190 wird wie folgt neu eingefügt:

„§ 190

Schwere Ehrverletzung im Internet

(1) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer einen ehrverletzenden Inhalt (§§ 185 bis 187) dergestalt im Internet zugänglich macht, dass dieser von einer erheblichen Anzahl von Personen wahrgenommen werden kann, wenn die Tat geeignet ist, das Opfer in seiner Lebensgestaltung schwerwiegend zu beeinträchtigen.

(2) Wer durch eine Tat nach Absatz 1 wenigstens leichtfertig die Selbsttötung des Opfers verursacht, wird mit Freiheitsstrafe bis zu fünf Jahren bestraft.“

5. § 194 Absatz 1 Satz 2 wird durch folgenden Satz ersetzt:

„Ein Antrag ist nicht erforderlich, wenn

1. die Tat durch Verbreiten oder öffentliches Zugänglichmachen einer Schrift (§ 11 Abs. 3), in einer Versammlung oder dadurch begangen wird, dass beleidigende Inhalte mittels Rundfunk oder Telemedien der Öffentlichkeit zugänglich gemacht worden sind, und der Verletzte als Angehöriger einer Gruppe unter der nationalsozialistischen oder einer anderen Gewalt- und Willkürherrschaft verfolgt wurde, diese Gruppe Teil der Bevölkerung ist und die Beleidigung mit dieser Verfolgung zusammenhängt oder

2. der Verletzte Opfer einer Tat gemäß § 190 geworden ist.“

Artikel 2

Änderung der Strafprozessordnung

Die Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. S. 1074, 1319), die zuletzt durch Artikel 1 des Gesetzes vom 27. August 2017 (BGBl. I S. 3295) geändert worden ist, wird wie folgt geändert:

1. § 158 Absatz 1 Satz 1 wird wie folgt geändert:

   Nach dem Wort „mündlich“ wird ein Komma gesetzt und das Wort „elektronisch“ eingefügt.

2. § 395 wird wie folgt geändert:

   a. Nach Absatz 1 Satz 1 Nummer 1 wird folgende neue Nummer 1a eingefügt:

   „§ 190 Absatz 1 des Strafgesetzbuches,“.

   b. Nach Absatz 2 Nummer 1 wird folgende neue Nummer 1a eingefügt:

   „deren Kinder, Eltern, Geschwister, Ehegatten oder Lebenspartner sich selbst aufgrund einer Ehrverletzung im Internet getötet haben (§ 190 Absatz 2 des Strafgesetzbuches) oder“.

3. § 397a wird wie folgt geändert:

   a. Nach Absatz 1 Nummer 2 wird folgende neue Nummer 2a eingefügt:

   „Angehöriger im Sinne des § 395 Absatz 2 Nummer 1a ist,“

   b. In Absatz 1 Nummer 5 wird zwischen „§§“ und „221“ „190 Absatz 1“ eingefügt.

Artikel 3

Änderung des Telemediengesetzes

Das Telemediengesetzes vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 1. September 2017 (BGBl. I S. 3352) geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

Nach der Angabe zu § 13 werden folgende Angaben eingefügt:

„§ 13a Ermächtigung zum Erlass der Rechtsverordnung

§ 13b Umgang mit Beschwerden über persönlichkeitsrechtsverletzende Inhalte

§ 13c Anspruch auf Auskunft bei Persönlichkeitsrechtsverletzungen

§ 13d Inländischer Zustellungsbevollmächtigter“.

2. Nach § 2 Satz 1 Nummer 1 wird folgende Nummer 1a angefügt:

„sind Diensteanbieter sozialer Telemedien Diensteanbieter, die mit Gewinnerzielungsabsicht Plattformen im Internet betreiben, die es Nutzern ermöglichen, beliebige Inhalte der Öffentlichkeit zugänglich zu machen und mit anderen Nutzern auszutauschen oder zu teilen; die Diensteanbieter sozialer Telemedien im Sinne dieses Gesetzes werden durch eine Rechtsverordnung nach § 13a näher bestimmt,“

3. Nach § 13 werden die folgenden §§ 13a, 13b, 13c und § 13d eingefügt:

„§ 13a

Ermächtigung zum Erlass der Rechtsverordnung

[1]Das Bundesministerium für Wirtschaft und Energie bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft und der betroffenen Diensteanbieter im Einvernehmen mit dem Bundesministerium der Justiz und für Verbraucherschutz, welche Diensteanbieter wegen ihrer Bedeutung und Reichweite als Diensteanbieter sozialer Telemedien gelten. [2]Spätestens einen Monat nach Inkrafttreten der Rechtsverordnung nach Satz 1 haben Diensteanbieter sozialer Telemedien die Vorgaben aus §§ 13b, 13c und 13d zu erfüllen. [3]Gleiches gilt für die Befugnis aus § 14 Abs. 3 Satz 2.

§ 13b

Umgang mit Beschwerden über persönlichkeitsrechtsverletzende Inhalte

(1) [1]Diensteanbieter sozialer Telemedien sind verpflichtet, bei der Bereitstellung ihrer Dienste geeignete technische Maßnahmen zur Meldung persönlichkeitsrechtsverletzender Inhalte vorzuhalten. [2]Dies kann insbesondere durch die Bereitstellung einer Melde-Schaltfläche erfolgen. [3]Die Diensteanbieter sozialer Telemedien haben durch geeignete technische Maßnahmen dafür Sorge zu tragen,

dass die technischen Maßnahmen zur Meldung nicht durch automatisch agierende Computerprogramme missbraucht werden.

(2) [1]Diensteanbieter sozialer Telemedien sind verpflichtet, persönlichkeitsrechtsverletzende Inhalte unverzüglich nach Meldung deutlich sichtbar zu kennzeichnen und eine Dokumentation des Inhalts und der Wahrnehmung und Verbreitung dieses Inhalts durch Dritte zu erstellen. [2]Der gemeldete Inhalt ist zusätzlich mit dem Hinweis zu versehen, dass eine Dokumentation erfolgt und die Weiterverbreitung des Inhalts rechtliche Konsequenzen nach sich ziehen kann. [3]Dem Verfasser des gemeldeten Inhalts ist binnen einer Frist von einer Woche Gelegenheit zur Stellungnahme gegenüber dem Diensteanbieter sozialer Telemedien zu geben.

(3) Die Kennzeichnung und die diesbezüglichen Hinweise sind unverzüglich zu entfernen, wenn sich die Meldung als offensichtlich unberechtigt erweist, die Meldung zurückgenommen wird oder ein Gericht die Rechtmäßigkeit des Inhalts festgestellt hat.

(4) Die Verantwortlichkeit eines Diensteanbieters nach § 10 bleibt unberührt.

§ 13c

Anspruch auf Auskunft bei Persönlichkeitsrechtsverletzungen

(1) [1]In Fällen einer öffentlich zugänglichen Persönlichkeitsrechtsverletzung hat der Verletzte nach vorheriger richterlicher Anordnung zur Durchsetzung zivilrechtlicher Ansprüche einen Anspruch auf Auskunft gegenüber der Person, die die für die rechtsverletzende Tätigkeit genutzte Dienstleistung erbracht hat. [2]Die richterliche Anordnung ist von dem Verletzten zu beantragen. [3]Für den Erlass dieser Anordnung ist das Amtsgericht, in dessen Bezirk der Verletzte seinen Wohnsitz oder gewöhnlichen Aufenthalt hat, ohne Rücksicht auf den Streitwert ausschließlich zuständig. [4]Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. [5]Die Kosten der richterlichen Anordnung trägt der Verletzte. [6]Gegen die Entscheidung des Amtsgerichts ist die Beschwerde statthaft. [7]Die Vorschriften zum Schutz personenbezogener Daten bleiben im Übrigen unberührt.

(2) [1]Der Auskunftsanspruch umfasst insbesondere

1. den Namen und die Anschrift des Rechtsgutverletzers, sofern diese dem Diensteanbieter sozialer Telemedien bekannt sind und

2. den Tag und die Uhrzeit der Persönlichkeitsrechtsverletzung.

[2]Zudem ist eine vorhandene Dokumentation der Wahrnehmung und Verbreitung des Inhalts durch Dritte der Persönlichkeitsrechtsverletzung dem Verletzten zur Verfügung zu stellen. [3]Der zur Auskunft Verpflichtete kann von dem Verletzten den Ersatz der für die Auskunftserteilung erforderlichen Aufwendungen verlangen.

(3) Erteilt der zur Auskunft Verpflichtete die Auskunft vorsätzlich oder grob fahrlässig nicht, falsch oder unvollständig, so ist er dem Verletzten zum Ersatz des daraus entstehenden Schadens verpflichtet.

(4) Der Diensteanbieter sozialer Telemedien ist verpflichtet, seine Nutzer über diesen Auskunftsanspruch zu informieren.

(5) Durch Absatz 1 wird das Grundrecht des Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) eingeschränkt.

§ 13d

Inländischer Zustellungsbevollmächtigter

[1]Anbieter sozialer Telemedien haben für Zustellungen in Bußgeldverfahren nach diesem Gesetz gegenüber der Verwaltungsbehörde, der Staatsanwaltschaft und dem zuständigen Gericht, sowie in zivilgerichtlichen Verfahren gegenüber dem zuständigen Gericht einen inländischen Zustellungsbevollmächtigten unverzüglich zu benennen. [2]Für Auskunftsersuchen einer inländischen Strafverfolgungsbehörde ist eine empfangsberechtigte Person im Inland zu benennen.“

4. § 14 wird wie folgt geändert:

   a. Der Wortlaut des § 14 Absatz 2 wird zu Satz 1.

   b. § 14 Absatz 2 wird um folgenden Satz 2 ergänzt:

   „Das berechtigte Auskunftsersuchen ist durch den Diensteanbieter innerhalb einer Frist von einer Woche zu beantworten.“

   c. § 14 Absatz 3 wird ersetzt durch:

   „Der Diensteanbieter ist befugt, Bestandsdaten an eine in § 158 Absatz 1 der Strafprozessordnung genannte Stelle zu Zwecken der Strafverfolgung zu übermitteln. Darüber hinaus gilt diese Befugnis für Diensteanbieter sozialer Telemedien auch für die in § 13c Absatz 2 Satz 1 und 2 genannten Informationen.“

   d. § 14 Absatz 4 und 5 werden aufgehoben.

5. In § 15 Absatz 5 wird Satz 4 wie folgt gefasst:

„§ 14 Abs. 2 und 3 findet entsprechende Anwendung.“

6. Nach § 16 Absatz 2 Nummer 3 werden folgende neue Nummern 3a, 3b, 3c und 3d ergänzt:

„3a. es entgegen § 13b Abs. 1 unterlässt, geeignete technische Maßnahmen zur Meldung persönlichkeitsrechtsverletzender Inhalte vorzuhalten,

3b. es entgegen § 13b Abs. 2 unterlässt, gemeldete persönlichkeitsrechtsverletzende Inhalte nicht unverzüglich deutlich sichtbar zu kennzeichnen oder

3c. es entgegen § 13d unterlässt, einen inländischen Zustellungsbevollmächtigten zu benennen,

3d. nicht innerhalb der in § 14 Abs. 2 Satz 2 festgesetzten Frist auf ein berechtigtes Auskunftsersuchen reagiert,“.

Artikel 4

Aufhebung des Netzwerkdurchsetzungsgesetzes

Das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG), welches am 30. Juni 2017 durch den Deutschen Bundestag beschlossen wurde, wird aufgehoben.

Artikel 5

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Im Internet ist bereits seit längerem eine Verrohung des zwischenmenschlichen Umgangs zu beobachten, welcher sich vor allem in Form von Persönlichkeitsrechtsverletzungen äußert. Das Internet erscheint aufgrund des Umfangs und der weitreichenden Akzeptanz bzw. Hinnahme dieser Entwicklung vielfach als rechtsfreier Raum. Dadurch wird die freiheitliche Entfaltung aller in Deutschland lebenden Menschen stark eingeschränkt und das Zusammenleben beeinträchtigt.

Besonders relevant ist das sog. Cybermobbing, das Beleidigen, Bedrohen, Bloßstellen oder Belästigen von Personen mithilfe neuer Kommunikationsmedien, welches schwerwiegende Folgen für die Betroffenen haben kann und deshalb ein ernstzunehmendes gesellschaftliches Problem darstellt. Dass Cybermobbing längst in der Mitte der Gesellschaft angelangt ist, belegt eine Studie, der zufolge über 30 Prozent der Jugendlichen zwischen 12 und 19 Jahren in Deutschland bereits Opfer irgendeiner Art von Cybermobbing geworden sind.[2]

Trotz der Existenz freiwilliger Initiativen von privaten Unternehmen, gegen strafbare Inhalte konsequent vorzugehen, hat dies bislang nicht zum gewünschten Erfolg geführt. Dieser Effekt wird dadurch verstärkt, dass Staatsanwaltschaften und Gerichte solche Taten derzeit selbst bei erheblichen Vorwürfen kaum strafrechtlich verfolgen.

Soweit es demnach an der Rechtsdurchsetzung in sozialen Netzwerken mangelt, müssen effektivere Methoden zum Auffinden, Melden und schnellen Löschen bzw. Sperren rechtswidriger Inhalte angedacht und umgesetzt werden. Hierbei verspricht ein sinnvolles Zusammenwirken der Internetnutzer, der Internetwirtschaft und der Justiz mehr Erfolg als die Auferlegung einseitiger Löschungspflichten. Überdies fehlt es an geeigneten straf- und strafprozessrechtlichen Instrumenten, die der Dynamik des zu regulierungsbedürftigen Bereichs, hinreichend Rechnung tragen.

Die Anbieter der sozialen Netzwerke tragen eine gesellschaftliche Verantwortung, der sie gerecht werden müssen. Aufgrund der Erfolglosigkeit bisheriger freiwilliger Initiativen der Diensteanbieter bedarf es einer klaren gesetzlichen Regelung, um der Gefahr durch Persönlichkeitsrechtsverletzungen im Internet wirksam begegnen zu können.

II. Wesentlicher Inhalt des Entwurfs

Um die Nutzer von sozialen Medien besser vor Ehrverletzungen im Internet zu schützen, sieht der Entwurf für ein Persönlichkeitsrechtsschutzgesetz (PRG) die

[2] Cyberlife II Studie 2017, http://bgcmob.de/fileadmin/pdf/2016_05_02_Cybermobbing_2017End.pdf.

Änderung beziehungsweise Ergänzung des Straf-, Strafprozess- und Telemedienrechts vor. Durch diesen breiten Regelungsansatz soll der Bedeutung und Schutzbedürftigkeit des Persönlichkeitsrechts, welches durch die technischen Möglichkeiten des Internets in besonderem Maße betroffen ist, Rechnung getragen werden.

Herausragende Bedeutung im Rahmen der Änderungen des Strafgesetzbuches hat die Schaffung eines § 190 StGB-E, welcher die Begehung von Cybermobbing mit Freiheitsstrafe von bis zu fünf Jahren, im Falle des Selbstmordes des Opfers sogar bis zu fünf Jahren, pönalisiert. Hierdurch wird auf die massive Verbreitung von Cybermobbing in den sozialen Netzwerken mit seinen oftmals schwerwiegenden Folgen für die Opfer reagiert. Auch wird die Begehung von Beleidigungen und die Verunglimpfung des Andenkens Verstorbener im Internet, aufgrund der der Begehungsweise immanenten Breiten- und Perpetuierungswirkung, mit einem höheren Strafrahmen versehen. Um der geringen Verfolgungsrate von Ehrverletzungen im Internet Rechnung zu tragen, entfällt das Strafantragserfordernis für alle diese neu eingeführten Straftatbestände.

Indem der Entwurf die Stellung einer Strafanzeige oder eines Strafantrags (soweit noch erforderlich) auch auf elektronischem Wege ermöglicht, wird ein Hemmnis für die effektive Verfolgung von Ehrverletzungsdelikten im Internet beseitigt. Außerdem wird der Opferschutz durch die Einführung der psychologischen Prozessbegleitung auch für Opfer von Cybermobbing verbessert. Zudem wird der Opferschutz durch die Erweiterung der Befugnis, als Nebenkläger aufzutreten und einen Beistand zu beantragen, manifestiert.

Der Entwurf führt im Rahmen des Telemedienrechts eine Definition für soziale Netzwerke ein, welche auf den Prinzipien der Gewinnerzielungsabsicht, des Austauschs unter den Nutzern und der Öffentlichkeit fußt. Durch die Regelung in § 13c TMG-E wird ein Auskunftsanspruch für die Nutzer sozialer Telemedien, welcher bislang nur durch eine Auslegung von § 242 BGB anerkannt war, rechtlich verankert. Dadurch wird die Rechtsverfolgung, welche aufgrund der Anonymität im Internet oftmals massiv erschwert war, vereinfacht. Die Rechte auf Anonymität gemäß Artikel 2 Abs. 1, 1 Abs. 1 GG und der Meinungsfreiheit gemäß Artikel 5 Abs. 1 GG werden aufgrund der Beschränkung auf besonders schwerwiegende Persönlichkeitsrechtsverletzungen, die offensichtlich rechtswidrig sind, nicht unverhältnismäßig eingeschränkt. Des Weiteren wird den Diensteanbietern unter Androhung eines Bußgeldes von bis zu 50.000 Euro die Pflicht auferlegt, ein technisches System zur Meldung von rechtswidrigen Inhalten vorzuhalten. Außerdem wird geregelt, wie mit derartigen Beschwerden von Nutzern umzugehen ist. Im Rahmen dessen wird den Diensteanbietern zwar die Möglichkeit zur Sperrung eingeräumt, eine Löschung erfolgt jedoch erst, nachdem eine gerichtliche Entscheidung diesbezüglich vorliegt. Dadurch wird die grundgesetzliche Kompetenzverteilung gewahrt, und es kommt nicht zu einer Privatisierung der Rechtsdurchsetzung mit der damit verbundenen unverhältnismäßigen Einschränkung der Grundrechte der Betroffenen. Im Übrigen wird durch weitere Maßnahmen, wie etwa die verpflichtende Benennung eines Zustellungsbevollmächtigten, die Abwicklung von Ermittlungsverfahren erleichtert.

III. Alternativen

Keine. Das Netzwerkdurchsetzungsgesetz ist nach Auffassung vieler Experten europa- und verfassungswidrig und erfasst auch nicht die hier geregelte Thematik des Cybermobbings. Nur ein Zusammenspiel dezidierter Straftatbestände, wirksamer Strafverfahrens- und Opferschutzvorschriften sowie eine zielführende und verhältnismäßige Mitwirkung der Diensteanbieter sozialer Telemedien vermag eine Verbesserung des Persönlichkeitsrechtsschutzes im Internet herbeizuführen.

IV. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes ergibt sich aus Artikel 74 Absatz 1 Nummer 1 GG (Strafrecht) sowie aus Artikel 74 Absatz 1 Nummer 11 GG (Recht der Wirtschaft). Die Neuregelungen im StGB und in der StPO sind unproblematisch dem Strafrecht zuzuordnen. Aber auch die Ergänzungen im TMG unterfallen der Gesetzgebungskompetenz des Bundes. Zum „Recht der Wirtschaft“ zählt auch das Recht der Netz- oder Internetwirtschaft. Auch wenn es bei der Bekämpfung von Cybermobbing um Aspekte geht, die zugleich die öffentliche Sicherheit und Ordnung betreffen, begründet das noch keine alleinige Gesetzgebungskompetenz der Länder. Die hier neu eingeführten §§ 13a ff. TMG regeln vielmehr bestimmte Mitwirkungspflichten von Diensteanbietern sozialer Telemedien bei der Reaktion auf rechtswidrige, ehrverletzende Inhalte. Diese wiederum betreffen keine Löschungspflichten wie beim umstrittenen Netzwerkdurchsetzungsgesetz, sondern Regelungen zur Organisation von Plattformen. Diese wiederum gehören zur klassischen Regulierung von Telemediendiensten im Kontext der E-Commerce-Richtlinie. Dort wird die Regelungsbefugnis der Mitgliedsstaaten ausdrücklich anerkannt, zu Zwecken des Abstellens oder der Verhinderung von Rechtsverletzungen „Verfahren für die Entfernung einer Information oder die Sperrung des Zugangs zu ihr festlegen.“ (Art. 14 Abs. 3 E-Commerce-Richtlinie) Genau um die Regelung solcher (technischer) Verfahren geht es bei der Ergänzung des TMG.

Dass diesbezüglich der Bund gesetzgebungsbefugt ist, ergibt sich aus der Notwendigkeit der Herstellung gleichwertiger Lebensverhältnisse im Bundesgebiet und die Wahrung der Rechts- oder Wirtschaftseinheit im gesamtstaatlichen Interesse, Artikel 72 Absatz 2 GG. Durch eine einheitliche Bundesgesetzgebung im Bereich der juristischen Plattformgestaltung wird gewährleistet, dass die Nutzung sozialer Netzwerke, die ihrerseits ja länderübergreifend erfolgt, auch überall unter den gleichen Bedingungen erfolgt. Für die Diensteanbieter wäre ein uneinheitliches Rechtsregime wirtschaftlich nachteilig, weil es einen unverhältnismäßigen Programmieraufwand bedeuten würde, sich auf unterschiedliches Landesrecht einstellen zu müssen.

V. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

1. Änderung des Strafgesetzbuches sowie der Strafprozessordnung

Die Übertragung von Hoheitsrechten auf die Europäische Union ist insbesondere in Bereichen wie dem Strafrecht, die konstituierend für die demokratische Selbstgestaltungsfähigkeit eines Verfassungsstaates sind, sachlich begrenzt (Art. 5 EUV). Auch mit Blick auf den Vertrag von Lissabon bleibt die originäre Gesetzgebungskompetenz im Bereich des formellen und materiellen Strafrechts bei den nationalen Gesetzgebern, vor allem, da ein supranationales Strafrecht nicht besteht.

2. Änderungen des Telemediengesetzes

Die in den §§ 13b ff., 14 Abs. 3 TMG-E vorgesehenen Mitwirkungspflichten von Diensteanbietern sozialer Telemedien sind mit dem europäischem Recht vereinbar.

a) Richtlinie 2000/31/EG (E-Commerce-Richtlinie)

Die §§ 13a ff. TMG sind mit den Vorgaben der Artikel 14, 15 E-Commerce-RL vereinbar. Insbesondere ist die Verpflichtung zur Schaffung technischer Vorkehrungen im Hinblick auf die Meldung und Dokumentation rechtswidriger Inhalte ein europarechtskonformes Verfahren zur Umsetzung der Vorgaben der E-Commerce-Richtlinie.

Aus der E-Commerce-Richtlinie ergeben sich keine Vorgaben bezüglich der Einrichtung und Ausgestaltung eines Melde- und Dokumentationsverfahrens. Vielmehr belässt der Richtliniengeber nach den Vorgaben des Erwägungsgrundes 48 der E-Commerce-RL den Mitgliedsstaaten die Möglichkeit, innerstaatliche Rechtsvorschriften zur Aufdeckung und Verhinderung bestimmter Arten rechtswidriger Taten zu erlassen. Diese Möglichkeit greift der Entwurf auf, indem ein entsprechendes Verfahren rechtsverbindlich für alle betroffenen Diensteanbieter normiert wird.

Das vorgesehene Meldeverfahren verstößt nicht gegen die Vorgaben des Artikel 14 E-Commerce-RL.

Sofern die Voraussetzungen des Artikel 14 Abs. 1 E-Commerce-RL gegeben sind, ist der Diensteanbieter, der im Auftrag eines Nutzers Informationen speichert, nicht verantwortlich. Der Diensteanbieter genießt daher keine umfassende Privilegierung. Der zentrale Gedanke, nach welchem eine Haftungsfreistellung in der Regel erst dann greift, wenn der Diensteanbieter unverzüglich nach Kenntnis tätig wird, um die rechtsverletzenden Inhalte zu entfernen (EuGH Urt. v. 12.07.2011 – C-324/09 Rn. 119), wird durch den vorgelegten Entwurf aufgegriffen und rechtssicher normiert.

Art. 14 Abs. 3 E-Commerce-RL lässt die Möglichkeit unberührt, „dass ein Gericht oder eine Verwaltungsbehörde nach den Rechtssystemen der Mitgliedsstaaten vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern, oder dass die Mitgliedsstaaten Verfahren für die Entfernung einer Information oder die Sperrung des Zugangs zu ihr festlegen.“ Um genau ein solches technisches Verfahren geht es bei § 13b TMG-E. Gerade weil Diensteanbieter – anders als im Netzwerkdurchsetzungsgesetz – keine rechtlichen (Vor-)Entscheidungen (Löschen oder Sperren), sondern lediglich technische Vorkehrungen für eine gerichtliche Auseinandersetzung zu treffen haben, geht das Regelungsregime der §§ 13b ff. TMG-E nicht weiter als der in der E-Commerce-Richtlinie normierte Pflichtenkreis.

Anders als das Netzwerkdurchsetzungsgesetz verzichtet der Entwurf in Übereinstimmung mit den Vorgaben in Artikel 14 Abs. 1 lit. b E-Commerce-RL auf starre Fristen und belässt es bei der Unverzüglichkeit. Die Diensteanbieter werden auf Grund des konkreten Hinweises lediglich verpflichtet, den konkret beanstandeten Inhalt zu kennzeichnen und zu dokumentieren. Darüber hinaus wird keine Verpflichtung zur Sichtung des Netzwerkes begründet. Der Diensteanbieter ist nicht gehalten, seinen Datenbestand auf weitere Rechtsverletzungen zu durchsuchen oder gegebenenfalls weitere Daten in ihrer Sichtbarkeit einzuschränken.

Die §§ 13c, 14 Abs. 3 TMG-E stehen auch nicht im Widerspruch zu Artikel 15 E-Commerce-RL.

Nach Artikel 15 Abs. 2 E-Commerce-RL können die Mitgliedsstaaten „Anbieter von Diensten der Informationsgesellschaft dazu verpflichten, die zuständigen Behörden unverzüglich über mutmaßliche rechtswidrige Tätigkeiten oder Informationen der Nutzer ihres Dienstes zu unterrichten, oder dazu verpflichten, den zuständigen Behörden auf Verlangen Informationen zu übermitteln, anhand derer die Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung geschlossen haben, ermittelt werden können.“

Davon erfasst werden gleichermaßen die Auskunftspflichten in § 13c TMG-E als auch die Weitergabe von Bestandsdaten in § 14 Abs. 3 TMG-E.

Die Regelungen stehen im Einklang mit den Vorgaben der E-Commerce-RL, sodass ein Verstoß gegen das in Artikel 3 festgelegte Herkunftslandprinzip ausgeschlossen ist.

Gemäß Artikel 3 Abs. 1 der E-Commerce-RL ist derjenige Mitgliedsstaat für die Einhaltung der Bestimmungen der Richtlinie verantwortlich, in dem der Diensteanbieter niedergelassen ist. Die Beaufsichtigung hat also grundsätzlich im Sinne aller Mitglieder der europäischen Gemeinschaft an der Quelle zu erfolgen. Ausgehend von diesem „Herkunftslandprinzip“ bemisst sich die Rechtslage für die Diensteanbieter grundsätzlich nach dem Recht des Mitgliedsstaates, in dem sich die Niederlassung befindet. Mithin darf ein Diensteanbieter bei der Erbringung eines Dienstes in einem weiteren Mitgliedsstaat keinen strengeren Anforderungen unterliegen als in seinem Heimatland (EuGH Urt. v. 25.10.2011 – verb. Rs. C-509/09 und C-161/10). Vorliegend ist allerdings zu berücksichtigen, dass die Richtlinie ausweis-

lich der Erwägungsgründe 7 und 8 maßgeblich zur Rechtssicherheit der Verbraucher beitragen will, indem der rechtliche Rahmen zur Sicherstellung des freien Verkehrs von Diensten der Informationsgesellschaft zwischen den Mitgliedsstaaten harmonisiert wird. Die §§ 13b ff. TMG-E überschreiten nicht die Standards der E-Commerce-RL, sondern konkretisieren deren Vorgaben. Solange aber der Gesetzgeber lediglich die Vorgaben der grundsätzlich harmonisierenden Richtlinie umsetzt, kann diesem nicht entgegenhalten werden, dass andere Mitgliedsstaaten untätig bleiben. Auf einen Ausnahmetatbestand im Sinne des Artikel 3 Abs. 4 – 6 E-Commerce-RL kommt es daher nicht mehr an.

b) Notifizierungspflicht nach der Richtlinie (EU) 2015/1535

Gemäß Artikel 5 Abs. 1 der Notifizierungspflicht-Richtlinie (RL (EU) 2015/1535) sind die Mitgliedsstaaten grundsätzlich verpflichtet, der Kommission unverzüglich jeden Entwurf einer technischen Vorschrift zu übermitteln. Technische Vorschriften in diesem Sinne umfassen dabei insbesondere auch Vorschriften, die sich auf Dienste der Informationsgesellschaft beziehen, Artikel 1 Abs. 1 lit. f) RL (EU) 2015/1535 i.V.m. Artikel 1 Abs. 1 lit. b) RL (EU) 2015/1535. Der Richtlinien-Geber möchte dadurch größtmögliche Transparenz zwischen den Mitgliedsstaaten herstellen und die Funktionsfähigkeit des Binnenmarktes durch Vorabkontrollen gewährleisten. Der vorliegende Entwurf ist daher notifizierungspflichtig und der Kommission vorab zu übermitteln.

VI. Gesetzesfolgen

1. Rechts- und Verwaltungsvereinfachung

Der Gesetzentwurf dient nicht der Rechts- und Verwaltungsvereinfachung.

2. Nachhaltigkeitsaspekte

Das grundlegende Ziel des Entwurfs besteht darin, Cybermobbing und Ehrverletzungen im Internet entgegenzutreten, um so das friedliche Zusammenleben in einer freien, offenen und demokratischen Gesellschaft zu fördern. Dieses Ziel entspricht den Leitgedanken der Bundesregierung für eine nachhaltige Entwicklung im Sinne der Deutschen Nachhaltigkeitsstrategie.[3] Denn Nachhaltigkeit zielt nach der Managementregel Nummer 10 auch auf sozialen Zusammenhalt: „Um den sozialen Zusammenhalt zu stärken und niemanden zurückzulassen, sollen Armut und sozialer Ausgrenzung soweit wie möglich vorgebeugt und Ungleichheit reduziert werden“. Dies ist auch Ziel des vorliegenden Gesetzes.

3. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

---

[3] Siehe https://www.bundesregierung.de/Content/DE/_Anlagen/Nachhaltigkeit-wiederhergestellt/2017-01-11-nachhaltigkeitsstrategie.pdf;jsessionid=BA0E790F6D3D2451C6242E42681F38D4.s1t2?__blob=publicationFile&v=20 (zuletzt abgerufen am 26.9.2017).

4. Erfüllungsaufwand

4.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Keiner.

4.2 Erfüllungsaufwand für die Wirtschaft

###

4.3 Erfüllungsaufwand der Verwaltung

###

5. Weitere Kosten

###

6. Weitere Gesetzesfolgen

Der Entwurf hat Auswirkungen von gleichstellungspolitischer Bedeutung. Er trägt dazu bei, Diskriminierungen auch wegen des Geschlechts durch ehrverletzende Inhalte im Internet wirksamer zu bekämpfen.

VII. Evaluierung

Dieses Gesetz wird spätestens drei Jahre nach Inkrafttreten evaluiert. Dabei wird die Bundesregierung in fachlich geeigneter Weise prüfen, ob und inwieweit die beabsichtigten Wirkungen auf die sozialen Netzwerke mit Blick auf ihren Umgang mit Beschwerden über Cybermobbing und andere strafbare Inhalte erreicht worden sind. Die Bundesregierung wird ferner untersuchen, wie sich der Erfüllungsaufwand für Wirtschaft und Verwaltung entwickelt hat und ob die Entwicklung in einem angemessenen Verhältnis zu den festgestellten Regelungswirkungen steht. Die Evaluierung wird die Frage nach unbeabsichtigten Nebenwirkungen sowie nach der Akzeptanz und Praktikabilität der Regelungen einschließen.

B. Besonderer Teil

Zu Artikel 1 (Änderung des Strafgesetzbuches)

Zu Nr. 1, § 185 Satz 2 StGB-E

Der Beleidigungstatbestand wird um einen Satz 2 ergänzt, welcher eine Qualifikation enthält, die den Strafrahmen von einem Jahr auf zwei Jahre anhebt, wenn eine Beleidigung im Internet begangen wird. Es wird dadurch die besondere Begehungsweise pönalisiert.

Die §§ 186 und 187 StGB enthalten bereits Qualifikationen, wenn die Delikte durch Verbreitung von Schriften begangen wurden. „Schriften“ im Sinne des Strafgesetzbuches umfassen auch Inhalte im Internet, soweit diese öffentlich abrufbar sind. Der Strafgrund der nicht mehr kontrollierbaren Gefahr für das Opfer durch die Verbreitung von Schriften ist auch bei Ehrverletzungen im Internet und der damit verbundenen weitreichenden Verbreitung ehrverletzender Inhalte erfüllt. Die Veröffentlichung über das Internet geht mit einer sehr großen Reichweite und Nachhaltigkeit einher, sodass bei Begehung der Straftat ein höherer Unrechtsgehalt verwirklicht ist. Außerdem besteht im Internet eine geringere Hemmschwelle als in der persönlichen Konfrontation und es werden andere Nutzer angeregt sich zu beteiligen („Troll Effekt“). Die Norm bedient sich nicht des Begriffs der „Schriften“, da dieser mehr als nur Inhalte im Internet umfasst und beispielsweise Schriftstücken nicht die gleiche Nachhaltigkeit und Reichweite immanent ist, die ein höheres Strafmaß für eine Beleidigung rechtfertigen könnte.

Der Anwendungsbereich der Norm wird auf Fälle der Zugänglichmachung für eine erhebliche Anzahl von Personen beschränkt. Es handelt sich dabei um ein zentrales Tatbestandsmerkmal der Norm. Dadurch werden Fälle ausgeschlossen, denen gerade nicht die besonders strafwürdige Breitenwirkung innewohnt. Dies können Beleidigungen sein, die zwar mithilfe des Internets begangen werden, jedoch lediglich für den Betroffenen selbst einsehbar sind. Eine dem Telos der Rechtsnorm widersprechende Ausuferung der Strafbarkeit wird dadurch vermieden. Eine Strafbarkeit kommt demnach in Peer to Peer-Fällen wie zum Beispiel bei der Kommunikation zwischen zwei Einzelpersonen im Rahmen von privaten Messenger Diensten, wie Facebook Messenger oder WhatsApp nicht in Betracht.

Der Begriff „Internet“ im Sinne der Norm ist weit zu verstehen und meint den weltweiten Verbund von Computern und Computernetzwerken, in dem spezielle Dienstleistungen (wie E-Mail, World Wide Web, Telefonie) angeboten werden.

Für die Definition der Begrifflichkeit des „Zugänglichmachens“ kann auf andere strafrechtliche Vorschriften zurückgegriffen werden, die diese bereits verwenden, wie beispielsweise § 184 StGB, § 130a StGB und § 131 StGB. Dafür spricht neben der begrifflichen Eignung auch die Einheitlichkeit der Rechtsordnung. Nach dieser Definition liegt ein Zugänglichmachen vor, wenn ein Inhalt in den Wahrnehmungs- oder Herrschaftsbereich des Empfängers gebracht wird, so dass die-

ser die Möglichkeit hat, von ihrem Inhalt Kenntnis zu nehmen. Für ein Zugänglichmachen selbst ist also nicht erforderlich, dass tatsächlich eine erhebliche Anzahl von Personen vom Inhalt der Beleidigung Kenntnis erlangt. Aufgrund des Tatbestandsmerkmals der Kundgabe ist es für eine Beleidigung im Internet aber letztlich trotzdem erforderlich, dass zumindest eine Person Kenntnis erlangt hat. Ein Zugänglichmachen kann beispielsweise durch das Absetzen eines Beitrags auf einem Blog oder in einem sozialen Netzwerk wie Facebook erfolgen. Ob das Teilen eines bereits veröffentlichten Beitrags ebenfalls ein Zugänglichmachen ist und sich der Teilende dadurch wegen einer Beleidigung über das Internet strafbar macht, ergibt sich bereits bei genauer Betrachtung der oben genannten Definition. Durch ein Nutzen dieser Funktion liegt erneut ein Berühren der Wahrnehmungssphäre mit der Möglichkeit zur Kenntnisnahme durch andere Nutzer vor. Der Begriff des Zugänglichmachens ist also weiter als ein bloßes „Einstellen“, welches nur den „Erstbeleidiger“ erfassen würde. Dies deckt sich auch mit dem Sinn und Zweck der Rechtsnorm. Durch einen öffentlichen Beitrag des Erstbeleidigers hätten zwar potentiell alle Nutzer weltweit von der Beleidigung Kenntnis erlangen können. Dies ist jedoch faktisch oft nicht der Fall, da ein Profil aufgrund bestimmter (Vor-) Einstellungen sozialer Netzwerke nie jeden Nutzer erreichen kann. Durch einen erneuten Beitrag tritt durch den damit initiierten Besuch des Profils des Erstbeleidigers neben die bloß potentielle Einsehbarkeit des Posts für alle eine auch tatsächlich größere Reichweite. Auch die Nachhaltigkeit der Beleidigung wird dadurch erhöht. Ein Zugänglichmachen erfordert schließlich nicht, dass ein Inhalt gewissermaßen „neu“ ist, sondern lediglich, dass die Möglichkeit einer Kenntnisnahme gegeben ist, was für einen geteilten Beitrag ebenso der Fall ist wie für den Erstbeitrag.

Zu Nr. 2, § 190 StGB wird zu § 191 StGB

Die Norm des § 191 StGB ist derzeit nicht belegt, sodass die jetzige Norm des § 190 StGB „Wahrheitsbeweis durch Strafurteil“ diesen Platz im Normgefüge einnehmen kann. Dadurch ergibt sich ein systematisch einheitlicher Regelungsort für die Pönalisierung von Cybermobbing in Form eines § 190 StGB-E. Denn der Wahrheitsbeweis durch Strafurteil entfaltet auch für Cybermobbing rechtliche Wirkung. Durch die Regelung im Rahmen eines § 191 StGB wird dies systematisch klar umgesetzt.

Zu Nr. 3, § 190 StGB-E

Eine maßgebliche Stellung innerhalb der Reform des Persönlichkeitsrechtsschutzes hat die Einführung eines neuen Straftatbestandes für schwere Ehrverletzungen im Internet (sog. Cybermobbing) im Rahmen des § 190 StGB-E. Cybermobbing kann in vielfältiger Art und Weise auftreten, wobei das Beleidigen die häufigste Form ist. Es kann jedoch auch durch die Verbreitung von Unwahrheiten (Ge-

rüchten) oder durch Ausgrenzung erfolgen.[4] Die rechtspolitische Bedeutung von Cybermobbing erwächst aus seinen erheblichen Folgen für die Opfer.[5] Jeder fünfte Betroffene von Cybermobbing hat Suizidgedanken und 14% versuchten mithilfe von Alkohol oder Tabletten die Geschehnisse zu verarbeiten.[6] Die Abgrenzung von Cybermobbing gegenüber „einfachen“ Ehrverletzungen erfolgt mithilfe mehrerer Kriterien.

Die verstärkte negative Wirkung von Cybermobbing gegenüber herkömmlichen Ehrverletzungen erwächst aus den Möglichkeiten, die das Internet und die große Verbreitung informationstechnischer Systeme bieten. Zum einen endet Cybermobbing nicht nach der Schule oder Arbeit, sondern kann rund um die Uhr erfolgen, sodass sich das Opfer den Anfeindungen kaum entziehen kann.[7] Zum anderen ist die Reichweite der verletzenden Inhalte unüberschaubar und die Verbreitungsgeschwindigkeit extrem schnell. Der Begehung von Ehrverletzungen im Internet wohnt folglich eine erhebliche Reichweite, Dauerhaftigkeit und Prangerwirkung inne.[8] Außerdem sinkt die Hemmschwelle bei den Tätern, da diese ohne Klarnamen agieren können und zum anderen dem Opfer nicht persönlich in einem Gespräch gegenübertreten, sodass empathische Reaktionen aufgrund der Wahrnehmung des Gegenübers und seiner Reaktion weniger wahrscheinlich sind.[9] Darüber hinaus unterscheidet sich Cybermobbing von einer üblichen Ehrverletzung dadurch, dass Cybermobbing nur vorliegt, wenn die Ehrverletzung derartig schwer ist, dass sie das Opfer in seiner Lebensführung beeinträchtigen kann. Beispiele für Cybermobbing können etwa die Verbreitung von verleumderischen, schwerwiegenden Gerüchten (zum Beispiel zu pädophilen Neigungen) oder massive Beleidigungen gegenüber erkennbar labilen Personen, verbunden mit der Aufforderung zum Suizid, sein. Ebenfalls unter § 190 StGB-E kann die Erstellung eines Fake-Profils (mit gefälschten Bildern und verleumderischen Textbeiträgen) in einem sozialen Netzwerk fallen, das das Opfer in einer verächtlich machenden Weise darstellt. Die Eignung zur Beeinträchtigung der Lebensgestaltung kann sich hier dadurch ergeben, dass sich nach der Lebenserfahrung weitere Nutzer im Rahmen der sozialen Vernetzung des Profils an Beleidigungen und Verleumdungen beteiligen. Dies wiederum kann eine unüberschaubare Eigendynamik entfalten, so dass sich das Opfer selbst nach der Löschung des Fake-Profils den ehrverletzenden Verstrickungen nicht entziehen kann.

Bislang kommt in Fällen von Cybermobbing eine Strafbarkeit nach verschiedenen bereits bestehenden Strafnormen in Betracht. So kann sich der Täter wegen der §§ 185 ff. StGB strafbar machen, wenn er beleidigende Inhalte oder unwahre Tatsachenbehauptungen veröffentlicht.[10] Außerdem besteht die Möglichkeit einer

---

[4] http://bgcmob.de/fileadmin/pdf/2016_05_02_Cybermobbing_2017End.pdf S. 82 (zuletzt besucht am 21.08.2017). Vgl. auch http://www.grimme-institut.de/handreichungen/pdf/mekonet-kompakt_cybermobbing.pdf (zuletzt besucht am 21.08.2017).
[5] *Cornelius*, ZRP 2014, 164, 165.
[6] http://bgcmob.de/fileadmin/pdf/2016_05_02_Cybermobbing_2017End.pdf S. 86 (zuletzt besucht am 21.08.2017).
[7] http://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/cybermobbing/ (zukletzt besucht am 21.08.2017)
[8] Cornelius, ZRP 2014, 164, 165.
[9] http://www.klicksafe.de/themen/kommunizieren/cyber-mobbing/cyber-mobbing-was-ist-das/ (zuletzt besucht am 21.08.2017)
[10] *Cornelius*, ZRP 2014, 164, 165.

Strafbarkeit wegen Nötigung gemäß § 240 StGB und Bedrohung gemäß § 241 StGB. Es kommt auch eine Strafbarkeit wegen Nachstellung gemäß § 238 Abs. 1 Nr. 2, 4, 5 StGB in Betracht, wenngleich dies teilweise im Rahmen einer teleologischen Reduktion der Rechtsnorm aufgrund der verschiedenen Zielsetzung des Täters verneint wird.[11] Denn der Mobbende will das Opfer meist psychisch „fertig machen“, während der Stalker sein Opfer in den meisten Fällen gerade nicht loswerden will, sondern dessen Nähe sucht.[12] So wird auch vertreten, über § 238 Abs. 1 Nr. 5 StGB dürfe nicht die Entscheidung des Gesetzgebers umgangen werden, der (Cyber-)Mobbing aufgrund der bereits bestehenden Rechtsnormen hiermit nicht unter Strafe stellen wollte.[13] Hält man die Norm dagegen grundsätzlich für anwendbar, ließe sich eine Vielzahl von Cybermobbingfällen unter § 238 StGB subsumieren. Denn das Tatbestandsmerkmal des Nachstellens umfasst sämtliche Handlungen, die darauf ausgerichtet sind, durch unmittelbare oder mittelbare Annäherungen an das Opfer in dessen persönlichen Lebensbereich einzugreifen und dadurch seine Handlungs- und Entschließungsfreiheit zu beeinträchtigen.[14] Solche Verhaltensweisen sind auch Cybermobbing eigen, wenngleich hinter einem klassischen Stalking meist andere Beweggründe wie etwa Zuneigung stehen mögen. Dies schließt jedoch die potentielle Tatbestandsmäßigkeit von Cybermobbinghandlungen im Sinne des § 238 StGB nicht aus. Erforderlich ist weiterhin eine Beharrlichkeit des Täters, welche erfordert, dass der Täter wiederholt handelt.[15] Nichtsdestotrotz hindert die mögliche Einschlägigkeit von § 238 StGB in bestimmten Cybermobbingfällen nicht die Schaffung eines eigenen Cybermobbingtatbestandes. Zum einen erfolgt damit eine rechtspolitische Klarstellung, die der gerade im Strafrecht erforderlichen Rechtssicherheit dient. Stalking und Cybermobbing richten sich zwar gleichfalls gegen den persönlichen Lebensbereich des Opfers, jedoch wohnt diesen ein verschiedenartiger Unrechtsgehalt inne.[16] Zum anderen ist für eine Tatbestandsmäßigkeit gemäß § 238 StGB ausreichend, dass der Täter gegenüber dem Opfer handelt. Bei Cybermobbing ergibt sich die besondere Strafwürdigkeit jedoch aufgrund der Zugänglichkeit des jeweiligen Inhalts für eine Vielzahl von Personen.

Für die Schaffung eines eigenen Straftatbestandes neben § 238 StGB spricht auch, dass in Österreich mit § 107a StGB-Ö ebenfalls ein dogmatisch vergleichbarer Stalking-Paragraph bestand und trotzdem ein eigener Cybermobbingtatbestand in Form des § 107c StGB-Ö geschaffen wurde. Auch hier war der Hintergrund, dass mithilfe des § 107a StGB-Ö zwar Teilakte von Cybermobbing verfolgt werden konnten, nicht jedoch der Unrechtsgehalt der Tat in ihrer Gesamtheit.[17]

Auch soweit durch Fälle von Cybermobbing andere Straftatbestände wie § 201a StGB oder §§ 223, 229 StGB erfüllt sein mögen, lässt dies das Bedürfnis für eine

---

[11] *Sonnen*, Kindhäuser/Neumann/Paeffgen StGB 2017, § 238 Rn. 41.
[12] *Göpfert/Siegrist*, NZA 2007, 47.
[13] *Seiler*, § 238 StGB- Analyse und Auslegung des Nachstellungstatbestandes, https://publikationen.uni-tuebingen.de/xmlui/bitstream/handle/10900/43746/pdf/238_neu_StGB.pdf?sequence=1.
[14] *Valerius*, BeckOK StGB, v. Heintschel-Heinegg 2017, 3 238 Rn. 4.
[15] *Fischer*, StGB 2016, § 238 Rn. 18.
[16] *Bieszk/Sadtler*, NJW 2007, 3382, 167.
[17] https://sscrechtswissenschaften.univie.ac.at/fileadmin/user_upload/s_rechtswissenschaft/Doktoratsstudium_PhD/Expose1/Strafrecht/Cybermobbing_-_Eine_dogmatische_Untersuchung_des____107c_StGB_idF_StGB_2015.pdf S.4.

Neuregelung nicht entfallen. Durch die derzeit bereits anwendbaren Strafnormen und deren niedrigen Strafrahmen wird dem erhöhten Unrechtsgehalt, welcher aus der Nachhaltigkeit und Perpetuierungswirkung beim Cybermobbing erwächst, nicht ausreichend Rechnung getragen.

Zu Absatz 1

Absatz 1 stellt schwere Ehrverletzungen bei Androhung einer Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe unter Strafe.

Im Rahmen § 190 StGB-E wird die weite Formulierung des „ehrverletzenden Inhalts“ verwendet. Dieser allgemeine Begriff ist als Oberbegriff für die Tatbestände der §§ 185 ff. StGB zu verstehen, um dadurch alle Alternativen von Ehrverletzungen im Internet, sei es durch Beleidigung (§ 185 Satz 2 StGB-E), üble Nachrede (§ 186 letzter Halbsatz StGB) oder Verleumdung (§ 187 letzter Halbsatz StGB) zu erfassen. All diesen Qualifikationstatbeständen gemein ist die Begehung „über das Internet“ (ggf. in der Auslegung einer „Verbreitung von Schriften“).

Einen maßgeblichen Teil des Tatbestands stellt die Anknüpfung an eine Beeinträchtigung der Lebensgestaltung des Opfers dar. Kennzeichnend für Mobbing ist im direkten Vergleich zu einer einfachen Beleidigung, dass eine psychische Belastungssituation hervorgerufen wird, die den Betroffenen besonders schwer beeinträchtigt. Der Unrechtsgehalt ist demnach gesteigert. Die Tathandlung muss geeignet sein, eine schwerwiegende Beeinträchtigung der Lebensgestaltung des Opfers herbeizuführen, sie muss diese Verhaltensänderung des Opfers aber (noch) nicht herbeigeführt haben. Im Rahmen der Beurteilung kommt dabei in erster Linie dem Grad des psychischen Drucks, den der Täter mit seinem Verhalten erzeugt, Bedeutung zu. Als Indizien können unter anderem die Intensität aber gegebenenfalls auch Häufigkeit und die beim Opfer eventuell schon eingetretene Änderung der Lebensumstände sowie psychische und körperliche Folgen Berücksichtigung finden. Die Beeinträchtigung kann, muss aber nicht durch wiederholte Schmähungen erfolgen, sodass eine wiederholte Ehrverletzung als Voraussetzung nicht erforderlich ist. Eine die Lebensgestaltung beeinträchtigende Wirkung kann beispielsweise auch durch einen einzelnen, etwa die Intimsphäre des Opfers betreffenden Beitrag erreicht werden, wenn dieser durch seinen Inhalt und seine Platzierung eine entsprechende Tiefen- und Breitenwirkung entfaltet. Die (objektive) Geeignetheit einer Ehrverletzung zur Beeinträchtigung der Lebensführung bemisst sich nach der Sensibilität einer Durchschnittsperson. Der objektivierende Beurteilungsmaßstab ist damit von besonderer Bedeutung. Der Wortlaut von § 190 Abs. 1 StGB-E orientiert sich an der Formulierung des § 238 StGB. Beide Normen stellen gleichermaßen ein Eignungsdelikt dar.[18]

Darüber hinaus genügt nicht jede potentielle oder unerhebliche lebensgestaltungsbeeinflussende Wirkung. Vielmehr muss diese schwerwiegend sein. Das ist der Fall, wenn davon ausgegangen werden kann, dass ein Durchschnittsopfer aufgrund der erfolgten Ehrverletzungen sein Alltagsverhalten ändern würde. Dies ist zu bejahen, wenn üblicherweise in dieser Situation psychologische Hilfe in An-

[18] BT-Drs. 18/9946, S. 10, 13 f.

spruch genommen würde, die Arbeits- oder Ausbildungsstätte gewechselt oder sogar gänzlich die Öffentlichkeit gemieden würde.

§ 190 StGB-E bilden wie die §§ 185 ff. StGB in ihrer bisherigen Fassung eine Schranke der grundrechtlich geschützten Meinungsfreiheit (Artikel 5 Absatz 2 GG: „Diese Rechte finden ihre Schranken in den Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutze der Jugend und in dem Recht der persönlichen Ehre."). Vermochte schon die einfache Beleidigung als Ausdruck des grundrechtlichen Persönlichkeitsschutzes (Artikel 1 Absatz 1 i.V.m. Artikel 2 Absatz 1 GG) die Meinungsfreiheit einzuschränken, so gilt dies erst recht für Fälle einer schweren Ehrverletzung im Sinne von § 190 StGB-E. In allen Fällen ist aber die überragende Bedeutung der Meinungsfreiheit zu beachten, die für die Demokratie schlechthin konstituierend ist. Ist also eine bestimmte Äußerung in Abwägung zwischen dem Persönlichkeitsschutz und der Meinungsfreiheit noch als zulässig anzusehen, dann gilt dies in gleicher Weise für herkömmliche Äußerungen (im persönlichen Gespräch oder in der Presse) wie auch für Äußerungen im Internet. Der „Vertriebskanal Internet" verschiebt die Grenze des Zulässigen bzw. Strafbaren nicht per se, sondern wirkt sich bei strafbaren Äußerungen nur strafverschärfend aus. Deshalb gilt für § 190 StGB-E auch die bekannte Rechtsprechung zu den §§ 185 ff. StGB und die ihr innewohnende Abgrenzungsdogmatik.

Sollten die jeweiligen Aussagen nicht Artikel 5 Abs. 1 GG unterfallen, wird die Abgrenzung zwischen §§ 185 Satz 2 StGB-E, 186, 187 StGB und § 190 StGB-E relevant. Die Normen stehen in einem Stufenverhältnis zueinander. Auf der ersten Stufe sind Ehrverletzungen einzuordnen, die § 185 Satz 2 StGB-E unterfallen. Dies könnte beispielsweise die Bezeichnung mit groben Schimpfworten in einem sozialen Netzwerk sein, die weder in ihrem Wortlaut noch in ihrem Kontext rechtfertigungsfähig sind. Es handelt sich hier um Beleidigungen, deren Unrechtsgehalt gegenüber § 185 Satz 1 StGB zwar durch ihre öffentliche Einsehbarkeit im Netz erhöht ist. Nichtsdestotrotz bergen diese Ehrverletzungen nicht bereits eine derart hohe Intensität für das Opfer, dass eine Ehrverletzung vorliegt, die eine Strafbarkeit im Sinne des § 190 StGB-E begründen könnte. Selbst wenn der Täter diese Beleidigung mit Personenbezug einige wenige Male in verschiedenen Kommentarspalten veröffentlicht, wird im Regelfall die für § 190 StGB-E erforderliche lebensbeeinträchtigende Wirkung zu verneinen sein. Denn ein Durchschnittsmensch wird aufgrund einer solchen, vergleichsweise „leichten" Ehrverletzung erwartungsgemäß noch nicht seine Lebensgewohnheiten ändern. Nicht ausreichend für eine Ehrverletzung im Sinne des § 190 StGB-E sind grundsätzlich selbst schwerwiegende Formalbeleidigungen. Vielmehr betrifft § 190 StGB-E nur schwere Ehrverletzungen, so dass die Norm auf einer weiteren Stufe über § 185 Satz 2 StGB-E zu verorten ist. Wann eine solche vorliegt, bestimmt sich nach dem Einzelfall und kann deshalb nicht abschließend auf eine gewisse Anzahl von Posts oder bestimmte Formalbeleidigungen festgelegt werden.

Bei schweren Ehrverletzungen im Internet besteht aufgrund der erhöhten Reichweite und Perpetuierung entsprechender Postings die ständige Konfrontierung des Opfers mit den Aussagen sowohl digital als auch in der analogen Welt, durch (immer neue) Personen, die die Ehrverletzung aufgreifen. Bereits ein einziges Pos-

ting kann von einer Vielzahl von Personen eingesehen werden und zu weiteren Posts oder Gerüchten in der analogen Welt führen. Ein Täter, der lediglich ein einzelnes Posting absetzt, welches aber einen großen Umfang hat und unter Umständen Beleidigungen mit Halbwahrheiten und Unwahrheiten kombiniert, kann nicht aufgrund der bloßen Einmaligkeit seiner Tat gegenüber einem Täter, der einzelne kurze Beleidigungen veröffentlicht, privilegiert werden. Vielmehr birgt ein solcher Inhalt ein erheblich höheres Gefährdungspotential für den Ehranspruch des Betroffenen, weil er nicht bloße, als solche erkennbare, Beleidigungen enthält, sondern auch den Anschein der Glaubwürdigkeit erweckt.

Was das Tatbestandsmerkmal der „erheblichen Anzahl von Personen“ betrifft, gelten die Ausführungen im Rahmen des § 185 S. 2 StGB-E auch für § 190 StGB-E. Es trägt der für Cybermobbing erforderlichen Reichweite und Nachhaltigkeit Rechnung.

In Hinblick auf das Zugänglichmachen der offensichtlich ehrverletzenden Inhalte kann ebenso auf die Ausführungen im Rahmen des § 185 S. 2 StGB-E verwiesen werden.

Die erhöhte Strafandrohung einer Freiheitsstrafe bis zu fünf Jahren orientiert sich an dem Strafrahmen in § 187 letzter Halbsatz StGB. So wie bereits nach bisherigem Recht eine Verleumdung im Internet unter dieses Strafmaß fällt, soll dies bei den anderen Ehrverletzungsformen in vergleichbarer Weise bestraft werden, soweit das qualifizierende Tatbestandsmerkmal der Beeinträchtigung der Lebensgestaltung erfüllt ist.

Zu Absatz 2

Tötet sich das Opfer aufgrund der zuvor erfolgten Schmähungen im digitalen Raum selbst und war diese Handlung für den Täter absehbar, dann findet die Regelung des § 190 Abs. 2 StGB-E Anwendung. Der Strafrahmen der Freiheitsstrafe ist derselbe wie bei § 190 Abs. 1 StGB-E (bis zu fünf Jahre). Abweichend hierzu wird bei einem Suizid des Mobbingopfers eine alternative Geldstrafe aufgrund der besonderen Schwere der Tat ausgeschlossen. Die damit zwingende Verhängung einer Freiheitsstrafe soll auch verdeutlichen, welche gravierenden Folgen Cybermobbing haben kann.

§ 190 Abs. 2 StGB-E ist der Regelung des § 238 Abs. 3 StGB („Stalking mit Todesfolge“) nachempfunden. Genauso wie Stalking im Extremfall zu einem Suizid des Opfers führen kann, kann dies bei Cybermobbing der Fall sein. Gerade die Nachhaltigkeit und die unkontrollierbare Weiterverbreitung ehrverletzender Äußerungen im Internet können die ohnehin schon belastenden Wirkungen schwerer Beleidigungen und Verleumdungen so verstärken, dass das Opfer keinen anderen Ausweg sehen mag, als seinem Leben ein Ende zu setzen. Diese Fälle mögen nicht häufig sein, kommen aber vor.

Dass mit dem Suizid ein vermeintlich eigenverantwortliches Handeln des Opfers zwischen die Tatbestandsverwirklichung i.S.d. § 190 Abs. 1 StGB-E und die eine strengere Sanktion auslösende Todesfolge tritt, spricht nicht gegen die Regelung

des § 190 Abs. 2 StGB-E. Es ist zulässig, den Suizid des Opfers zu berücksichtigen, da der Täter durch sein Handeln eine rechtlich verbotene Gefahr geschaffen hat und sich gerade diese realisiert hat. Das Opfer nimmt vorliegend zwar die eigentliche Tötungshandlung selbst vor, allerdings nur, weil es sich in einer durch die schweren Ehrverletzungen im Internet hervorgerufenen psychischen Notlage befindet. So lässt sich auch ein Unmittelbarkeitszusammenhang bejahen, wenn die Fähigkeit zu klaren Denkabläufen und folgerichtigem Handeln durch die zugrundeliegende Tat eingeschränkt war. Eine solche psychische Einschränkung könnte bei besonders schwerem Cybermobbing gegeben sein. Anders mag dies bei einer Selbsttötung sein, die nicht spontan im Affekt in einer psychischen Ausnahmesituation vorgenommen werden, sondern von langer Hand geplant ausgeführt wurde. Inwieweit der Suizid des Opfers motivational auf die Handlungen des Täters zurückführbar ist, muss im Einzelfall von den Gerichten festgestellt werden (vgl. zu einem parallelen Fall mit vorhergehendem Stalking BGH, Beschl. v. 15.02.2017 – 4 StR 375/16, NJW 2017, 2211).

Gegen § 190 Abs. 2 StGB-E spricht auch nicht, dass die gleichen Rechtsfolgen bereits bei entsprechender Auslegung des § 190 Abs. 1 StGB-E erzielt werden können, wenn man den Suizid als Indiz für eine besonders schwere Tatbegehung würdigt. In solchen Fällen würde wohl kaum eine bloße Geldstrafe verhängt werden. Es ist dem Gesetzgeber unbenommen, die rechtspolitische Missbilligung solcher Fälle ausdrücklich hervorzuheben und insoweit eine graduelle Abstufung verschiedener Mobbing-Fälle vorzunehmen.

Zur Nr. 4, § 194 Satz 2 StGB-E

Die Straftaten des § 190 StGB-E werden durch eine Ausnahme vom Strafantragserfordernis als Offizialdelikte ausgestaltet. Hierzu wird Satz 2, welcher diese Ausnahme bislang nur für die Opfergruppe der Opfer des Nationalsozialismus vorsieht, umformuliert und um die genannten Normen erweitert.

Dadurch, dass es sich bei den einschlägigen Vorschriften um Antragsdelikte handelt, deren Verfolgung nur auf förmlichen Strafantrag bei den Strafverfolgungsbehörden erfolgt, besteht ein erhebliches Hemmnis für eine effektive Bekämpfung von Ehrverletzungen im Internet. Die Ursache hierfür liegt vor allem darin begründet, dass viele Opfer aus Scham, wegen des damit verbundenen Aufwands und aufgrund des fehlenden Bewusstseins innerhalb der Gesellschaft für die Schwere und die Gefahren von Cybermobbing, einen Strafantrag nicht in Betracht ziehen. Dies wird auch durch die derzeit noch geringe Anzahl von Strafverfahren, Internet-Ehrverletzungen und Cybermobbing betreffend, belegt.

Zum Schutz des antragsberechtigten Angehörigen gilt auch in diesen Fällen die Regelung des § 194 Abs. 1 S. 3 StGB. So ist es den Angehörigen einer Tat nach § 190 Abs.1 StGB-E auch in diesen Fällen freigestellt, sich durch Widerspruch gegen eine strafrechtliche Verfolgung der Tat zu entscheiden. Dadurch bleibt es in deren Ermessen gestellt, ob ein Strafverfahren mit einer unter Umständen großen

Öffentlichkeit stattfinden soll. Dies dient auch dem postmortalen Persönlichkeitsschutz.

Zu Artikel 2 (Änderung der Strafprozessordnung)

Zu Nr. 1, § 158 Abs. 1 StPO

In Satz 1 wird bei der Art und Weise der Anzeigenstellung die Formulierung „elektronisch“ zur Klarstellung eingefügt, um dadurch das Stellen einer Strafanzeige zu vereinfachen. Aufgrund des technischen Fortschritts und der großen Verbreitung von elektronischen Übermittlungsgeräten erscheint eine solche Regelung geeignet das Verfahren der Strafanzeige zu beschleunigen und zu vereinfachen. Dadurch werden insbesondere bei Straftaten im Internet, welche derzeit nur zurückhaltend zur Anzeige gebracht werden, Hemmnisse in Form eines zu großen Aufwands bei der Anzeigenstellung, beseitigt.

Zu Nr. 2, § 395 StPO

Durch das Instrument der Nebenklage wird dem Verletzten die Option eingeräumt, im gerichtlichen Strafverfahren der Staatsanwaltschaft zur Seite zu treten, um seine persönlichen Interessen zu verfolgen. Das gilt für eine größere Anzahl an Straftaten, die insbesondere Sexualdelikte oder solche gegen die körperliche Unversehrtheit darstellen. Nunmehr soll dies auch für die schwere Ehrverletzung im Internet gelten. Betrachtet man die Schwere der jeweiligen Deliktsformen, aber auch das Schutzbedürfnis des jeweiligen Opfers, wäre es kaum zu vermitteln, die Fälle des § 190 StGB-E hier auszunehmen.

Zu Absatz 1

§ 395 Abs. 1 StPO ist um eine neue Nr. 1a mit einem Verweis auf § 190 Abs. 1 StGB-E zu ergänzen. Die schwere Ehrverletzung gemäß § 190 Abs. 1 StGB-E stellt ein Delikt dar, welches einen besonders schweren Unrechtsgehalt aufweist, so dass für Opfer immer eine Möglichkeit bestehen sollte, als Nebenkläger aufzutreten.

Zu Absatz 2

In § 395 Abs. 2 StPO wird eine neue Nr. 1a eingefügt, durch welche die Nebenklageberechtigung auch für die Kinder, Eltern, Geschwister, Ehegatten oder Lebenspartner eines Opfers von schweren Ehrverletzungen, der sich im Sinne des § 190 Abs. 2 StGB-E aufgrund der Tat das Leben genommen hat, normiert wird. Grundsätzlich ist nur der unmittelbar Verletzte nebenklageberechtigt und die Berechtigung geht nicht ipso iure mit dem Tode des Verletzten auf dessen Angehörige über. Um jedoch die persönlichen Interessen der Angehörigen, welche bei einem schuldhaft verursachten Suizid eines nahen Angehörigen aufgrund eines vorangegangenen Cybermobbings in erheblichem Maße betroffen sind, Rechnung zu tragen, wird die Nebenklageberechtigung auf die genannten Personen erweitert.

Zu Nr. 3, § 397a Abs. 1 StPO

Sinn und Zweck des Instruments der Bestellung eines Prozessbeistands im Sinne des § 397a StPO ist es, besonders schutzwürdige Nebenkläger zu entlasten. Die Vorschrift ist um eine Nr. 2a zu ergänzen, die auf § 395 Abs. 2 Nr. 1a StPO-E verweist. Außerdem wird in Nr. 5 der Vorschrift die Norm des § 190 Abs. 1 StGB-E eingefügt. Dadurch wird die Möglichkeit einer Bestellung eines Beistands entweder dem Opfer von Cybermobbing selbst oder im Falle eines Suizids auch den in § 395 Abs. 2 Nr. 1a StPO-E genannten Angehörigen eröffnet. Dafür spricht, dass Cybermobbing oftmals Minderjährige betrifft und außerdem eine schwerwiegende Beeinträchtigung darstellt. Aufgrund der Schwere der Tat besteht auch ein solches schutzwürdiges Interesse bei den Angehörigen im Falle eines Suizids.

Eine weitere – beabsichtigte – Folge der Ergänzung von § 397a Abs. 1 Nr. 5 StPO um den Tatbestand des § 190 Abs. 1 StGB-E ist, dass die „schwere Beleidigung im Internet“ nunmehr zu den Fällen zählt, in denen der Verletzte (das Opfer) Anspruch auf Beiordnung eines psychosozialen Prozessbegleiters hat (Verweis in § 406g Abs. 3 Satz 1 StPO). Und zwar immer dann, wenn der Verletzte bei Antragstellung das 18. Lebensjahr noch nicht vollendet hat oder seine Interessen selbst nicht ausreichend wahrnehmen kann. Dies erscheint angemessen. Nicht nur bei den bislang geregelten Fällen wie Sexualdelikten, erheblicher Körperverletzung, Geiselnahme, Raub u.ä., sondern auch im Fall des „Cybermobbing“ muss das Opfer dahingehend geschützt werden, dass es bei der Durchführung des auch seelisch belastenden Strafverfahrens kompetent und einfühlsam begleitet wird. Neben den juristischen Beistand tritt so ein psychologischer Beistand. Damit wird der Opferschutz bei schweren Persönlichkeitsrechtsverletzungen im Internet gestärkt. Der Umstand, dass es trotz offensichtlich häufiger Tatbegehung kaum Strafurteile in diesem Bereich gibt, liegt auch an der Belastung, die Opfer solcher Straftaten in dem Strafverfahren empfinden.

Zu Artikel 3 (Änderung des Telemediengesetzes)

Zu Nr. 1, § 2 TMG-E

Die gesonderte Definition für Diensteanbieter sozialer Telemedien in § 2 Nr. 1a TMG-E bezweckt eine klare Abgrenzung zu Anbietern einfacher Telemedien gemäß § 2 Nr. 1 TMG. Denn für solche Diensteanbieter sozialer Telemedien werden im Folgenden neue Pflichten normiert, welche nicht für die Anbieter einfacher Telemedien gelten.

Der Tatbestand sieht eine „Gewinnerzielungsabsicht“ vor, um so den Anwendungsbereich auf kommerzielle Telemedien zu beschränken. Eine Gewinnerzielungsabsicht liegt vor, wenn die Tätigkeit planmäßig, dauerhaft und nachhaltig erbracht wird. Dies ist bei entgeltlichen Dienstleistungen regelmäßig der Fall. Nicht entscheidend ist, ob der Dienstleistende das Entgelt unmittelbar von den Nutzern erhält oder beispielsweise in Form einer Werbefinanzierung durch Dritte.

Im Unterschied zu Anbietern einfacher Telemedien müssen die Betreiber sozialer Telemedien ihren Nutzern ermöglichen, beliebige Inhalte der Öffentlichkeit zugänglich zu machen und mit anderen Nutzern auszutauschen oder zu teilen. Dadurch werden nur Anbieter gemäß § 13c TMG verpflichtet, die internetbasiert Interaktionen und Transaktionen zwischen den Nutzern ermöglichen und erfassen. Dabei kommt es nicht darauf an, dass der Inhalt von bestimmten Personen tatsächlich wahrgenommen worden ist. Ausschlaggebend ist vielmehr, dass auf den Inhalt sowohl drahtgebunden als auch drahtlos, unabhängig von Ort oder Zeit über das Internet zugegriffen werden kann. Direktkommunikation, etwa in Form von E-Mailkommunikation o.ä., ist hingegen nicht erfasst.

Zu Nr. 2

Zu § 13a TMG-E

Eine Rechtsverordnung soll die Diensteanbieter, die wegen ihrer Bedeutung und Reichweite als Diensteanbieter sozialer Telemedien einzustufen sind, näher bestimmen. Zuständig ist aufgrund seiner Sachnähe das Bundesministerium für Wirtschaft und Energie. Die Rechtsverordnung soll nach Anhörung von Vertretern der Wissenschaft und der betroffenen Diensteanbieter im Einvernehmen mit dem Bundesministerium der Justiz und für Verbraucherschutz erlassen werden. Eine Regelung unmittelbar im Gesetz anstelle der Verordnungsermächtigung würde entweder den Gesetzestext überfrachten oder bei abstrakter Beschreibung zu Rechtsunsicherheit führen. Die nachfolgend genannten Pflichten aus §§ 13b ff. TMG-E sind durch die Diensteanbieter sozialer Telemedien spätestens einen Monat nach Inkrafttreten der Rechtsverordnung zu erfüllen. Gleiches gilt für die Befugnis aus § 14 Abs. 3 Satz 2 TMG-E.

Zu § 13b TMG-E

Durch § 13b TMG-E wird Diensteanbietern die Pflicht auferlegt, den Nutzern eine wirksame technische Möglichkeit zur Meldung rechtswidriger Inhalte bereitzustellen. Zwar gibt es solche Vorrichtungen, insbesondere in Form sog. „Meldebuttons“, schon auf freiwilliger Basis in zahlreichen Plattformen (auch bei Facebook). Die Einrichtung von „Melde-Schaltflächen“ wird nun als gesetzliche, bußgeldbewehrte Pflicht für alle relevanten Anbieter sozialer Telemedien normiert. Dies wiederum ist notwendig, weil die weitergehenden Pflichten in § 13b Abs. 1 bis 3 TMG-E (Missbrauchsvorsorge, Kennzeichnungspflicht, Hinweispflicht, Dokumentationspflicht, Entfernung der Kennzeichnung) keine klare Grundlage hätten, würde man das Meldeverfahren nicht regulieren.

Eine generelle Verpflichtung zur (technischen) Einrichtung eines Beschwerdemanagements enthält derzeit (noch) § 3 NetzDG. Um auch nach Aufhebung des NetzDG (siehe Art. 4 PRG) einen einheitlichen Umgang aller Anbieter von sozialen Telemedien mit Inhalten, die gemäß § 13b Abs. 1 TMG-E gemeldet wurden, zu erreichen, müssen klare Handlungsanweisungen gesetzlich vorgegeben werden. Die Beschränkung auf ein bloßes Melde- und Kennzeichnungsverfahren an Stelle von dezidierten Löschungspflichten (gar mit knappen Fristen versehen und mit hohen Bußgeldern bewehrt) wie im NetzDG vermeidet den berechtigten Vorwurf, der gesetzlich intendierte Persönlichkeitsrechtsschutz gegenüber ehrverletzenden Inhalten im Internet berge auch ein erhebliches Risiko des „Overblockings“. Es ist nämlich damit zu rechnen, dass ein Plattformbetreiber eher zu viel als zu wenig „verdächtige“ Inhalte löscht, um einer eigenen Haftung zu entgehen. Damit werde aber die Meinungsfreiheit, die sich gerade auch in den Interaktionen auf sozialen Medien manifestiert, unverhältnismäßig eingeschränkt. Diese Frage stellt sich erst gar nicht, wenn nicht die Diensteanbieter, sondern die Gerichte darüber zu entscheiden haben, ob ein gemeldeter Inhalt rechtswidrig und daher zu löschen ist.

Das PRG verfolgt ein alternatives Konzept: Diensteanbieter sozialer Telemedien werden dort in die Pflicht genommen, wo ihre eigene Kompetenz und zugleich ihr gefährdender Beitrag im Hinblick auf Ehrverletzungen liegt: bei der Bereitstellung von Kommunikationstechnologien. So gesehen gleichen die nunmehr normierten Pflichten nur das Risiko aus, dass die Diensteanbieter bei der technischen Ausgestaltung ihrer Geschäftsmodelle erst geschaffen haben. Weil etwa soziale Netzwerke ohne förmliche, validierte Registrierung auskommen, sorgen Auskunftspflichten für eine nachträgliche Identifizierbarkeit von Tätern. Und weil web 2.0-Technologien die Generierung von „user generated content“ ohne redaktionelle Kontrolle ermöglichen, sorgt die Kennzeichnungs- und Dokumentationspflicht für die Beweisführung in einer gerichtlichen Auseinandersetzung um die Rechtmäßigkeit inkriminierter Inhalte.

Zu Absatz 1

In einem ersten Schritt soll es den Betroffenen ermöglicht werden, dem Betreiber eines Dienstes sozialer Telemedien mithilfe geeigneter technischer Maßnahmen persönlichkeitsrechtsverletzende Inhalte zu melden. Diese gesetzliche Verpflichtung wird beispielsweise durch die Verwendung einer Melde-Schaltfläche erfüllt,

kann jedoch auch durch andere technische Verfahren befolgt werden, soweit durch diese die Meldung persönlichkeitsrechtsverletzender Inhalte gleich effektiv ist. Die Meldung muss durch den Betroffenen so vorgenommen werden können, dass es dem Diensteanbieter ermöglicht wird, auf Anhieb zu erkennen, um welchen Inhalt es sich handelt und worin die Rechtsverletzung liegt. Die Vorschrift ist bewusst technikoffen gestaltet, um der technischen Entwicklung Rechnung zu tragen. Die Diensteanbieter entscheiden im Rahmen der gesetzlichen Zwecke über das „Wie“ der Verfahrensgestaltung.

Im Übrigen hat der Diensteanbieter das Meldeverfahren so zu gestalten, dass ein Missbrauch durch automatisch agierende Computerprogramme, so genannte Bots, nicht erfolgen kann (§ 13b Abs. 1 Satz 3 TMG-E). Anderenfalls könnten sich mithilfe von Bots beispielsweise politische Gruppierungen des Meldebuttons bedienen, um in großem Umfang gegen Beiträge anderer Interessengruppen vorzugehen.

Zu Absatz 2

In einem zweiten Schritt ist der beanstandete Inhalt durch den Betreiber unverzüglich zu kennzeichnen und der Inhalt zur Beweissicherung zu dokumentieren. Dadurch wird verhindert, dass der Täter sich der zivil- oder strafrechtlichen Verfolgung durch Löschung des Inhalts entzieht. Die Kennzeichnung sollte gut sichtbar, beispielsweise durch eine farbliche Hervorhebung, erfolgen. Sie dient zusammen mit dem entsprechenden Hinweis dazu, Dritte darüber aufzuklären, dass es sich um einen potentiell strafbaren Inhalt handelt und bei einer Weiterverbreitung mit rechtlichen Konsequenzen zu rechnen ist. Dadurch wird ein Abschreckungseffekt erzielt, welcher die große Reichweite von Persönlichkeitsrechtsverletzungen im Internet beschränkt und dadurch die Folgen der Tat für das Opfer mindert. Es erfolgt keine Sperrung oder gar Löschung des Inhalts, um damit die Eingriffsintensität in die Grundrechte des Verfassers möglichst gering zu halten. Durch die bloße Kennzeichnung bleibt der Beitrag sichtbar und kann Teil des Meinungsbildungsprozesses bleiben. Denn selbst bei einer Sperrung, die ein Freischalten ermöglicht, liegt ein schwerwiegender Eingriff vor, da der Beitrag zum Zeitpunkt der Freischaltung bereits an Relevanz verloren haben kann.

Zudem ist nach § 13b Abs. 2 Satz 3 TMG-E dem Verfasser die Möglichkeit zu geben, sich gegenüber dem Diensteanbieter sozialer Telemedien zu dem beanstandeten Inhalt zu äußern und diesen gegebenenfalls unsichtbar zu schalten. In einem solchen Fall kann es sein, dass das Opfer von weiteren rechtlichen Schritten absieht und somit die Gerichte entlastet werden.

Zu Absatz 3

Die Kennzeichnung sowie die Hinweise i.S.d. § 13b Abs. 2 TMG-E sind unverzüglich zu entfernen, wenn sich die Meldung als offensichtlich unberechtigt erweist, die Meldung zurückgenommen wird oder ein Gericht die Rechtmäßigkeit des Inhalts festgestellt hat. Statt eines unwiederbringlichen Löschens, wie dies das NetzDG vorsieht, wahrt dieses Verfahren die Geltendmachung des Rechts auf rechtliches Gehör der Betroffenen gemäß Artikel 103 Abs. 1 GG.

Zu Absatz 4

Unberührt von der Einrichtung eines Meldesystems und der Entscheidung der Gerichte über die Rechtmäßigkeit des Inhalts bleibt die Verantwortlichkeit der Diensteanbieter nach § 10 TMG. Dieser begründet ein Haftungsprivileg für haftungsrechtliche und strafrechtliche Konsequenzen, solange der Betroffene keine Kenntnis von dem inkriminierten Inhalt besitzt. Das wiederum schließt aber eine Störerhaftung nicht ganz aus. Nach Vorlage einer gerichtlichen Entscheidung liegt eine Kenntnis über die Rechtswidrigkeit im Sinne des § 10 TMG vor, die auch ein Agieren des Diensteanbieters erfordert. Dies steht im Einklang mit der E-Commerce-Richtlinie.

Zu § 13c TMG-E

Zur besseren Rechtsdurchsetzung bei Persönlichkeitsrechtsverletzungen wird ein zivilrechtlicher Auskunftsanspruch für den Betroffenen begründet. Aufgrund der weitreichenden Anonymität im Internet ist es für die Täter oft möglich, Pseudonyme zu verwenden und somit für andere Nutzer unerkannt zu agieren. Dem Anbieter von sozialen Telemedien stehen teilweise die zur Rechtsdurchsetzung erforderlichen Daten wie etwa Name, Anschrift und IP-Adresse zur Verfügung.

§ 13c TMG-E schafft nunmehr einen solchen zivilrechtlichen Auskunftsanspruch bei Persönlichkeitsrechtsverletzungen. Die Geltendmachung eines solchen Anspruches war in der Vergangenheit aufgrund der Regelung des § 12 Abs. 2 TMG gehindert.

Zu Absatz 1

Aufgrund der besonderen Beeinträchtigung durch öffentlich zugängliche Persönlichkeitsrechtsverletzungen im Vergleich zu solchen, die im Rahmen privater Kommunikation erfolgen, ist der Auskunftsanspruch auf diese Fälle zu beschränken.

Erforderlich für die Herausgabe der Daten durch den Diensteanbieter ist eine richterliche Anordnung, welche vom Auskunftbegehrenden zu beantragen ist. Die Kostenlast für die richterliche Anordnung wird dem Auskunftsersuchenden auferlegt, um die Diensteanbieter durch die Vielzahl zu erwartender Auskünfte nicht unangemessen finanziell zu belasten. Der Richtervorbehalt dient auch in diesem Fall als Rechtsschutzmechanismus, mithilfe dessen Wahrheitsfindung und der Schutz individueller Rechte in Einklang gebracht werden. Dadurch soll sichergestellt werden, dass es nicht vorschnell zu einer Herausgabe von personenbezogenen Daten kommt. Eine solche richterliche Prüfung des Sachverhalts erscheint erforderlich, da insbesondere bei Sachverhalten mit Persönlichkeitsrechtsverletzungen komplexe rechtliche Abwägungen erforderlich sein können. Der Richter-

vorbehalt stärkt außerdem das Vertrauen der Bürger in rechtsstaatliche Prozesse bei Herausgabe personenbezogener Daten.

Der Anbieter soll durch die Norm nicht dazu verpflichtet werden, selbst Ermittlungen anzustellen, sondern nur solche Daten herausgeben müssen, die ihm bereits zur Verfügung stehen.

Zu Absatz 2

Absatz 2 konkretisiert die Informationen, auf die sich der Auskunftsanspruch im Einzelnen bezieht. Aus der Formulierung „insbesondere“ ergibt sich, dass diese Aufzählung nicht abschließend ist.

Die im Rahmen von § 13b Abs. 2 TMG-E angefertigte Dokumentation des Inhalts und dessen Verbreitung durch Dritte ist dem Berechtigten nach § 13c Abs. 2 Satz 2 zu übermitteln, damit diesem Beweismittel für eine etwaige (zivilrechtliche) Rechtsverfolgung zur Verfügung stehen. Dahinter steckt das mit diesem Gesetz verfolgte Konzept eines verbesserten (zivilrechtlichen) Persönlichkeitsschutzes, wonach die Rechtsverfolgung nicht bei den Plattformbetreibern, sondern vor den Gerichten stattfindet, die Betreiber aber durch technisch-organisatorische Maßnahmen jene Rechte zu schützen helfen, zu deren Gefährdung die Plattformen auch ein Stück weit beitragen.

Die Regelung eines Aufwendungsersatzanspruchs in Satz 3 dient der finanziellen Entlastung der Diensteanbieter, insbesondere, wenn es sich um aufwändige und damit kostenintensive Maßnahmen handelt.

Zu Absatz 3

Die Regelung eines Schadensersatzanspruchs bei fehlerhafter oder unterlassener Auskunft hat zum einen präventiven Charakter, indem für die Anbieter von sozialen Telemedien ein Anreiz geschaffen wird, zutreffende Auskünfte zu erteilen. Außerdem wird dem Betroffenen, der sich auf die Richtigkeit der erteilten Informationen verlassen können muss, eine Regressmöglichkeit eröffnet.

Zu Absatz 4

Um sein Recht überhaupt geltend machen zu können, muss der Nutzer über das Bestehen des Auskunftsanspruchs hinreichend deutlich informiert werden. Dies kann insbesondere durch einen Hinweis im Rahmen des Impressums, weiteren Informationspflichten oder in unmittelbarem Zusammenhang mit der Melde-Schaltfläche gemäß § 13b TMG-E erfolgen.

Zu Absatz 5

Absatz 5 trägt dem Zitiergebot gemäß Artikel 19 Abs. 1 Satz 2 GG Rechnung.

Zu § 13d TMG-E

Bereits im Rahmen des NetzDG wurde erkannt, dass eines der Hauptprobleme bei der Rechtsdurchsetzung in sozialen Netzwerken das Fehlen von verantwortlichen Ansprechpartnern bei den Betreibern der sozialen Netzwerke für Justiz, Bußgeldbehörden und Betroffene und das Fehlen einer zustellungsfähigen Adresse des Plattformbetreibers in Deutschland ist. Durch Satz 1 werden Diensteanbieter von sozialen Telemedien künftig gesetzlich verpflichtet, einen inländischen Zustellungsbevollmächtigten in Deutschland vorzuhalten und in Zivilprozessen, die gegen sie geführt werden, sowie in Bußgeldverfahren nach diesem Gesetz einschließlich des gerichtlichen Verfahrens unverzüglich zu benennen.

Die Vorschrift gilt für alle sozialen Telemedien unabhängig von ihrem Sitz im Inland oder im Ausland. Eine Beschränkung auf soziale Telemedien im Ausland, einen inländischen Zustellungsbevollmächtigen zu bestellen, wäre problematisch, weil damit auch EU-Ausländer (etwa in Irland) erfasst werden. Darin läge eine unzulässige Beschränkung der Dienstleistungsfreiheit, weil inländische soziale Telemedien nicht erfasst werden. Die Pflicht aus Satz 1 trifft deswegen alle sozialen Telemedien im In- und Ausland. Die bisher gegen soziale Telemedien geführten Zivilprozesse haben gezeigt, dass die europäischen Zustellungsmechanismen (Einschreiben mit Rückschein in Zivilverfahren) generell nicht ausreichen. Um einen wirksamen Persönlichkeitsschutz bei Ehrverletzungen im Internet zu erreichen, ist es dringend erforderlich, eine schnelle und sichere Zustellungsvariante zur Verfügung zu haben. Dies auch, weil nach der Grundkonzeption dieses Gesetzes etwaige Löschungen ehrverletzender Inhalte nur über einen gerichtlichen Rechtsschutz initiiert werden können. Ein Zustellungsbevollmächtigter im Heimatstaat des Anbieters sozialer Telemedien kann eine sichere und zügige Zustellung nicht in gleichem Maße gewährleisten, selbst wenn per Einschreiben zugestellt werden könnte.

Satz 2 erweitert die Pflicht der Diensteanbieter sozialer Telemedien, einen inländischen Ansprechpartner zu benennen, auf Strafverfahren, die gegen die Nutzer sozialer Telemedien geführt werden. Für Auskunftsersuchen nach §§ 14, 15 TMG, die die Bestands- und Nutzungsdaten der Verfasser strafrechtlich relevanter Inhalte zum Gegenstand haben, haben die Diensteanbieter eine inländische empfangsberechtigte Person zu benennen. Ziel der Regelung ist es sicherzustellen, dass die Diensteanbieter sozusagen einen „Briefkasten“ im Inland bereitstellen. Durch die Benennung eines Ansprechpartners werden daher keine zusätzlichen Auskunftspflichten begründet. Die Benennung eines Ansprechpartners verbessert jedoch die Möglichkeiten einer freiwilligen unmittelbaren Kooperation zwischen Strafverfolgungsbehörden und den Diensteanbietern. Weitere Verpflichtungen des oder rechtliche Folgen knüpfen sich an die Benennung des Empfangsberechtigten nicht; insbesondere handelt es sich nicht um einen Zustellungsbevollmächtigten im Sinne von § 132 Absatz 2 der Strafprozessordnung.

Durch die Verpflichtung der Diensteanbieter sozialer Telemedien, einen inländischen Zustellungsbevollmächtigten zu benennen, werden Ermittlungs- und Gerichtsverfahren beschleunigt. Dadurch entfällt die teils aufwändige Ermittlung des

jeweils zuständigen Zustellungsbevollmächtigten bei ausländischen Diensteanbietern. Insbesondere bei persönlichkeitsrechtsverletzenden Inhalten, die je nach Aufrufdauer im Internet auch einen eine große Verbreitung finden können, ist ein schnelles Verfahren unabdingbar.

Zu Nr. 3, § 14 Abs. 2, 3 TMG-E

§ 14 Abs. 3 bis 5 TMG werden aufgehoben. Die dort enthaltende Befugnis zur Datenweitergabe für die Durchsetzung ziviler Ansprüche wegen der Verletzung absolut geschützter Rechte aufgrund rechtswidriger Inhalte ist durch die Neuregelung des § 13c TMG-E erfasst.

Zu Absatz 2

Durch die Regelung einer Frist von einer Woche zur Auskunftserteilung in Satz 2 wird Rechtssicherheit geschaffen und eine schnellere Abwicklung von Ermittlungsverfahren als bisher garantiert.

Zu Absatz 3

Die neue Regelung soll es Dienstanbietern erlauben, strafbare Inhalte auf ihren Telemedien in Einklang mit dem Datenschutzrecht an die Strafverfolgungsbehörden zu übermitteln. Für die Übermittlung von personenbezogenen Daten ist es aufgrund des sogenannten „Zwei-Türen-Modells“ im Datenschutzrecht erforderlich, dass eine Befugnis zur Datenweitergabe besteht. Absatz 3 stellt eine solche Befugnisnorm für die Diensteanbieter für die Übermittlung von Bestandsdaten zur Strafverfolgung dar. Diese Befugnis wird in Satz 2 auf die vom Auskunftsanspruch gemäß § 13c Abs. 2 TMG-E erfassten Daten erweitert.

Zu Nr. 4, § 15 Abs. 5 Satz 4 TMG-E

Die Regelung wird an die Neufassung des § 14 TMG-E angepasst.

Zu Nr. 5, § 16 Abs. 2 Nr. 3a, b, c TMG-E

Um die Diensteanbieter von sozialen Telemedien auch tatsächlich zur Umsetzung der jeweiligen Pflichten anzuhalten, ist diese Pflicht bußgeldbewehrt ausgestaltet. Die Bußgeldtatbestände orientieren sich in der Systematik und den Rechtsfolgen weitgehend an dem bisherigen Kanon von Ordnungswidrigkeiten.

Zu Artikel 4 (Aufhebung des Netzwerkdurchsetzungsgesetzes)

Das NetzDG und das PRG können aufgrund des partiell gleichen Regelungszwecks und im Sinne einer Klarheit für den Rechtsanwender und Bürger nicht nebeneinander rechtliche Wirkung entfalten, weshalb das Netzwerkdurchsetzungsgesetz aufzuheben ist. Damit erledigen sich auch die europarechtlichen und verfassungsrechtlichen Bedenken gegen das NetzDG.

Zu Artikel 5 (Inkrafttreten)

Die Vorschrift enthält die Regelung über das Inkrafttreten dieses Gesetzes.