HateAid gGmbH

Stellungnahme

zum Entwurf des

Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität

(Drs. 19/17741)

Inhalt

A. Einleitung

Wir bedanken uns zunächst für die Möglichkeit im Rahmen der Sachverständigenanhörung noch einmal zum aktuellen Beratungsstand des Gesetzentwurfs Stellung nehmen zu können. Die Gelegenheit nehmen wir gern wahr und werden dabei vorranging auf die nach unserer Auffassung zentralen Problemstellungen eingehen. Wir stellen daher die Meldepflicht an das BKA (B.), Betreiberhaftung (C.) und Beauskunftung von Nutzungsdaten (D.) voran und wollen für die dort aufgeworfenen Problemkomplexe konkrete Lösungsvorschläge unterbreiten. Anschließend gehen wir auf die erst kürzlich in das Gesetzgebungsverfahren eingeführten Änderungen des § 15 b TMG (E.) und des Bundesmeldegesetzes (F.) ein. Im Nachgang werden die weiteren geplanten Änderungen kurz kommentiert (G.). Der Vollständigkeit halber wollen wir auch auf die bisherigen Stellungnahmen von HateAid gemeinsam mit anderen Vertretern der Zivilgesellschaft zu diesem und dem Entwurf zur Änderung des NetzDG verweisen.[1]

Wir begrüßen das gestiegene Bewusstsein dafür, dass Hassrede, Hasskriminalität und Rechtsextremismus auch im Internet als eine Bedrohung für unsere demokratische Gesellschaft und die Meinungsfreiheit wahrgenommen werden. Erkennbar wurde in den vergangenen Monaten mit Hochdruck an einem gesetzgeberischen Maßnahmenbündel zur Bekämpfung dieser Phänomene gearbeitet. Der Schwerpunkt des Entwurfs liegt im Bereich der Strafverfolgung: Es geht um höhere Strafen und auch um die Erhöhung des Verfolgungsdrucks durch Ausweitung der Befugnisse der Ermittlungsbehörden. Solche repressiven Ansätze sind zwar ein wichtiger Baustein, um Hasskriminalität und digitale Gewalt einzudämmen und sind durchaus zu begrüßen. Sie bergen aber zugleich die Gefahr, dass Freiheitsrechte mehr als erforderlich eingeschränkt werden. Hier muss genau abgewogen und nach einer Lösung gesucht werden, die Strafverfolgung vorantreibt aber die Grundrechte der Bürger*innen nicht unverhältnismäßig einschränkt. Deswegen plädieren wir dafür Freiheitsrechte und Datenschutz nicht kopflos hinten an zu stellen, sondern jetzt die Gelegenheit wahrzunehmen den Entwurf unter diesen Gesichtspunkten nachzubessern.

Die Weiterentwicklung des NetzDG und die übrigen geplanten Gesetzesänderungen sollen den freien Meinungsaustausch im Internet und unsere demokratische pluralistische Gesellschaft stärken und schützen. In diesem Sinne brauchen wir aber nicht nur Regelungen, die eine effizientere Strafverfolgung ermöglichen und die Durchsetzbarkeit zivilrechtlicher Ansprüche gewährleisten. Das Gesetzesvorhaben sollte vielmehr auch als Chance begriffen werden, Rechtsklarheit und Transparenz zu schaffen, die Rechte von Nutzer*innen sozialer Medien zu stärken und so die Akzeptanz für die Regelungen des NetzDG zu erhöhen. Diese Chance wurde trotz Nachbesserungen in wesentlichen Punkten versäumt.

Richtig ist: Eine Verschärfung des Kampfes gegen vielfach extremistisch motivierte Hasskriminalität ist dringend erforderlich. Dennoch überrascht es, dass die Evaluation des

[1] https://hateaid.org/wp-content/uploads/2020/02/Stellungnahme-ichbinhier-HateAid-NetzDG-II.pdfhttps://hateaid.org/wp-content/uploads/2020/01/Statement-aus-der-Zivilgesellschaft-zu-Novelle-NetzDG-Telemediengesetz_Strafrecht_final_17.01.2020.pdf und Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes (Stand 15.01.2020): https://hateaid.org/wp-content/uploads/2020/02/Stellungnahme-ichbinhier-HateAid-NetzDG-II.pdf.

NetzDG nicht abgewartet wurde. Es steht daher zu befürchten, dass die vorgesehenen Maßnahmen dieses und des ebenfalls vor wenigen Wochen verabschiedeten Entwurfs zur Änderung des NetzDG schon bald wieder revidiert werden müssen. Es bedarf hier statt punktueller Abhilfe eines Gesamtpakets, das die Vielfalt der Handlungsansätze miteinander vereint und möglichst umfassend ist. Einige der vorgesehenen Maßnahmen sind überfällig und werden insoweit begrüßt. Andere jedoch erscheinen höchst problematisch, während weitere Maßnahmen, die wir als Zivilgesellschaft bereits seit geraumer Zeit fordern, sich nicht in dem Entwurf wiederfinden.

B. Meldung von Inhalten an das BKA

Das Löschen schwerwiegender strafbarer Inhalte durch die Diensteanbieter darf nicht an die Stelle der Strafverfolgung treten. Darum bewerten wir die im Entwurf vorgesehene Meldepflicht für Diensteanbieter grundsätzlich positiv, bemängeln aber die konkrete Ausgestaltung. Diese sollen künftig gem. § 3 a NetzDG verpflichtet werden, als strafbar erachtete Inhalte, welche ihnen durch Nutzer*innen gemeldet wurden, gemeinsam mit der IP-Adresse und der Portnummer direkt an das BKA auszuleiten.

1. Meldepflicht, § 3a NetzDG

a) Aufnahme von § 214 StGB in Katalog der meldepflichtigen Delikte

Zu begrüßen ist die Aufnahme von § 214 StGB in Form der Bedrohung mit einem Verbrechen gegen die sexuelle Selbstbestimmung in den Katalog der meldepflichtigen Delikte. Vor allem Frauen erhalten Hasskommentare weit überwiegend mit sexualisierten Inhalten, welche häufig Vergewaltigungsandrohungen enthalten. Derartige Hasskommentare haben eine weitaus höhere Hürde durch die Betroffenen angezeigt zu werden, da die Auseinandersetzung hiermit schambelastet ist. Umso wichtiger ist es, dass Betroffene sich bei derartigen Äußerungen auf eine solide gesetzliche Grundlage berufen können.

b) Benachrichtigungsfrist der Nutzer*innen über Meldung an BKA

Kritisch sehen wir hingegen die Tatsache, dass nunmehr eine Benachrichtigung der Nutzer*innen, deren Inhalte an das BKA ausgeleitet werden, erst nach vier Wochen erfolgen soll. Die zunächst beabsichtigte Information nach zwei Wochen hielten wir gerade noch für vertretbar. Obschon die Änderung mutmaßlich an der voraussichtlichen Bearbeitungsdauer orientiert ist, erachten wir vier Wochen als zu lang um einen effektiven Rechtsschutz zu gewährleisten und regen an diesen Zeitraum zu verkürzen.

c) Speicherung von personenbezogenen Daten beim BKA

Zentrales Problem der Rechtsdurchsetzung bei Hassrede im Internet ist die Identifikation der Täter*innen. Dieses soll im Gesetzesentwurf durch die Ausgestaltung der geplanten Meldepflicht gelöst werden. So soll das BKA befähigt werden, zügig über die IP – Adresse die Identität der Täter*innen zu ermitteln und den Vorgang an die örtlich zuständige Staatsanwaltschaft abzugeben. Denn: Erfolgt die Abfrage der personenbezogenen Daten mithilfe der IP-Adresse beim Internetprovider nicht binnen sechs Tagen, sind diese gelöscht und durch die IP-Adresse kann kein Erkenntnisgewinn mehr herbeigeführt werden. Die Folge: Die Identifikation der mutmaßlichen Täter*innen ist auf diesem Wege nicht mehr möglich und eine Strafverfolgung in vielen Fällen somit obsolet.

Leider stellt die im Gesetzesentwurf dargelegte Vorgangsweise zwar die rasche Identifikation mutmaßlicher Täter*innen sicher, ist aber aus datenschutzrechtlichen Gründen höchst problematisch und stößt nicht nur bei Datenschützern sondern auch in weiten Teilen der Zivilgesellschaft auf berechtigte Kritik.

Begründung:

Die Abfrage der personenbezogenen Daten der gemeldeten Personen bei den Providern durch das BKA erfolgt automatisch und ohne, dass eine Staatsanwaltschaft jemals einen Anfangsverdacht festgestellt hat. Grundlage für die Speicherung ist alleine die juristische Einschätzung der gemeldeten Inhalte durch Mitarbeiter*innen der Social-Media Plattformen. Sie entscheiden im ersten Schritt über die mögliche strafrechtliche Relevanz der gemeldeten Inhalte und ob diese an das BKA ausgeleitet werden. Die Mitarbeiter*innen sind zum Großteil juristisch nicht vorgebildet. Eine zutreffende rechtliche Einschätzung ist ihnen nicht zuzutrauen. Hiervon werden vor allem grundrechtssensible Bereiche betroffen sein[2]. Beispielhaft sei hier die anspruchsvolle Bewertung satirischer Äußerungen oder karikaturistischer Darstellungen genannt. Trotzdem ist ihre rechtliche Beurteilung der gemeldeten Inhalte allein Maßstab für die Speicherung der personenbezogenen Daten durch das BKA. Denn Staatsanwaltschaften oder Gerichte werden nicht einbezogen. Es ist höchst bedenklich, dass das Urteil von juristischen Laien Grundlage für einen erheblichen Eingriff in die persönlichen Freiheitsrechte von vielen tausend Nutzer*innen werden soll. Sehr wahrscheinlich ist, dass hier in großem Maße Daten von Personen gespeichert werden, bei denen eine Staatsanwaltschaft keinen Anfangsverdacht feststellen würde. Der Eindruck einer Vorratsdatenspeicherung “light” liegt nahe.

Diese Vorgehensweise stellt nach unserer Auffassung einen unverhältnismäßigen Eingriff in die Freiheitsrechte der betroffenen Nutzer*innen dar und ist mit dem Grundsatz der Datensparsamkeit unvereinbar.

Um hier Freiheitsrechte ausreichend zu wahren, sollten nur Daten gespeichert werden, bei denen auch eine (spezialisierte) Staatsanwaltschaft einen Anfangsverdacht festgestellt hat.

[2]Facebook: NetzDG Transparenzbericht. Januar 2020. https://about.fb.com/wp-content/uploads/2020/01/facebook_netzdg_Januar_2020_German.pdf (Abgerufen am 05.05.2020).

Daher erachten wir statt einer Meldung direkt an das BKA eine Meldung an (spezialisierte) Staatsanwaltschaften als sinnvoll und rechtlich geboten. Diese könnten zunächst prüfen, ob tatsächlich ein Anfangsverdacht für eine Straftat vorliegt. Erst dann können eine Abrufung und Speicherung von personenbezogenen Daten mutmaßlicher Täter*innen beim BKA erfolgen. Zur Ausgestaltung machen wir in 3. einen konkreten Vorschlag angelehnt an die Praxis des Urheberrechtes. Die Bekämpfung von Hasskriminalität darf nicht als Vorwand verwendet werden, ausufernde Überwachungsrechte für eine größtmögliche Menge an Behörden zu schaffen.

2. Änderung des Bundeskriminalamtgesetzes (BKAG)

Die geplanten Änderungen des BKAG sind erforderlich, um die geplante Meldepflicht umzusetzen.

Wünschenswert wäre aber eine Klarstellung der Stellung und Funktion des BKA im Regelungskonstrukt des Gesetzentwurfs. Denn ausweislich der Begründung des Entwurfs wird das BKA im Rahmen seiner Zentralstellenfunktion gem. § 2 BKAG tätig. Eine explizite Regelung über die Verwendung der aufgrund der Meldepflicht erlangten Daten trifft er aber nicht.

Nach der derzeitigen Ausgestaltung würde das BKA also für jede einzelne Meldung die Anschlussinhaberdaten beim jeweiligen Internetprovider abfragen und somit nach Beauskunftung einen vollständigen Datensatz vorhalten. Die Befugnis hierfür ergibt sich aus dem geänderten § 10 Abs. 1 Nr. 1 BKAG. Dies ist vor allem bedenklich, weil zahlreiche Meldungen - wie in Punkt B 1. C ausgeführt - erfolgen werden, denen es an strafrechtlicher Relevanz mangelt, und dennoch umfangreiche Ermittlungen durch das BKA durchgeführt werden.

a) Meldungen ohne Anfangsverdacht

Es ist zwar zutreffend, dass es zum allgemeinen Lebensrisiko gehört, aufgrund einer Strafanzeige zu Unrecht als Beschuldigte*r geführt zu werden. Im Rahmen der Meldepflicht hingegen, erfolgen diese Meldungen massenhaft und aufgrund einer bußgeldbewährten Verpflichtung. Für Nutzer*innen sozialer Netzwerke wird so zukünftig die Wahrscheinlichkeit Subjekt von Ermittlungen des BKA zu werden ungleich höher sein als in anderen Lebensbereichen.

Dem trägt der Entwurf zur Meldepflicht bisher keine Rechnung[3]. Die Gefahr besteht, dass Nutzer*innen so von der aktiven Nutzung der Netzwerke abgehalten werden. Die Konsequenz wäre eine nicht unerhebliche Einschränkung der Meinungsfreiheit. Der Zweck des Gesetzes wird hierdurch gerade für die Bevölkerungsgruppen, deren Schutz er dient, konterkariert.

[3]Facebook: NetzDG Transparenzbericht. Januar 2020. https://about.fb.com/wp-content/uploads/2020/01/facebook_netzdg_Januar_2020_German.pdf (Abgerufen am 05.05.2020).

Hierauf wurde teilweise in der öffentlichen Diskussion von Seiten des BMJV entgegnet, dass **das BKA selbst** nach Erhalt der Meldung den Anfangsverdacht prüfen würde. Nur wenn das BKA nach Ausleitung durch die Social-Media Plattformen einen Anfangsverdacht feststellte, würde es eine Datenabfrage beim Internetprovider veranlassen.

Es bleibt allerdings unklar, woraus sich diese Befugnis herleitet. Gemäß §§ 152 Abs. 2, 160 StPO ist hierzu jedenfalls allein die Staatsanwaltschaft berufen. Gleiches gilt für die Einstellung von Ermittlungsverfahren, welche gem. §§ 153 ff., 170 StPO ebenfalls den Staatsanwaltschaften und Gerichten obliegt. Denn aus der in § 2 BKAG geregelten Zentralstellenfunktion geht lediglich die Befugnis zur **Unterstützung polizeilicher Aufgaben** hervor. Diese Unterstützung erfolgt durch das Sammeln und Auswerten von Informationen, sowie die Unterhaltung von Einrichtungen und Erhebung von Statistiken. Nach dem Wortlaut des Gesetzes umfasst die Auswertung daher lediglich eine unterstützende Aufbereitung der Daten, nicht jedoch die Übernahme staatsanwaltschaftlicher Kompetenzen. Lediglich im Rahmen von § 4 BKAG kommen dem BKA eigene Ermittlungsbefugnisse zu. Die von der Meldepflicht des § 3a NetzDG n.F. umfassten Delikte fallen aber explizit nicht unter diese Sonderregelungen.

Vor diesem Hintergrund muss also weiterhin davon ausgegangen werden, dass jede Meldung von Inhalten durch die Social-Media-Plattformen an das BKA in einer Datenabfrage und Speicherung der personenbezogenen Daten durch das BKA mündet.

b) Folgeproblem: (un)verhältnismäßige Datenverarbeitung

Es drängt sich nach alledem die Folgefrage des Speicherumfangs und -dauer der Anschlussinhaberdaten beim BKA auf. Große Teile der Zivilgesellschaft befürchten die Einrichtung einer Datenbank mit tausenden Datensätzen, welche dem BKA auch für andere Zwecke zur Verfügung stünde.

Rechtlich betrachtet ist diese auf den ersten Blick reflexhaft erscheinende Befürchtung auch teilweise berechtigt.

Unstreitig hat das BKA im Rahmen seiner Zentralstellenfunktion gemäß § 2 BKAG weitreichende Befugnisse zur Datenerhebung (§ 9, 10 BKAG). Die hierdurch erlangten Daten, werden in einem länderübergreifenden Informationsverbundsystem erfasst (§ 29 BKAG). Die Befugnisse zur Speicherung der Daten Tatverdächtiger (§ 18 BKAG) sind hierbei ebenso weitreichend wie die anderer Personen (§19 BKAG). Die personenbezogenen Daten können gemäß §§ 12, 16 BKAG einer Weiterverarbeitung für andere Zwecke und einem Datenabgleich zugeführt werden. Das heißt, dass eine Beschränkung lediglich auf Ermittlungen in Bezug auf die konkrete Meldung nicht gesetzlich vorgesehen ist. Dies bedeutet, dass alle am Informationsverbundsystem teilnehmenden Behörden auf diese Daten zu Ermittlungszwecken jederzeit zugreifen können.

Die gespeicherten Daten werden beim BKA erst gelöscht, wenn die Staatsanwaltschaften gemäß §§ 29, 30 BKAG diesem u.a. den Freispruch und die endgültige Verfahrenseinstellung mitteilen. Erst nach einer solchen Mitteilung entfällt für das BKA grundsätzlich der Anlass

einer weiteren Speicherung. In der Folge wären die betroffenen Daten zu löschen und nicht gemäß § 77 BKAG 10 Jahre vorzuhalten.

Angesichts der erwarteten Anzahl der Meldungen ist aber davon auszugehen, dass die Staatsanwaltschaften für die endgültige Bearbeitung mehrere Monate oder gar ein Jahr brauchen werden. Während dieses erheblichen Zeitraumes stehen die Daten also dem gesamten Informationsverbund des BKA zur Verfügung. Zudem sehen die §§ 18, 19 BKAG weitere Ausnahmen vor, die eine Datenverwendung auch über diesen Zeitpunkt hinaus ermöglichen.

Wann also einmal erhobene und gespeicherte Daten aus dem Prozess der Meldepflicht letztendlich beim BKA letztendlich gelöscht werden, ist für die Betroffenen nicht eindeutig ersichtlich. Letztendlich wird es ihnen selbst aufgebürdet ggf. über ein Auskunftsersuchen nach § 57 BKAG in Erfahrung zu bringen, ob eine Löschung erfolgte und diese ggf. gerichtlich zu erwirken.

3. Lösungsvorschlag: Quick Freeze

Durch eine ergänzende, bislang in keinem Gesetzentwurf vorgesehene Maßnahme, das “Quick Freeze”, würde sichergestellt, dass die Ausleitung von IP-Adressen trotz überlasteter Strafermittlungsbehörden überhaupt nutzbringend und damit geeignet sein kann. Denn nur dann ist der Grundrechtseingriff verhältnismäßig.

Anschlussinhaberdaten werden durch das Quick Freeze nur ermittelt, wenn sichergestellt ist, dass ein Anfangsverdacht besteht und die Speicherung nicht anlasslos erfolgt. Orientierung für diese Vorgangsweise bietet die gängige Praxis in Urheberrechtsverfahren: Dort ist es auf Grundlage des § 101 Abs. 1 UrhG üblich, einen sogenannten Sicherungsbeschluss zu erlassen. Dieser verpflichtet die Provider die betroffene IP-Adresse nunmehr anlassbezogen über 6 Tage hinaus zu speichern (“Quick Freeze”), bis eine richterliche Gestattung vorliegt. Wird diese nicht binnen einer Frist vorgelegt, löschen die Provider die IP-Adresse. Dies wird aus Kulanz praktiziert, ist jedoch zur Vermeidung weitergehender Ermittlungsmaßnahmen auch im Interesse der Provider. Die Folge: Es erfolgt keine Herausgabe und Speicherung der personenbezogenen Daten an Ermittlungsbehörden durch die Provider ohne, dass ein Anfangsverdacht durch ein Gericht festgestellt wird. Der Grundrechtseingriff ist verhältnismäßig.

In Anlehnung an diese Praxis könnte so auch die Ausgestaltung der Meldepflichterfolgen und eine massenhafte Speicherung von personenbezogenen Daten verhindert werden. So sollte die Möglichkeit geschaffen werden, dass die Internet-Provider auf automatisierte Anforderung des BKA die Verkehrsdaten zu einer ihnen übermittelten IP-Adresse nebst Datum und Uhrzeit einfrieren und für einen klar definierten Zeitraum vorhalten. Dies würde der zuständigen Staatsanwaltschaft die Zeit geben, die strafrechtliche Bewertung des gemeldeten Inhalts vorzunehmen und zu entscheiden, ob ein Anfangsverdacht besteht und die Verkehrsdaten tatsächlich vom Provider zu beauskunften sind. Wird dies verneint, verfügt

das BKA lediglich über anonyme und mithin wertlose IP-Adressen. Bejaht die Staatsanwaltschaft den Tatverdacht, fordert sie selbst die entsprechenden Auskünfte an.

Kann die örtliche Zuständigkeit und somit die zuständige Staatsanwaltschaft nicht bestimmt werden, wären die Fälle – und nur diese Fälle - bundesweit auf die Staatsanwaltschaften zu verteilen. Denkbar ist es dies automatisiert über entsprechende Schnittstellen anhand eines Verteilungsschlüssels zu lösen. Die Staatsanwaltschaften können das Verfahren abgeben, sobald eine örtliche Zuständigkeit bestimmbar ist. An dieser Stelle könnte man auch die Regeln zur örtlichen Zuständigkeit für im Internet begangene Äußerungsdelikte grundsätzlich überdenken. Nach unserem Dafürhalten spielt die örtliche Zuständigkeit in Fällen digitaler Gewalt eine allenfalls untergeordnete Rolle. Aus diesem Grund wäre eine Abgabe des Verfahrens nach erfolgter Abschlussentscheidung unschädlich, sodass das Verfahren nicht künstlich gestückelt werden muss.

Die Daten sollten für wenigstens drei Monate eingefroren werden, um eine Bearbeitung durch die Staatsanwaltschaft in der Zwischenzeit sicherzustellen.

Die rechtssichere Umsetzung eines Quick Freeze erfordert eine gesetzliche geregelte Verpflichtung der Provider, bei Benachrichtigung durch das BKA die IP – Adresse vorzuhalten und letztendlich die Anschlussdaten zu beauskunften.

Diese Vorgehensweise mag mit einem gewissen Mehraufwand verbunden sein. Diesen Mehraufwand sollte unser Rechtsstaat jedoch aufgrund der Relevanz für die Rechte der Betroffenen nicht scheuen.

c) Betreiberhaftung

Darüber hinaus ist die Verbesserung der Rechtsdurchsetzung insgesamt - losgelöst von den Katalogstraftaten wie §§ 86a, 130 StGB, welche die Meldepflicht betreffen - dringend erforderlich. Die Rechtsdurchsetzung scheitert häufig daran, dass den Auskunftsersuchen der Ermittlungsbehörden durch die Plattformen nicht nachgekommen wird. Agieren Täter*innen unter Pseudonymen, sind die Ermittlungsbehörden hierauf jedoch angewiesen. Die Beauskunftung, erfolgt höchst uneinheitlich und erscheint willkürlich. Die Plattformen beauskunften Anfragen der Ermittlungsbehörden nach eigenem Ermessen und “Einzelfallprüfung” abhängig von unternehmensinternen Richtlinien. Nationale Rechtssätze spielen hierfür eine untergeordnete Rolle. Die Beauskunftung erfolgt in erster Linie nach Gutdünken der Konzerne. Ermittlungsbehörden werden unter diesen Voraussetzungen darauf verwiesen, dass die angeforderten Daten im Ausland gespeichert seien und müssen dann ein Rechtshilfeersuchen anstrengen. Dieses verläuft in der überwiegenden Zahl der Fälle ergebnislos oder wird erst nach Monaten beantwortet. Das geltende Herkunftslandprinzip hat zur Folge, dass sich Plattformen stets auf “rechtliche Risiken” im Verhältnis zu Ihren Nutzer*innen berufen können, wenn es darum geht im Ausland gespeicherte Daten zu beauskunften. Es ist zu befürchten, dass selbst eine national geregelte Auskunftspflicht durch die Plattformen angezweifelt wird. Teilweise wird die Auffassung vertreten, dass aufgrund

einer nationalen Norm bereits keine Verpflichtung zur Herausgabe von Daten aus dem Ausland bestehen kann oder europäische Regelungen dem sogar entgegenstehen.

Im Ergebnis läuft der Gesetzgeber daher aktuell Gefahr gut gemeinte und grundsätzlich begrüßenswerte Änderungen zu schaffen, die praktisch ins Leere laufen.

Aus den genannten Gründen sollte für Telemedien zwingend das **Marktortprinzip** eingeführt werden. Hierdurch würden die Social Media Plattformen verpflichtet Daten der inländischen Geschäftstätigkeit auch in Deutschland zu speichern. Allein hierdurch kann sichergestellt werden, dass die Beantwortung von Anfragen der Ermittlungsbehörden aus Deutschland heraus erfolgen kann. Hierfür hat sich bereits der Antrag der Bundesländer Hamburg und Bremen zur Entschließung des Bundesrates: „Effektivierung von Auskunftserteilungen durch ausländische Anbieter sozialer Netzwerke“ vom 4.2.2020 (https://www.bundesrat.de/SharedDocs/drucksachen/2020/0001-0100/65-20.pdf;jsessionid=BEDBB45B600F460C8FE3340B3D68FB53.2_cid391?__blob=publicationFile&v=1)) ausgesprochen.

Der Anspruch auf Auskunftserteilung durch die Provider sollte in dieser Form gesetzlich geregelt werden.

d) Beauskunftung von Bestands- und Nutzungsdaten

Nicht nur das materielle Strafrecht muss den Anforderungen des digitalen Zeitalters angepasst werden. Um eine effektive Strafverfolgung zu gewährleisten, sind die vorgesehenen Änderungen der §§ 100g, 100j, 101a und 101b StPO unerlässlich und werden von uns befürwortet. Ob die Diensteanbieter künftig zuverlässiger mit den Ermittlungsbehörden kooperieren werden, bleibt abzuwarten. Bislang erfolgt eine Beauskunftung mangels Verpflichtung erst, wenn interne Richtlinien dies erlauben - sie beschränken sich jedoch meist auf Offizialdelikte wie Volksverhetzung oder das Zeigen von verfassungsfeindlichen Symbolen. Dieser Missstand sollte durch die Aufnahme von Telemediendiensten in § 100j StPO mit Blick auf die Auskunftsverpflichtung nach § 100j Abs. 5 StPO zumindest in Bezug auf die Bestands- und Nutzungsdaten der Vergangenheit angehören.

Die Ergänzung um “Nutzungsdaten” und “Telemediendienste” erscheint daher im Sinne einer effektiven Rechtsdurchsetzung konsequent und erforderlich.

Vereinheitlichung der zu beauskunftenden Daten

Nachdem die Plattformen bislang Auskünfte praktisch nicht erteilt haben, liegen leider keine Erkenntnisse darüber vor, welche Bestands- und Nutzungsdaten diese tatsächlich erheben und speichern. Es ist also nicht nachvollziehbar, ob im Fall einer Auskunft tatsächlich alle vorhandenen Daten mitgeteilt werden und ob mit deren Hilfe die Identifizierung der Täter*innen gelingen kann. Da IP-Adressen, gleich ob des Uploads oder letzten Zugriffs auf den Account nur wenige Tage gespeichert werden, wäre eine Vereinheitlichung der zu erhebenden Daten im Sinne der Rechtsdurchsetzung.

Bislang sind viele der Nutzungsdaten, die an Strafverfolgungsbehörden zur Identifikation der Täter*innen herausgegeben werden könnten, in der Praxis wertlos:

Es ist nicht erforderlich, dass sich Nutzer*innen bei der Registrierung auf den Plattformen zwangsläufig mit ihren zutreffenden Personalien anmelden. Die Anmeldeformulare der großen Plattformen verlangen zwar die Angabe von Vor- und Nachnamen, Geburtstag und Geschlecht. Verifiziert werden müssen diese Angaben allerdings nicht. Weiter sind eine Handynummer oder eine E-Mail-Adresse anzugeben. Es kommt sogar vor, dass gar kein Vor- und/oder Zuname vorliegt oder dies zumindest von den Plattformbetreiber*innen so angegeben wird.

Wurde eine E-Mail-Adresse angegeben, dann handelt es sich häufig um kostenfreie Webmail-Accounts. Selbst wenn die Mail-Provider bereit sind, den bei der Anmeldung hinterlegten Namen herauszugeben, ist eine Identifizierung noch immer nicht sichergestellt. Die Anbieter kostenfreier Webmail-Angebote unterliegen unseres Wissens nicht den Pflichten nach § 111 TKG. Somit ist es nicht nur einfach, unter Angabe von falschen persönlichen Daten an einen E-Mail-Account zu gelangen. Mit dieser E-Mail-Adresse kann dann auch ein Account bei den Plattformen angelegt werden, dessen Inhaber*in anhand dieser Daten praktisch nicht zurückverfolgt werden kann.

Beauskunften die Plattformen die IP-Adressen und Zeitpunkte des Zugriffs oder Uploads, wird hieraus in der Regel kein Erkenntnisgewinn zu ziehen sein, wenn dieser mehr als sechs bis sieben Tage zurückliegt. Zur Täteridentifizierung kann die IP-Adresse nur verhelfen, wenn sie so zügig beauskunftet wird, dass im nächsten Schritt vom Internet-Zugangsprovider die zugehörigen Verkehrsdaten angefordert werden können. Das gesamte Prozedere wird häufig so viel Zeit in Anspruch nehmen, dass die benötigten Daten von den Zugangsprovidern gar nicht mehr herausgegeben werden können. Denn wegen des verfassungsrechtlich gebotenen und deswegen nicht in Zweifel zu ziehenden Verbots der anlassunabhängigen Vorratsdatenspeicherung werden die IP-Adressen und die weiteren zugehörigen Verkehrsdaten bei den Providern nur maximal eine Woche vorgehalten.

Wenn allerdings tatsächlich eine Handynummer hinterlegt wurde, bestehen aufgrund der Identitätsprüfungspflicht nach § 111 TKG gute Aussichten, dass die den Account nutzende Person ermittelt werden kann. Diese wird von einigen Plattformbetreibern zur Wiederherstellung des Accounts oder im Rahmen der Zwei-Faktor-Authentifizierung ohnehin schon erhoben.

Es muss daher sichergestellt werden, dass die Identität der Täter*innen auch ermittelt werden kann, wenn Auskünfte an die Strafverfolgungsbehörden durch die Social Media Plattformen erteilt werden.

Denkbar sind an dieser Stelle verschiedene (kumulative) Lösungsansätze:

- Aktuell wird über eine Authentifizierungspflicht für Nutzer*innen Sozialer Medien diskutiert. Angestoßen wird diese Debatte derzeit von den Bundesländern Niedersachsen und Mecklenburg-Vorpommern über einen in den Bundesrat eingebrachten Gesetzesantrag. Eine

solche Identitätsprüfungspflicht sehen wir aus datenschutzrechtlichen und anderen Gründen allerdings sehr kritisch. Bislang schreibt das Gesetz den Telemediendiensteanbietern aus gutem Grunde ausdrücklich vor, dass sie eine anonyme oder unter Pseudonym erfolgende Nutzung ermöglichen müssen. Der Gedanke an die persönlichen Daten aller Nutzer*innen in der Hand der Plattformbetreiber bereitet ein großes Unwohlsein. Denn diese können sodann mit einer Unmenge von Daten zum Nutzungsverhalten der nun vom Unternehmen identifizierbaren Nutzer*innen verknüpft und gezielt für Microtargeting genutzt werden. Es ist außerdem zu befürchten, dass durch eine Identitätsprüfungspflicht auch Menschen aus den Sozialen Medien ferngehalten werden, die nicht etwa aus unlauteren Motiven, sondern aus Gründen des Selbstschutzes vermeiden möchten, ihre korrekten persönlichen Daten anzugeben.

● Uneingeschränkt abzulehnen ist eine Klarnamenpflicht in dem Sinne, dass die Nutzer*innen mit ihrem authentischen Namen auf der Plattform auftreten müssen. Ohne Klarnamen im Netz aktiv sein zu können, ist für viele Internetnutzer*innen immens wichtig. Dies gilt vor allem für diejenigen, die in besonderem Maße gefährdet sind, zur Zielscheibe von Anfeindungen zu werden – sei es wegen ihrer Herkunft, ihrer Religion, ihres Geschlechts, ihrer sexuellen Ausrichtung oder ihrer politischen Haltung.

● Eine vergleichsweise einfache, weit weniger eingriffsintensive Maßnahme mit hohem Nutzen könnte es dem gegenüber sein, wenn die Plattformbetreiber bei Anmeldung zwingend die Mobilfunknummer der Nutzer*innen erfragen und sie verifizieren müssten. Die Handynummer wäre bei der Anmeldung über einen per SMS zugesandten Code zu bestätigen. Diese Maßnahme würde es ermöglichen, dass Bestandsdaten erhoben und beauskunftet werden, die relativ zuverlässig weitere Nachforschungen zu der dahinterstehenden Person durch entsprechende Auskunftsersuche bei den Telekommunikationsdiensteanbietern ermöglichen. Die Zulässigkeit der in § 111 TKG geregelten Identifizierungspflicht, welche dem Missbrauch von anonym erworbenen “Wegwerf-SIM-Karten” vor allem im Bereich der Rauschgift-, organisierten Kriminalität und Terrorismus entsprungen ist, hat der EGMR jüngst bestätigt (Urt. v. 30.01.2020, Az. 50001/12).

● Soll weiterhin gleichermaßen eine Registrierung unter Angabe einer E-Mail-Adresse möglich sein, so wäre es erforderlich, dass künftig auch Webmail-Anbieter verpflichtet werden, eine Verifizierung der angegebenen persönlichen Daten vorzunehmen. Für das Prozedere und die sich hieraus ergebenden Ermittlungsmöglichkeiten gilt das für die Authentifizierung mittels Mobilfunknummer Gesagte.

● Weiterhin sehen wir Handlungsbedarf bei der Schaffung beschleunigter Auskunftsverfahren für IP-Adressen. Es muss verhindert werden, dass diese durch Zeitablauf wertlos werden. Hier bietet es sich an, sich für eine Lösung am Urheberrecht zu orientieren. Insofern wird auf die Ausführungen unter B. 3. verwiesen.

e) § 15 b TMG n.F.

Wir begrüßen die Neugestaltung des § 15 b TMG. Die Befugnis zur Beauskunftung u.a. von Passwörtern war im Referentenentwurf etwas unglücklich untergebracht und begegnete daher viel öffentlicher Kritik. Die Neufassung der Regelung erscheint geeignet, die Akzeptanz zu erhöhen. Die Orientierung an den Katalogstraftaten des § 111 b StPO und Einfügung des Richtervorbehalts stehen nunmehr nachvollziehbar im Einklang mit den bereits jetzt im Strafprozessrecht geltenden Vorschriften.

Der konkrete Nutzen ist jedoch weiterhin unklar. Dies gilt vor allem vor dem Hintergrund der im Einklang mit der jüngst im Zuge der DSGVO durch den dortigen Artikel Art. 32 Abs. 1 lit. a DSGVO eingeführten Verpflichtung zur verschlüsselten Speicherung von Passwörtern. Folglich widerspräche eine Speicherung von Passwörtern im Klartext und ungehasht nicht nur elementaren Regeln der IT-Sicherheit, sondern auch geltendem Recht. Eine Änderung der DSGVO ist jedenfalls zum aktuellen Zeitpunkt nicht angedacht, sodass sich die Frage aufdrängt, welchen Mehrwert die Weitergabe verschlüsselter Passwörter Strafverfolgungsbehörden überhaupt erbringen kann.

f) § 51 Bundesmeldegesetz n.F.

Zu begrüßen ist die jüngst in das Gesetzgebungsvorhaben aufgenommene Konkretisierung der schutzwürdigen Interessen als Voraussetzung zur Erlangung einer Melderegistersperre. Auch wenn es sich hierbei in erster Linie um eine Klarstellung handelt, ist diese dringend notwendig und geeignet zum Schutz vieler Betroffener beizutragen. Betroffenen ist nachvollziehbar daran gelegen zu verhindern, dass Täter*innen Kenntnis von Ihrem Wohnsitz erlangen. Das sogenannte “Doxxing”, also die Veröffentlichung der Privatanschrift zum Zweck der Einschüchterung, hat nach unserer Erfahrung in der Beratung im vergangenen Jahr besorgniserregend zugenommen. Neben der enormen psychischen Belastung, die mit dem Verlust des Zuhauses als privatem Schutzraum einhergeht, werden Betroffene hierdurch vor weitere besondere Herausforderungen gestellt, die zeit- und kostenintensiv sind. So erleben sie es häufig, dass die durch Hasskriminalität geschaffene Bedrohungslage von Behörden nicht mit der notwendigen Ernsthaftigkeit behandelt und nicht als konkrete Bedrohungslage wahrgenommen und eingeschätzt wird. Hier mangelt es offenbar ebenso wie im Bereich der Strafverfolgung an der erforderlichen Weiterbildung und Sensibilisierung im öffentlichen Dienst. Dies gilt vor allem für die durch digitale Gewalt geschaffene Bedrohungslage, die häufig unterschätzt wird. Dass hiervon eine reale analoge Gefahr ausgehen kann, haben die Tötung des Kasseler Regierungschefs Walter Lübcke und die Attentate von Halle und Hanau bewiesen.

Vor diesem Hintergrund begrüßen wir die Konkretisierung. Sie erscheint geeignet, um eine einheitliche Rechtsanwendung zu gewährleisten und kann so einen Beitrag zum Opferschutz leisten.

Zu begrüßen ist vor allem die ausdrückliche Einbeziehung des Schutzes vor Beleidigung als schutzwürdiges Interesse. Die hieraus hervorgehende Würdigung der Bedeutung und Auswirkungen von Beleidigungen ist ein Novum. Vor allem im Internet begangene Beleidigungen werden bislang meist als Einzelfall und Bagatelle abgetan. Dies verkennt jedoch die gezielte Nutzung der Beleidigung vor allem rechtsextremistischer Gruppierungen im Netz zum Zweck der Einschüchterung und Verdrängung aus dem öffentlichen Diskurs.[4] Die Bedeutung des Internets für die gesellschaftliche Teilhabe und die Organisiertheit der Täter*innen, finden nach unserer Erfahrung nur in seltenen Ausnahmefällen überhaupt bei der Bewertung der schutzwürdigen Interessen Berücksichtigung. Weitaus häufiger wird Betroffenen von Strafverfolgungsbehörden und Mitarbeiter*innen von Meldebehörden geraten, sich im Netz nicht kontrovers zu äußern oder sich gar "abzumelden". Dies führt dazu, dass Aktivist*innen, Journalist*innen und (Lokal-)Politiker*innen sich notgedrungen aus dem Internet oder sogar von Ihren Positionen zurückziehen, wenn der Hass überhand nimmt und die Gefahr für die Familie unhaltbar wird.[5]

Es erscheint aus diesem Grund naheliegend den Zusammenhang zu ehrenamtlicher oder beruflicher Tätigkeit bei der Beurteilung der Gewährung von Meldesperren herauszustellen. Zu befürchten ist jedoch, dass hierdurch hervorgerufene Abgrenzungsschwierigkeiten zu ungerechten Ergebnissen führen. Nach dem Wortlaut wäre wohl das Eintreten für gesellschaftliche Themen in einem privaten Blog oder durch Teilnahme an Demonstrationen nicht als "ehrenamtliche Tätigkeit" erfasst. Aus der Beratungspraxis von HateAid geht aber hervor, dass solche Aktivist*innen jedoch ebenso häufig von (organisierter) Hasskriminalität betroffen sind wie bspw. (Kommunal-)Politiker*innen.

g) Sonstige Änderungen und Reformvorschläge

"Kleiner Zeugenschutz" für Betroffene von Digitaler Gewalt

Eine bisher nicht vorgesehene Neuregelung, welche HateAid aber dringend zum Schutze der Betroffenen fordert, ist die Vereinfachung des Zeugenschutzes in Verfahren wegen Hasskriminalität. Wenn Betroffene von Digitaler Gewalt Strafantrag oder Strafanzeige gegen die Täter*innen erstatten wollen, werden sie oftmals dazu verpflichtet die eigene private Anschrift anzugeben. Die Anwälte der mutmaßlichen Täter*innen können dann Akteneinsicht beantragen und die Anschrift der Betroffenen ermitteln. Nicht nur dass Täter*innen dann über ihre Privatadresse verfügen, hält viele Angegriffene in der Folge davon ab, Anzeige zu erstatten. Dahinter steht vor allem auch die Angst davor, dass die eigene Adresse im Internet veröffentlicht werden könnte. Tatsächlich beobachten wir in der Beratungspraxis von HateAid derzeit eine signifikante Zunahme dieser Form von digitaler Gewalt. Nicht selten schlägt die

[4] J.Ebner, J.Davey: The fringe insurgency. Connectivity, convergence and mainstreaming of the extreme right. Institute for Strategic Dialogue, London, 2017. https://www.isdglobal.org/wp-content/uploads/2017/10/The-Fringe-Insurgency-221017.pdf (Abgerufen am 04.05.2020).

[5] Erhardt, Christian: Kommunalpolitiker: Bedrohungen sind an der Tagesordnung. Repräsentative Befragung von 2494 Bürgermeister*innen durch Kommunal. https://kommunal.de/kommunalpolitiker-umfrage-2020 (Abgerufen am 04.05.2020).

Veröffentlichung der privaten Daten in eine analoge Belästigung durch Postsendungen oder Aufsuchen der Anschrift und Markierung des Hauses oder der Wohnung durch Kot oder Schmierereien um.

Normalerweise beginnt gemäß § 68 Abs. 1 StPO die Vernehmung von Zeug*innen mit der Abfrage des Namens, Alters, Berufes und Wohnort. Die Angabe dieser persönlichen Daten kann aber mitunter sehr heikel sein. Im ohnehin grundsätzlich öffentlichen Strafverfahren können nicht zuletzt mit der oder dem Beschuldigten, Personen anwesend sein, die potenziell ein Interesse daran haben können, sich an den Zeug*innen zu rächen. Die im Verfahren veröffentlichten Informationen, insbesondere die Preisgabe des Wohnortes können Racheaktionen extrem vereinfachen. Vielfach sind Zeug*innen dadurch stark eingeschüchtert. Um der Gefährdungssituation Rechnung zu tragen, sieht § 68 StPO im Absatz 2 die Möglichkeit vor, wenn eine Bedrohung befürchtet wird, die Angabe über den Wohnort durch die Angabe einer sonstigen ladungsfähigen Adresse zu ersetzen. Absatz 3 sieht sogar vor, dass, sofern Leib und Leben in Gefahr sind, gänzlich von der Angabe von Daten zur Person abgesehen werden kann. Ob die entsprechenden Daten preisgegeben werden müssen, liegt im Ermessen des vernehmenden Gerichts. Dieses muss das Schutzinteresse der Zeug*innen mit dem Aufklärungs-, Informations- und Verteidigungsinteresse in Ausgleich bringen. In Zeiten, in denen Menschen, die öffentlich unsere Demokratie und Grundrechte verteidigen, mit dem Tod bedroht sind, wie sich im Fall Lübke[6] gezeigt hat, können wir uns nur dafür aussprechen diesen sogenannten „Kleinen Zeugenschutz“ in Gerichtsverfahren hinsichtlich Digitaler Gewalt grundsätzlich in Betracht zu ziehen und bundesweit zu vereinheitlichen.

1. Änderung des Strafgesetzbuchs

Der Entwurf misst einer effektiven Strafverfolgung bei der Bekämpfung von Digitaler Gewalt und digitaler Gewalt große Bedeutung zu. Grundsätzlich begrüßen wir die Anpassung des Strafrechts an die großen Herausforderungen unserer Zeit durch Digitale Gewalt und Rechtsextremismus. Die geplanten Änderungen zeigen deutlich: Der Gesetzgeber und wir alle als Gesellschaft wollen nicht tatenlos zusehen, wenn aus menschenverachtenden und demokratiefeindlichen Gründen verbale und tätliche Gewalt verübt wird.

Entscheidend für den Erfolg des geplanten Gesetzes wird jedoch nicht bloß die Einführung und Verschärfung von Straftatbeständen, sondern vor allem auch deren **Durchsetzbarkeit** sein. Neben der Schaffung entsprechender Ressourcen und Kompetenzen in der Justiz, müssen also auch hierfür gesetzliche Rahmenbedingungen geschaffen werden, die auch im Internet greifen.

Im Einzelnen bewerten wir die geplanten Änderungen als überwiegend positiv - allerdings nicht durchgehend.

[6]Der Fall Walter Lübcke: ”Abgelegt unter Volksverräter.”. Frankfurter Rundschau. https://www.fr.de/rhein-main/abgelegt-unter-volksverraeter-12360274.html (10.04.2020).

§ 46 Absatz 2 StGB

Antisemitische Motive spielen bei Digitaler Gewalt eine große Rolle. Die Aufnahme des Antisemitismus als hervorgehobenen, konkreten Strafschärfungsgrund zum Zwecke der "Klarstellung und Bekräftigung der bereits jetzt geltenden Rechtslage" erscheint uns dennoch nicht notwendig.

Antisemitismus findet nach der aktuell gültigen Fassung des § 46 StGB als "sonstiger menschenverachtender Beweggrund" strafschärfend Berücksichtigung. Menschenverachtend sind solche Motive, die einzelne Gruppen von Menschen mit Blick auf bestimmte Merkmale wie die Religionszugehörigkeit, die sexuelle Orientierung, das Geschlecht, die Herkunft oder Menschen im Allgemeinen als minderwertig oder verächtlich ansehen. Bislang knüpft § 46 StGB für die Strafzumessung beispielhaft an die in Abs. 2 S. 2 der Vorschrift aufgelisteten, allgemein und abstrakt gefassten Kriterien an. Die Nennung speziell antisemitischer Motive widerspräche dieser Systematik. Auch verkennt seine Aufnahme als konkreter, strafschärfender Umstand zum aktuellen Zeitpunkt nicht nur, dass Antisemitismus schon seit geraumer Zeit ein Problem ist. Sie missachtet auch weitere Motive gruppenbezogener Menschenfeindlichkeit. Angehörige anderer Minderheiten mit Diskriminierungserfahrung werden nicht explizit benannt. Die Ergänzung des Motivs scheint in erster Linie symbolischer Natur zu sein - wichtiger wären praxisrelevante Maßnahmen, die mit einer solchen Symbolpolitik einhergehen wie die finanzielle Unterstützung von Betroffenen oder spezialisierten Beratungsstellen.

§ 115 StGB

Nicht nur im Netz ist die Hemmschwelle für respektloses und aggressives Auftreten gesunken; die durch Hass im Netz zum Ausdruck kommende Haltung beeinflusst das gesellschaftliche Klima und findet Einzug auch in unsere analoge Welt. Darum halten wir es für sachgerecht und notwendig, Mitarbeiter*innen eines ärztlichen Notdienstes oder einer Notaufnahme ebenso wie die bereits in § 115 Abs. 3 StGB genannten hilfeleistenden Berufsgruppen den Vollstreckungsbeamten gleichzustellen, soweit in § 115 i.V.m. §§ 113 und 114 StGB Widerstandshandlungen und tätliche Angriffe unter Strafe gestellt sind.

§§ 126 und 140 StGB

Wir befürworten auch die Ausweitung der Strafbarkeit nach § 126 StGB auf die friedenstörende Androhung gefährlicher Körperverletzungen. Hierdurch wird eine Strafbarkeitslücke geschlossen. Ebenso zu begrüßen ist der Ansatz, nicht nur die Billigung bereits begangener, sondern möglicher künftiger Gewalt- und Sexualdelikte nach § 140 StGB unter Strafe zu stellen. Vor allem weiblichen Nutzerinnen wird in den sozialen Medien häufig die Vergewaltigung gewünscht. Diese Form massiver Herabwürdigung und digitaler Gewalt war bislang strafrechtlich nur schwer greifbar. Es läge nebenbei bemerkt nahe, derartige Delikte auch in den Katalog des § 126 Abs. 1 StGB aufzunehmen.

§§ 185 ff. StGB (Beleidigungsdelikte)

Die Schaffung des weiteren Qualifikationstatbestandes der öffentlich oder durch Schriften - also auch im Internet - verbreiteten Beleidigung in § 185 StGB ist überfällig. Sie berührt das Phänomen Hate Speech im Kern. Für Nutzer*innen, die sich in den sozialen Medien zu Wort melden und sich menschenfeindlichen Narrativen entgegenstellen, sind massive Beleidigungen an der Tagesordnung. Ehrverletzungen finden im Netz einen großen Resonanzraum und verbreiten sich außerordentlich schnell. Sie wiegen damit für die Betroffenen ungleich schwerer als solche Beleidigungen, die analog in kleinerem Rahmen geäußert werden. Auf eine Abschreckungswirkung der Verschärfung des strafrechtlichen Ehrschutzes darf gehofft werden; diese wird aber nur dann von Dauer sein, wenn die zuständigen Strafverfolgungsbehörden gegen diese Delikte mit aller Konsequenz vorgehen und sich nicht allein auf Offizialdelikte fokussieren.

Wenn auch der Entwurf eine konsequentere strafrechtliche Ahndung von Hasskriminalität intendiert, ist in der Praxis der Strafverfolgung festzustellen, dass bislang in Bezug auf die Beleidigungsdelikte faktisch keine Strafverfolgung stattfindet. Zu befürchten ist, dass sich dies auch nach den vorgesehenen Gesetzesänderungen nicht grundlegend ändert. Der Fokus der angestrebten Reformen wird insbesondere durch die vorgesehene Meldepflicht nach § 3a NetzDG-E auf Morddrohungen und Volksverhetzungen gelegt. Dieser Ansatz verkennt, dass die fatale Verdrängung von Nutzer*innen aus dem öffentlichen Diskurs (Silencing)[7] auch und sogar vor allem den Beleidigungsdelikten geschuldet ist. Diese werden von einschlägigen Gruppierungen systematisch benutzt, um Nutzer*innen einzuschüchtern, sie mundtot zu machen und so den Eindruck einer gefühlten Meinungshoheit zu vermitteln. Wissenschaftliche Studien[8], aber auch die Zahlen des BKA[9] belegen, dass dieses gezielte Vorgehen vor allem aus dem rechtsextremen Spektrum kommt. Die Täter*innen machen sich die Defizite bei der Strafverfolgung hierbei bewusst zunutze. In einschlägigen Handbüchern, welche im Internet zur Organisation von sog. Hatestorms verbreitet werden, wird ausdrücklich darauf hingewiesen, dass man sich nicht zu strafrechtlich relevanten Aussagen hinreißen lassen, sondern sich vielmehr auf Beleidigungen konzentrieren solle.[10] Konkret wird dabei bspw. empfohlen, die Familie als schwachen Punkt und junge Frauen und Studentinnen in den Fokus zu nehmen. Dies zeigt überdeutlich, dass der in der Praxis bisher kaum relevante Straftatbestand der Beleidigung als solcher von Täter*innen überhaupt nicht wahrgenommen wird -nicht zuletzt aufgrund elementarer Defizite bei der Rechtsdurchsetzung.

---

[7]Institut für Demokratie und Zivilgesellschaft: Hass im Netz. Der schleichende Angriff auf unsere Demokratie. Eine bundesweite repräsentative Untersuchung. Jena 2019. https://www.idz-jena.de/forschungsprojekte/hass-im-netz-eine-bundesweite-repraesentative-untersuchung-2019/ (20.04.2020).

[8]The Fringe Insurgency: Connectivity, Convergence and Mainstreaming of the Extreme Right. https://www.isdglobal.org/wp-content/uploads/2017/10/The-Fringe-Insurgency-221017.pdf

[9]BKA: Straf- und Gewaltdaten im Bereich Hasskriminalität 2017 und 2018. https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2019/pmk-2018-hasskriminalitaet.pdf?__blob=publicationFile&v=4

[10]ARD-Faktenfinder: Infokrieg mit allen Mitteln. 13.02.2018. https://www.tagesschau.de/faktenfinder/inland/organisierte-trolle-101.html.

Die Angleichung der Strafschärfung von § 186 StGB an die Begehung bei einer Versammlung ist konsequent und zu befürworten.

Wir begrüßen zudem die Anpassung des § 188 StGB. Unzureichend erscheint uns in diesem Zusammenhang jedoch die beabsichtigte Neufassung des § 194 StGB. Es ist nicht ersichtlich, warum die Verfolgung von übler Nachrede (§ 186 StGB) und Verleumdung (§ 187 StGB) auch ohne Strafantrag auf Kommunalpolitiker*innen zu beschränken ist. Vielmehr sollte eine Verfolgung dieser Delikte ohne Strafantrag und mit Widerspruchsmöglichkeit nicht von einem politischen Amt abhängen, sondern von der Schwere und Reichweite der geäußerten Diffamierung. Denn die Dynamik, die sich durch den Hass ergibt und die im Entwurf skizziert wird, bleibt in der Praxis nicht nur auf Kommunalpolitiker*innen beschränkt. Die öffentliche Brandmarkung und massenhafte Diffamierung von Personen, die sich im Netz äußern, entwickelt immer dann "...eine Außenwirkung, die geeignet ist, das Rechtsempfinden der Bevölkerung dauerhaft zu stören", wenn eine massenhafte Verbreitung (Reichweite) und eine besondere Schwere (Betroffenheit) der beleidigten Personen gegeben ist. Aktivist*innen, Journalist*innen, Wissenschaftler*innen usw. sind vermehrt ähnlichen Angriffen wie Kommunalpolitiker*innen ausgesetzt, und der demokratiegefährdende Effekt dieser Angriffe ist bei entsprechender Schwere und Reichweite gleichzusetzen. Es wäre daher zu begrüßen, wenn diese Faktoren als Kriterium für Ermittlungen ohne Strafantrag bei § 186 StGB und § 187 StGB zugrunde gelegt würden. Im Übrigen fragen wir uns, warum bei der Überarbeitung des § 194 StGB nicht ein "großer Wurf" gewagt und auch für Beleidigungen i.S.d. § 185 StGB die Möglichkeit der Verfolgung von Amts wegen eröffnet wird. Viele Geschädigte scheuen die Mühen einer Strafanzeige, fürchten weitere Repressalien und die Preisgabe personenbezogener Daten in einem öffentlichen Strafverfahren oder sehen aus falsch verstandener Bescheidenheit davon ab, Strafantrag zu stellen. Insbesondere im Internet sind jedoch teils Beleidigungen zu lesen, die weit mehr zur Folge haben als die Persönlichkeitsrechtsverletzung einer individuellen Person. Die Verrohung der Kommunikation bedroht nicht weniger als den sozialen Frieden und die Freiheit der politischen und gesellschaftlichen Debatte, denn stille Mitleser*innen ziehen sich vollständig zurück und melden **sich** nicht mehr zu Wort. Ein besonderes öffentliches Interesse an der Ahndung auch solcher Beleidigungen kann deshalb im Einzelfall mit Händen zu greifen sein; dass die Strafverfolgung in einem solchen Fall trotzdem nicht möglich sein soll, ist schwer hinnehmbar. Wir plädieren für eine Vereinfachung und Vereinheitlichung des § 194 StGB insgesamt und für eine Abkehr von der Ausgestaltung der Beleidigungsdelikte als absolute Antragsdelikte. Jedenfalls spricht einiges dafür, dass zumindest die Qualifikationstatbestände in geeigneten Fällen auch ohne Strafantrag verfolgt werden können. Dass bei der Staatsanwaltschaft künftig in Massenverfahren regelmäßig das besondere öffentliche Interesse zu bejahen wäre, ist nicht ernsthaft zu befürchten. Die Möglichkeit zur Verfolgung von Amts wegen würde allerdings den Verfolgungsbehörden mehr Handlungsspielraum bieten und für Hasskommentator*innen das Verfolgungsrisiko erhöhen.

Änderung des § 238 StGB: Nachstellung gegenüber Amts- und Mandatsträgern

Unterstützen möchten wir das Anliegen des Städte- und Gemeindebundes[11] eine Nachstellung von Amts- und Mandatsträgern durch einen gesonderten Straftatbestand zu berücksichtigen. Bekanntlich führt zunehmende Hasskriminalität vielerorts dazu, dass vor allem Kommunalpolitiker*innen sich zurückziehen oder Ämter gar nicht mehr besetzt werden können.[12, 13, 14]

Im Gegensatz zum dem sehr weitgehenden Vorschlag des Städte- und Gemeindebundes möchten wir uns jedoch dafür aussprechen, statt eines eigenen Straftatbestandes einen weiteren Absatz in § 238 StGB einzufügen. Analog der Regelungssystematik des § 188 StGB erscheint hier eine Strafschärfung oder Androhung einer Freiheitsstrafe als Mindeststrafe geeignet.

§ 241 StGB (Bedrohung)

Positiv zu bewerten ist die Schließung von Strafbarkeitslücken bei Bedrohungen. In den sozialen Medien begegnen wir regelmäßig massiven Einschüchterungsversuchen in Gestalt der Androhung von Gewalt. Oft sind sie allerdings so formuliert, dass sich die Bedrohung mit einem Verbrechen - der vorsätzlichen Tötung oder zumindest der schweren Körperverletzung - nicht direkt ablesen lässt. Bislang blieb eine Bedrohung mit einer vorsätzlichen oder gefährlichen Körperverletzung straflos, obwohl sie die Betroffenen erheblich beeinträchtigt. Auch die vorgesehenen Qualifikationen und damit die Abstufung der Strafandrohung je nach Schwere (Bedrohung mit einem Verbrechen) bzw. Reichweite (öffentlich oder durch Verbreiten von Schriften) halten wir für sachgerecht.

2. **Änderung des Netzwerkdurchsetzungsgesetzes (NetzDG)**

§ 1 Abs. 1 und 2 NetzDG

Offenbar ist nicht beabsichtigt, den Anwendungsbereich des NetzDG auszuweiten. Außer Acht gelassen wird dabei aber, dass auch Plattformen, auf denen keine “beliebigen”, also allgemeinen, sondern spezielle Inhalte verbreitet werden, sowie kleinere Plattformen von

[11] Stellungnahme zum Referentenentwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität vom 02.01.2020.

[12] Erhardt, Christian: Kommunalpolitiker: Bedrohungen sind an der Tagesordnung. Repräsentative Befragung von 2494 Bürgermeister*innen durch Kommunal. https://kommunal.de/kommunalpolitiker-umfrage-2020 (20.04.2020).

[13] Deutscher Städte- und Gemeindebund: Hass, Bedrohungen & Übergriffe gegen Mandatsträger. Ursachen & Gegenstrategien. Strategiepapier des Deutschen Städte und Gemeindebundes. https://www.dstgb.de/dstgb/Homepage/Aktuelles/Archiv/Archiv%202018/Hass,%20Bedrohungen%20und%20Übergriffe%20gegen%20Mandatsträger/2118%20Anlage%20HassBedrohungenÜbergriffe_240518.pdf (Abgerufen am 20.04.2020).

[14] Umfrage: Bedrohung von Bürgermeistern stark gestiegen. ARD Report München. https://www.br.de/fernsehen/das-erste/sendungen/report-muenchen/gewalt-gegen-buergermeister-umfrage-100.html (20.04.2020).

Hasskriminalität betroffen sind. Lediglich beispielhaft genannt seien hier große Gamingplattformen. Diese sind in der Vergangenheit als Sammelstelle und Ausgangspunkt für groß angelegte Hasskampagnen aufgefallen. Als Beispiel dient die Plattform VKontakte, welche höchst problematische Inhalte aufweist, jedoch bisher vom Geltungsbereich des NetzDGs ausgeschlossen wird. Zumindest sollte in regelmäßigen Abständen und in Beratung mit Expert*innen aus Forschung und Zivilgesellschaft geprüft werden, welche Plattformen zwischenzeitlich unter NetzDG-Richtlinien fallen und ob es wirklich sinnvoll ist, Plattformen mit weniger als zwei Millionen Nutzer*innen von den Verpflichtungen nach dem NetzDG auszunehmen. Wenn dem Grundsatz Geltung verschafft werden soll, dass das Netz kein rechtsfreier Raum ist, dann stellt sich die Frage, warum kleinere Plattformen oder solche, die der Verbreitung spezifischer Inhalte dienen, nicht in die Verantwortung genommen werden. Soweit hier eine organisatorische und - mit Blick auf die Bußgeldvorschriften nach § 4 NetzDG - wirtschaftliche Überforderung kleiner Plattformen ins Feld geführt wird, ist daran zu erinnern, dass lediglich systematische Verstöße geahndet werden. Auch kann bei der Bemessung von Bußgeldern auf die Reichweite und die finanzielle Leistungsfähigkeit der jeweiligen Plattform Rücksicht genommen werden. Denkbar wäre, kleine Plattformen von Berichts- und Schulungspflichten auszunehmen.

§ 1 Abs. 4 NetzDG

Die eher unscheinbar daherkommende Klarstellung des Begriffs der Beschwerde in § 1 Abs. 4 NetzDG-E dürfte weitreichende Folgen haben, weil hiermit die bislang von den Dienstanbietern vorgenommene, strikte Trennung zwischen Beschwerden nach dem NetzDG und solchen wegen Verstoßes gegen Gemeinschaftsstandards keinen Bestand haben kann. Der Referentenentwurf verfolgt offenbar die Absicht, die Diensteanbieter zur Berücksichtigung aller Beanstandungen von Inhalten zu verpflichten und durchzusetzen, dass rechtswidrige Inhalte nach jedweder Meldung entfernt werden, sofern dies erkennbar gewünscht wird. Dies begrüßen wir sehr, denn es bedeutet, dass Nutzer*innen Beschwerden zukünftig nicht ausschließlich über die häufig kompliziert ausgestalteten Meldewege des NetzDG an die Diensteanbieter richten können, sondern gemeldete Inhalte unabhängig von der Art und Weise der Kenntniserlangung durch die Diensteanbieter bearbeitet und gegebenenfalls nach dem neuen § 3a NetzDG-E übermittelt werden müssen. Die bisher durch die Diensteanbieter etablierten Wege für die Meldung nach dem NetzDG sind von sehr unterschiedlicher Qualität und so hochschwellig, dass betroffene Nutzer*innen hier häufig vor unnötige Hürden gestellt werden. Teilweise ist hierin eine bewusste Umgehung des NetzDG zu erkennen. Ob die Plattformen ihr Beschwerdemanagement entsprechend anpassen werden, bleibt abzuwarten.

§ 3 NetzDG

Die geplante Informationspflicht der Diensteanbieter über die Möglichkeiten zur Erstattung von Strafanzeige und Strafantrag nach § 3 Abs. 2 Nr. 5 NetzDG-E ist begrüßenswert, sofern

Antragsdelikte in Rede stehen, welche von der Meldepflicht nach § 3a NetzDG-E nicht umfasst sind. Diese Informationspflicht soll zudem unabhängig von der Entscheidung des Diensteanbieters über die Löschung des Inhalts bestehen. Diese Maßnahme erscheint durchaus geeignet, dem häufig anzutreffenden Informationsdefizit von Nutzer*innen entgegenzuwirken, denen es häufig bereits am Bewusstsein dafür mangelt, dass das Internet kein rechtsfreier Raum ist, und die Anzahl der Strafanzeigen und fristgerechten Strafanträge zu erhöhen.

HateAid gGmbH

Die gemeinnützige Organisation HateAid gGmbH unterstützt Betroffene von digitaler Gewalt. Durch Hassattacken werden Menschen gezielt aus den Debatten im Netz herausgedrängt, aber selten werden Täter*innen zur Verantwortung gezogen. Hier setzt HateAid an und bestärkt Betroffene durch stabilisierende Erst-, Sicherheits-, und Kommunikationsberatung und rechtliche Durchsetzung. Als Prozesskostenfinanzierer unterstützt HateAid Betroffene gegen Täter*innen (zivil-)rechtlich vorzugehen. Im Rahmen des Bündnisses “Keine Macht dem Hass” kooperiert HateAid mit der Schwerpunktstaatsanwaltschaft ZIT in Hessen.