



Deutscher Bundestag

Ausschuss für Recht und Verbraucherschutz

Wortprotokoll der 91. Sitzung

Ausschuss für Recht und Verbraucherschutz

Berlin, den 6. Mai 2020, 11:01 Uhr

Berlin, Marie-Elisabeth-Lüders-Haus, Raum 3.101
(Anhörungsraum)

Vorsitz: Stellvertretender Vorsitzender
Dr. Heribert Hirte, MdB

Tagesordnung - Öffentliche Anhörung

Einzigiger Tagesordnungspunkt

Seite 9

- a) Gesetzentwurf der Fraktionen der CDU/CSU und SPD

Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität

BT-Drucksache 19/17741

Federführend:

Ausschuss für Recht und Verbraucherschutz

Mitberatend:

Ausschuss für Inneres und Heimat
Ausschuss für Wirtschaft und Energie
Ausschuss für Familie, Senioren, Frauen und Jugend
Ausschuss für Menschenrechte und humanitäre Hilfe
Ausschuss für Bildung, Forschung und
Technikfolgenabschätzung
Ausschuss für Kultur und Medien
Ausschuss Digitale Agenda
Ausschuss für Bau, Wohnen, Stadtentwicklung und
Kommunen
Haushaltsausschuss

Berichterstatter/in:

Abg. Ingmar Jung [CDU/CSU]
Abg. Dr. Johannes Fechner [SPD]
Abg. Florian Post [SPD]
Abg. Roman Johannes Reusch [AfD]
Abg. Dr. Jürgen Martens [FDP]
Abg. Niema Movassat [DIE LINKE.]
Abg. Renate Künast [BÜNDNIS 90/DIE GRÜNEN]



b) Gesetzentwurf der Bundesregierung

**Entwurf eines Gesetzes zur Bekämpfung des
Rechtsextremismus und der Hasskriminalität**

BT-Drucksache 19/18470

Federführend:

Ausschuss für Recht und Verbraucherschutz

Mitberatend:

Ausschuss für Inneres und Heimat

Ausschuss für Wirtschaft und Energie

Ausschuss für Familie, Senioren, Frauen und Jugend

Ausschuss für Menschenrechte und humanitäre Hilfe

Ausschuss für Bildung, Forschung und

Technikfolgenabschätzung

Ausschuss für Kultur und Medien

Ausschuss Digitale Agenda

Ausschuss für Bau, Wohnen, Stadtentwicklung und
Kommunen

Haushaltsausschuss

Berichterstatter/in:

Abg. Ingmar Jung [CDU/CSU]

Abg. Dr. Johannes Fechner [SPD]

Abg. Florian Post [SPD]

Abg. Roman Johannes Reusch [AfD]

Abg. Dr. Jürgen Martens [FDP]

Abg. Niema Movassat [DIE LINKE.]

Abg. Renate Künast [BÜNDNIS 90/DIE GRÜNEN]



Teilnehmende Abgeordnete	Seite 4
Sprechregister Abgeordnete	Seite 6
Sprechregister Sachverständige	Seite 7
Anlagen:	
Stellungnahmen der Sachverständigen	Seite 35
Ausschussdrucksache 19(6)134	Seite 170
Ausschussdrucksache 19(6)121	Seite 186

**Mitglieder des Ausschusses für Recht und Verbraucherschutz**

	Ordentliche Mitglieder	Unter- schrift	Stellvertretende Mitglieder	Unter- schrift
CDU/CSU	Heil, Mechthild Heveling, Ansgar Hirte, Dr. Heribert Hoffmann, Alexander Jung, Ingmar Lehrieder, Paul Luczak, Dr. Jan-Marco Müller, Axel Müller (Braunschweig), Carsten Sensburg, Dr. Patrick Steineke, Sebastian Thies, Hans-Jürgen Ullrich, Dr. Volker Warken, Nina Wellenreuther, Ingo	☐ ☐ ☒ ☒ ☒ ☐ ☐ ☒ ☒ ☐ ☐ ☐ ☐ ☐ ☐ ☐	Amthor, Philipp Frei, Thorsten Gutting, Olav Hauer, Matthias Launert, Dr. Silke Lindholz, Andrea Maag, Karin Middelberg, Dr. Mathias Nicolaisen, Petra Noll, Michaela Oellers, Wilfried Schipanski, Tankred Throm, Alexander Vries, Kees de Weisgerber, Dr. Anja	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☒ ☐ ☐ ☐ ☐
SPD	Brunner, Dr. Karl-Heinz Dilcher, Esther Fechner, Dr. Johannes Groß, Michael Heidenblut, Dirk Lauterbach, Prof. Dr. Karl Post, Florian Scheer, Dr. Nina Steffen, Sonja Amalie	☒ ☐ ☒ ☐ ☐ ☐ ☒ ☐ ☐ ☐	Esken, Saskia Högl, Dr. Eva Miersch, Dr. Matthias Müller, Bettina Nissen, Ulli Özdemir (Duisburg), Mahmut Rix, Sönke Schieder, Marianne Vogt, Ute	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐
AfD	Brandner, Stephan Jacobi, Fabian Maier, Jens Maier, Dr. Lothar Peterka, Tobias Matthias Reusch, Roman Johannes	☐ ☐ ☒ ☐ ☐ ☒	Curio, Dr. Gottfried Hartwig, Dr. Roland Haug, Jochen Seitz, Thomas Storch, Beatrix von Wirth, Dr. Christian	☐ ☐ ☐ ☐ ☐ ☐
FDP	Buschmann, Dr. Marco Helling-Plahr, Katrin Martens, Dr. Jürgen Müller-Böhm, Roman Willkomm, Katharina	☐ ☐ ☒ ☐ ☐	Fricke, Otto Innen, Ulla Schinnenburg, Dr. Wieland Skudelny, Judith Thomae, Stephan	☐ ☐ ☐ ☐ ☐



	Ordentliche Mitglieder	Unter- schrift	Stellvertretende Mitglieder	Unter- schrift
DIE LINKE.	Akbulut, Gökay Mohamed Ali, Amira Movassat, Niema Straetmanns, Friedrich	☐ ☐ ☒ ☐	Jelpke, Ulla Lay, Caren Möhring, Cornelia Renner, Martina	☐ ☐ ☐ ☐
BÜNDNIS 90/DIE GRÜNEN	Bayram, Canan Keul, Katja Rößner, Tabea Rottmann, Dr. Manuela	☒ ☐ ☒ ☐	Kühn (Tübingen), Christian Künast, Renate Mihalic, Dr. Irene Schauws, Ulle	☐ ☒ ☐ ☐

sowie weiteres Mitglied des Deutschen Bundestages

SPD	Zimmermann, Dr. Jens	☒
-----	----------------------	-------------------------------------



Sprechregister Abgeordnete

	Seite
Johannes Fechner (SPD)	20
Stellvertretender Vorsitzender Dr. Heribert Hirte (CDU/CSU)	9, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 25, 26, 27, 28, 30, 32, 33, 34
Alexander Hoffmann (CDU/CSU)	20
Ingmar Jung (CDU/CSU)	19
Renate Künast (BÜNDNIS 90/DIE GRÜNEN)	20, 32
Jens Maier (AfD)	32
Dr. Jürgen Martens (FDP)	21
Niema Movassat (DIE LINKE.)	19
Carsten Müller (Braunschweig) (CDU/CSU)	32
Florian Post (SPD)	21
Roman Reusch (AfD)	21
Tankred Schipanski (CDU/CSU)	32
Dr. Jens Zimmermann (SPD)	32



Sprechregister Sachverständige

	Seite
Prof. Dr. Matthias Bäcker, LL.M. Johannes Gutenberg-Universität Mainz Lehrstuhl für Öffentliches Recht und Informationsrecht, insbesondere Datenschutzrecht	10, 30
Josephine Ballon HateAid gGmbH, Berlin Rechtsanwältin	11, 28
Dr. Uda Bastians Deutscher Städtetag, Berlin Leiterin des Dezernats Recht und Verwaltung Beigeordnete	12, 33
Stefan Conen Deutscher Anwaltverein e. V., Berlin Mitglied im Strafrechtsausschuss, Rechtsanwalt	12, 27
Prof. Dr. Armin Engländer Ludwig-Maximilians-Universität München Lehrstuhl für Strafrecht, Strafprozessrecht, Rechtsphilosophie und Rechtssoziologie	13, 26
Klaus-Dieter Hartleb Generalstaatsanwaltschaft München Zentralstelle zur Bekämpfung von Extremismus und Terrorismus Hate-Speech-Beauftragter der bayerischen Justiz; Oberstaatsanwalt	14, 25
Markus Hartmann Staatsanwaltschaft Köln Oberstaatsanwalt als Hauptabteilungsleiter Leiter der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen	14, 23, 25, 33
Henning Lesch eco – Verband der Internetwirtschaft e. V., Hauptstadtbüro Berlin Leiter Hauptstadtbüro, Geschäftsbereichsleiter Politik & Recht, Rechtsanwalt	15, 22



Uwe Lübking Deutscher Städte- und Gemeindebund, Berlin Beigeordneter	16
Andreas May Generalstaatsanwaltschaft Frankfurt am Main Zentralstelle zur Bekämpfung der Internetkriminalität Leitender Oberstaatsanwalt	17, 33
Jürgen Peter Vizepräsident beim Bundeskriminalamt Berlin	18, 21, 34
Dr. Klaus Ritgen Deutscher Landkreistag	19



Der stellvertretende Vorsitzende **Dr. Heribert Hirte**: Einen schönen guten Tag zusammen, verehrte Kolleginnen und Kollegen und liebe Gäste, liebe Sachverständige. Wir sind zur 91. Sitzung des Ausschusses für Recht und Verbraucherschutz zusammengekommen, zur öffentlichen Anhörung zum Gesetzentwurf der Fraktionen der CDU/CSU und SPD zu Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität auf Bundestagsdrucksache 19/17741 sowie zu dem gleichlautenden Gesetzentwurf der Bundesregierung auf Bundestagsdrucksache 19/18470. Nochmals herzlich willkommen an die Abgeordneten, die sich heute Morgen hier schon zur ordentlichen Rechtsausschusssitzung getroffen hatten. Ich begrüße die Sachverständigen, von denen zwei, nämlich Herr Bäcker und Herr Lesch, per Webex zugeschaltet sind. Und die sollten jetzt – hoffentlich – auf dem Videowürfel zu sehen sein und hören mich – hoffentlich – reden. Aus dem winkenden Signal sehe ich, dass das offensichtlich der Fall ist: Einen schönen guten Morgen.

Ich begrüße die Vertreter der kommunalen Spitzenverbände, die alphabetisch in die Reihe der Sachverständigen eingereiht sind, obwohl sie auf der Grundlage eines Sonderstatus hier vertreten sind. Ich begrüße die Vertreterinnen und Vertreter der Bundesregierung und die Zuhörer auf der Tribüne. Wir haben uns verständigt, die heutige Anhörung – unter Einhaltung der geltenden Abstandsregelungen – als Präsenzveranstaltung durchzuführen, hier aber erstmals Sachverständige per Webex zuzuschalten. Weitere Zuschaltungen sind nicht vorgesehen, weil der Ausschuss das so beschlossen hatte. Die per Webex zugeschalteten Sachverständigen können leider nicht den Saal sehen, sondern nur einander. Ich werde deshalb besonders darauf achten, die Rednerinnen und Redner mit Namen zu nennen, damit Sie wissen, wer gerade redet. Ich hoffe, dass diese Premiere für uns als Ausschuss gelingt. Sollten technische Probleme auftreten, bitte ich vorab um Ihr Verständnis.

Gegenstand der Anhörung sind ein Gesetzentwurf der Fraktionen der CDU/CSU und SPD sowie ein textgleicher Gesetzentwurf der Bundesregierung.

Zu dem Gesetzentwurf hat die Fraktion BÜNDNIS 90/DIE GRÜNEN einen Änderungsantrag (Anlage) vorgelegt, der den Sachverständigen ebenfalls zugesandt worden ist. Der Gesetzentwurf sieht Maßnahmen vor, die auf eine intensivere und effektivere Strafverfolgung zur Bekämpfung des Rechtsextremismus und der Hasskriminalität zielen. Insbesondere sollen Anbieter sozialer Netzwerke verpflichtet werden, bestimmte strafbare Inhalte an das Bundeskriminalamt (BKA) zu melden. Außerdem soll das materielle Strafrecht durch angepasste Tatbestände und verschärfte Strafandrohungen noch deutlicher auf die mit Hasskriminalität verbundenen Rechtsverletzungen ausgerichtet werden.

Einige Hinweise zum Ablauf: Die Sachverständigen erhalten zunächst die Gelegenheit zu einer kurzen Eingangsstellungnahme. Wir beginnen dabei alphabetisch, heute also mit Herrn Bäcker, der uns per Video zugeschaltet ist. An die Sachverständigen die Bitte: Bitte bemühen Sie sich, anfangs nicht länger als drei Minuten zu sprechen, weil wir ja insgesamt zwölf Sachverständige haben. Alles, was dann noch nicht beantwortet ist, kann anschließend in der Fragerunde geklärt werden. Da wir die Bildschirme in der Mitte des Saales heute für die Videozuschaltung benötigen, müssen wir auf die übliche Redezeitanzeige, die sonst oben auf dem Würfel stattfindet, verzichten. Wir messen die Zeit deshalb hier vorne. Wenn ich Ihnen ein Signal gebe, bedeutet das, dass die Redezeit abgelaufen ist und Sie bitte zum Ende Ihres Vortrags kommen sollten. Die zugeschalteten Sachverständigen bitte ich, ihre Mikrofone auszuschalten, solange sie nicht sprechen; gegebenenfalls wird das Sekretariat das technisch übernehmen. An den Vortrag der Stellungnahmen schließen sich die Fragerunden an, eine oder mehrere, je nachdem wie viele Fragen es gibt. An die Kolleginnen und Kollegen: Sie kennen das bewährte Verfahren. In jeder Fragerunde hat einer höchstens zwei Fragen, zwei Fragen an einen Sachverständigen oder eine Frage an zwei Sachverständige. Die Sachverständigen werden nach der ersten Fragerunde in umgekehrter alphabetischer Reihenfolge, heute also beginnend mit Herrn Ritgen, um ihre Antworten gebeten. Die Bitte an die Sachverständigen: sich bei diesen Antworten kurz halten. In der zweiten Fragerunde



geht es dann umgekehrt wieder in alphabetischer Reihenfolge.

Nochmals grundsätzlich: Die Anhörung ist öffentlich. Das Sekretariat fertigt auf der Grundlage einer Tonaufzeichnung ein Wortprotokoll an. Bild- und Tonaufnahmen von der Tribüne oder per Webex sind nicht gestattet. Ebenfalls nicht gestattet sind Beifalls- oder Missfallensbekundungen von der Tribüne. Rein vorsorglich möchte ich darauf hinweisen, dass Störungen in der Sitzung nach dem Ordnungswidrigkeitenrecht oder Strafrecht geahndet werden können. Ich danke Ihnen für Ihre Aufmerksamkeit. Damit können wir in die Eingangsstatementsrunde einsteigen. Herr Bäcker, Sie haben als Erstes das Wort. Bitte schön.

SV Prof. Dr. Matthias Bäcker: Herzlichen Dank, Herr Vorsitzender, und vielen Dank, dass mir eine Teilnahme in diesem ungewöhnlichen Format ermöglicht wird. Ich möchte zu zwei der drei großen Themenkomplexe, die der Entwurf enthält, etwas in meinem Eingangsstatement sagen. Wozu ich jetzt nichts sage, sind die Änderungen im materiellen Strafrecht, die vorgesehen sind. Erster Themenkomplex: Die Änderung des Netzwerkdurchsetzungsgesetzes (NetzDG) und die Verpflichtung der Telemedienanbieter, Daten an das Bundeskriminalamt zu übermitteln. Meiner Ansicht nach bestehen gegen diesen Plan prinzipiell keine Bedenken. Es gibt allgemein die Frage, ob das Netzwerkdurchsetzungsgesetz mit dem Unionsrecht vereinbar ist, insbesondere mit dem Herkunftslandprinzip der E-Commerce-Richtlinie. Dazu sage ich nichts, denn das ist eine alte Diskussion, die meiner Ansicht nach durch diesen Entwurf nicht verschärft wird. Das einzige Problem, das ich im Zusammenhang mit dieser geplanten Regelung sehe, ist, dass das Bundeskriminalamt sofort neben den potentiell strafbaren Inhalten auch Identifikationsdaten übermittelt bekommen soll. Das halte ich dann nicht für erforderlich, wenn das BKA letztlich einen Tatverdacht verneint. Meiner Ansicht nach müsste deswegen das Übermittlungsverfahren zweistufig ausgestaltet werden. Zunächst müssten alle Dateninhalte übermittelt werden, die dem BKA die Prüfung ermöglichen, ob ein Tatverdacht vorliegt. Nur wenn das bejaht wird, sollten auch die Identifikationsdaten zur Verfügung gestellt werden. Man kann sich hier unterschiedliche

technische Modelle vorstellen, um das möglichst schnell und effektiv zu gestalten. Dazu habe ich in meiner Stellungnahme etwas gesagt. Zweiter Themenkomplex: Zugriff auf Telemediendaten durch Sicherheitsbehörden und Übermittlung von Telemediendaten an Sicherheitsbehörden. Prinzipiell ist es meiner Ansicht nach rechtspolitisch und auch verfassungsrechtlich begrüßenswert, dass hierzu Regelungen geschaffen werden sollen, weil insgesamt der Zugriff auf komplexe gesellschaftliche Datenbestände im Strafprozess bisher nicht wirklich befriedigend geregelt ist. Der Entwurf enthält meiner Ansicht nach eine Reihe von eher kleinteiligen konzeptionellen handwerklichen Problemen, die ich in meiner Stellungnahme ausgeführt habe. Das Doppeltürmodell des Bundesverfassungsgerichts wird nicht komplett durchgehalten. Es gibt Probleme mit dem Zitiergebot. Das ist alles im Prinzip auf der handwerklichen Ebene behebbar. Ich möchte heute in meinem Eingangsstatement doch auf ein etwas fundamentaleres Problem des Ganzen hinweisen. Meiner Ansicht nach spiegeln letztlich diese kleinteiligen Probleme wider, dass der Zugriff auf Telemediendaten doch eine ziemlich komplexe Regulierungsanstrengung erfordert. Der Entwurf geht davon aus, dass man die im Prinzip parallelisiert mit Telekommunikationsdaten und man die verschiedenen Datenkategorien bei beiden Arten von technischen Kommunikationsdiensten gewissermaßen bündelt und jeweils gleich behandelt. Das Problem, das ich dabei sehe, ist, dass Telemedien ein viel vielgestaltigeres Phänomen sind als Telekommunikationsdienste, dass es viel mehr Anbieter gibt und dass man eine sehr viel größere Spannweite, sozusagen an der Sensibilität der Daten, zu bewältigen hat. Deswegen bin ich mir nicht sicher, ob das wirklich funktioniert. Hinzu kommt, dass die unionsrechtliche Entwicklung hier sehr dynamisch ist. Der EuGH hat bestimmte Dienste den Telemedien zugeschlagen, die man vorher als Telekommunikation angesehen hat. Es gibt verschiedene Regelungsentwürfe: ePrivacy, Kommunikationskodex, E-Evidence-Verordnung. All das wäre hier mit zu berücksichtigen. Das alles findet sich überhaupt nicht im Entwurf, so dass ich Ihnen sehr empfehlen möchte: Stellen Sie das zurück und machen Sie es, wenn man etwas genauer sieht, wo auch auf der europäischen Ebene die Reise langgeht. Herzlichen Dank.



Der **stellvertretende Vorsitzende**: Vielen Dank, Herr Bäcker. Damit kommt als Nächste Frau Ballon ans Mikrofon. Bitte schön, Sie haben das Wort.

SVe **Josephine Ballon**: Sehr geehrte Damen und Herren, sehr geehrter Herr Stellvertretender Vorsitzender, ich bedanke mich für die Einladung und die Möglichkeit, heute hier im Namen von HateAid vor dem Rechtsausschuss sprechen zu dürfen. HateAid ist die einzige Beratungsstelle allein für Betroffene von digitaler Gewalt in ganz Deutschland. Wir beraten nicht nur, sondern unterstützen auch als Prozessfinanzierer bei Zivilprozessen. Ich würde heute gerne auf drei wesentliche Punkte eingehen. Aber zunächst begrüßen wir das gestiegene Bewusstsein dafür, dass Hassrede, Hasskriminalität und organisierter Rechtsextremismus eng zusammenhängen und vor allem im Internet eine Bedrohung für unsere Meinungsfreiheit darstellen. Gleiches gilt für die Motivation, die Strafverfolgung an die Herausforderung des Internetzeitalters anzupassen. Löschen allein genügt hierfür nicht. Wir begrüßen in dem Entwurf vor allem die Vereinfachung von Meldesperren und die Schaffung und Präzisierung von neuen Straftatbeständen. Auch erscheint das Herzstück dieses Gesetzes, die Einführung der geplanten Meldepflicht, grundsätzlich als geeignet, diese Ziele zu erreichen. Hier aber unser erster Kritikpunkt: Die Ausgestaltung stellt aus unserer Sicht einen unverhältnismäßigen Eingriff in elementare Freiheitsrechte dar. Nicht nur Datenschützer, sondern auch weite Teile der Zivilgesellschaft lehnen das zurecht ab. Ich möchte das kurz begründen: Der aktuelle Stand des Entwurfs sieht vor, dass das BKA im Rahmen seiner Zentralstellenfunktion weitreichende Befugnisse zur Datenerhebung, -verwendung und -speicherung erhält, für die es in diesem Umfang keine Notwendigkeit gibt. Das BKA speichert in diesem Prozess zwangsläufig Daten von Tausenden von Menschen, und dies geschieht allein auf der Grundlage, dass Mitarbeiter der sozialen Netzwerke, also Facebook, Twitter und Google, die eine dreiwöchige juristische Schulung erhalten haben, die Inhalte für rechtswidrig halten. All das geschieht, ohne dass jemals eine Staatsanwaltschaft geprüft hat, ob es überhaupt einen Anfangsverdacht gibt, der hierfür Anlass geben würde. Eine gesetzliche Grundlage dafür, dass die Daten beim BKA nach der Ausleitung an

die Staatsanwaltschaft sofort gelöscht werden müssen, gibt es nicht. Vielmehr können die gespeicherten Daten aufgrund großzügiger Spielräume sogar einer Weiterverwendung in einem länderübergreifenden Verbundsystem zugeführt werden. HateAid setzt sich seit Jahren für die effektive Strafverfolgung ein. Wir sind jedoch davon überzeugt, dass es verhältnismäßige Wege geben muss, die Strafverfolgung zu ermöglichen und trotzdem den Datenschutz zu wahren. Wir empfehlen daher dringend, den Entwurf an dieser Stelle nachzubessern. Es gibt hierfür ausgewogene Lösungen. Eine mögliche Lösung wäre z. B. eine an das Urheberrecht angelehnte Praxis, das sogenannte Quick Freeze. In diesem Fall würde das BKA nach Erhalt einer Meldung beim Internet-Provider beantragen, dass die IP-Adresse für einen gewissen Zeitraum nicht gelöscht wird. Die IP-Adresse, die nämlich anderenfalls nach wenigen Tagen gelöscht werden würde, wäre so auch nach Prüfung eines Anfangsverdachts durch eine Staatsanwaltschaft noch verfügbar. Diese im Urheberrecht erprobte Praxis könnte hier auch problemlos angewandt werden, wenn es eine gesetzliche Grundlage geben würde. Zweiter Kritikpunkt ist, dass der Entwurf keine Grundlage für die Identifizierung der Täterinnen außerhalb der Meldepflicht bietet, denn auch die Ausweitung der Ermittlungsbefugnisse löst das grundlegende Problem der mangelhaften Betreiberhaftung nicht.

Die Realität sieht nämlich so aus: Selbst gegenüber Strafverfolgungsbehörden berufen sich die sozialen Netzwerke regelmäßig darauf, dass die angeforderten Daten nicht in Deutschland, sondern in den USA oder in Irland gespeichert seien.

Lösung hierfür wäre die Einführung des Marktortprinzips, deren Probleme auf europarechtlicher Ebene wir uns bewusst sind, die allerdings empfehlenswert wäre, weil sie die Betreiber verpflichten würde, die Daten der inländischen Geschäftstätigkeit auch im Inland vorzuhalten. Als letzten Punkt möchte ich die Beleidigungsdelikte ansprechen. Mit ihnen beginnt aus unserer Erfahrung immer die Verrohung der Sprache im Internet. Und vor allem rechtsextremistische Gruppierungen nutzen Beleidigungen gezielt, um Menschen mundtot zu machen und einzuschüchtern. Leider werden



diese Delikte aktuell schlichtweg kaum verfolgt. Wünschenswert wäre es daher, den großen Wurf zu wagen und die Beleidigungsdelikte als relative Antragsdelikte auszugestalten. Vielen Dank.

Der **stellvertretende Vorsitzende**: Vielen Dank. Frau Bastians hat als Nächste das Wort.

SVe **Dr. Uda Bastians**: Herzlichen Dank, auch für die Einladung, Herr Vorsitzender, meine sehr geehrten Damen und Herren, Professor Hirte hat es angesprochen. Wir sind eingeladen aufgrund unseres Sonderrechts als kommunale Spitzenverbände. Ehrlich gesagt, in diesem Gesetzentwurf sind wir und die kommunale Ebene auch sehr unmittelbar betroffen. Es ist eine alte Forderung von uns, dass hier Verbesserungen notwendig sind. Wir begrüßen diesen Gesetzentwurf daher insgesamt und halten ihn für einen ausgesprochen wichtigen Baustein im Bereich: Wie können wir gegen Hasskriminalität und Rechtsextremismus vorgehen? Ich möchte aber auch betonen: Es ist nur ein Baustein, um unsere Demokratie, unsere freiheitliche Grundordnung zu schützen und auch um die Diskussionskultur nicht völlig den Bach hinuntergehen zu lassen. Wir brauchen noch Weiteres. Aber erstmal ist es richtig und wichtig, gegen Hasskommentare und Beleidigungen, gegen Drohungen usw. stärker vorzugehen. Warum? Weil die Menschen, die vor Ort bedroht werden, die beleidigt werden, die müssen das Gefühl haben, dass der Staat sie schützt, dass es wirksame Maßnahmen gibt. Und diese Haltung können wir im Moment nicht spüren. Die brauchen wir aber. Wir brauchen wirksame Hemmschwellen gegen extreme Auswüchse im Netz und auch gegen direkte Bedrohungen. Die Statistiken sind Ihnen bekannt, und diese Entwicklung, dass immer mehr Amts- und Mandatsträgerinnen, auch Ehrenamtliche, bedroht und beleidigt werden, diese Entwicklung gefährdet unsere Demokratie, gerade auf der kommunalen Ebene. Das ist die Wiege unserer Demokratie. Hier brauchen wir ein Verständnis der Gesellschaft, dass menschenverachtende Hetze nicht salonfähig werden darf. Sonst macht es am Ende keiner mehr, und dann hat unsere Gesellschaft ein riesiges Problem. Deswegen brauchen wir dieses Gesetz. Strafbarkeitslücken müssen geschlossen werden. Es ist gut und richtig, wenn Kommunalpolitikerinnen und

Kommunalpolitiker auch gesondert geschützt und als im politischen Leben des Volkes stehende Personen bewertet werden. Das ist eine Forderung von allen kommunalen Spitzenverbänden. Das brauchen wir unbedingt, auch als Zeichen. Und wir brauchen die Ergänzung des Straftatbestands der Bedrohung. Es kann nicht sein, dass eine Mitarbeiterin im Bürgeramt mit Taten gegen die sexuelle Selbstbestimmung bedroht wird und dann nichts passiert, weil es straflos ist. Wir brauchen wirklich diese Verschärfung, damit der Staat auch seine Handlungsfähigkeit zeigt. Wir brauchen auch die Verfolgung solcher Taten im Netz, insbesondere in den sozialen Medien. Wir brauchen aber auch – und das möchte ich betonen – eine gut ausgestattete Justiz und Staatsanwaltschaft. In vielen Ländern gibt es schon Schwerpunktstaatsanwaltschaften – heute ist ja auch eine hier vertreten. Das ist ein sehr guter und richtiger Schritt, der vor Ort zu Vertrauen führt. Ich möchte noch einmal betonen: Der Gesetzentwurf ist nur ein Baustein. Wir brauchen auch politische Bildung, wir brauchen Diskussionen, wie wir unser Zusammenleben gestalten wollen, wir brauchen noch viel mehr. Aber dieses Gesetz brauchen wir auf jeden Fall. Danke schön!

Der **stellvertretende Vorsitzende**: Vielen Dank. Herr Conen hat als Nächster das Wort.

SV **Stefan Conen**: Vielen Dank. Auch ich bedanke mich für die Einladung und die Gelegenheit, hier zu sprechen. Aus Sicht des Deutschen Anwaltsvereins und aus meiner Sicht als Strafverteidiger ist an dem Ziel und der Intention dieses Gesetzes überhaupt nichts zu bemängeln oder zu kritisieren. Zu kritisieren ist – und das habe ich in unserer Stellungnahme auch ausgeführt – allerdings die Umsetzung und überhaupt die Frage, ob man die Antworten auf die aufgeworfenen Probleme, die auch meine Vorrednerinnen benannt haben, nämlich zunehmende Beschimpfung, Hasskriminalität im Netz, ob man diese Antworten tatsächlich im Strafrecht finden kann. Wir bezweifeln das als Praktiker im Strafrecht aus der Erfahrung. Wir glauben nicht, dass die Anhebung von Sanktionsdrohungen in Paragraphen, die bislang kaum empirisch in Erscheinung treten, dazu führen wird, dass sich im Netz etwas ändert. Wir glauben, dass es da anderer Antworten bedarf. Die Strafschärfungen sind das Eine. Das Andere – das



ist auch genannt worden – ist die Ausweitung von Tatbeständen, insbesondere § 241 StGB, wo der Strafraum erhöht werden soll, verdoppelt werden soll, und gleichzeitig eine massive Ausweitung stattfindet. Es gibt in dem Begründungsentwurf eine überschlägige Evaluierung, was das an zusätzlichen Justizressourcen bedingen würde. Es gibt dazu eine kritische Stellungnahme eines Praktikers – Herr Hartmann, der noch dazu sprechen wird. Ich glaube nicht, dass die Justiz nach dieser Pandemie, die die Justiz im Moment lahmlegt, wenn das noch als Gesetzentwurf oben draufkommt, das leisten kann, was Sie sich hier von ihr erhoffen. Ich glaube, dass ein Vollzugsdefizit in diesem Bereich die Frustration und den Zweifel der Bürger an dem Rechtsstaat eher steigert, als dass es tatsächlich hilft. Dazu kommt, dass das Gesetz an mehreren Stellen auch handwerklich nicht gut gemacht ist. Gelinde gesagt: Ich halte es für einen Fehler – dazu habe ich meiner Stellungnahme auch Ausführungen gemacht – in § 46 StGB als besonderem Strafzumessungsgrund einzelne Bevölkerungsgruppen herauszuheben. Antisemitismus als Motivation soll strafscharfend berücksichtigt werden. Da habe ich juristische Ausführungen zu gemacht. So, wie das im Gesetz jetzt vorgesehen ist, muss man befürchten, dass teilweise das Gegenteil eintreten wird, nämlich eine öffentliche Wahrnehmung. Dazu kann ich vielleicht noch weitere Ausführungen machen. Das andere ist: § 241 StGB wird auf die Beschädigung von Gegenständen von bedeutendem Wert erweitert. Das ist eine Formulierung aus § 315 StGB, aus den Straßenverkehrsdelikten: Damit sind normalerweise Autos über 750 € gemeint. Wenn ich mir angucke, dass jetzt die Bedrohung, dass ich eine Sachbeschädigung an einem Gegenstand von bedeutendem Wert begehe, mit zwei Jahren Maximalstrafe bestraft wird, dann ist das systematisch nicht mehr kongruent mit der vollendeten Sachbeschädigung, wenn ich es nämlich tatsächlich tue: Da ist genau der gleiche Strafraum einschlägig. Das halte ich für handwerklich schlecht gemacht. Das Gleiche gilt für die Androhung von Straftaten der gefährlichen Körperverletzung. Das sind lediglich Begehungsweisen, die da kriminalisiert werden, aber keine „besonderen“ Körperverletzungen, sondern nur Handlungsweisen, mit denen man sowieso nicht droht, aber auch das soll strafverschärfend

berücksichtigt werden. Das ist meines Erachtens zu kurz gedacht. Und im Übrigen kann ich mich – auch, wenn ich da sonst Differenzen habe, was die Speicherungsbedenken angeht – voll Frau Ballon anschließen: Dass das BKA da eine Datenbank aufbaut, halten wir auch nicht für angezeigt. Danke.

Der **stellvertretende Vorsitzende**: Vielen Dank, Herr Conen. Als Nächster hat das Wort Herr Engländer.

SV Prof. Dr. Armin Engländer: Einen schönen guten Morgen und vielen Dank für die Einladung. Ich werde mich bei meinen Ausführungen auf die vorgeschlagenen Änderungen des materiellen Strafrechts konzentrieren. Eine Vorbemerkung: Bei der Verwendung des Mittels des Strafrechts sind generell zwei Dinge zu beachten: zum einen die ultima-ratio-Funktion des Strafrechts und zum anderen die Praktikabilität. Da ist die Frage: Sind die Strafverfolgungsorgane mit ihren Ressourcen hinreichend zur Ahndung in der Lage? Aus meiner Sicht ist der Gesetzentwurf weitgehend gelungen, insbesondere bei den vorgeschlagenen Änderungen bei den Beleidigungsdelikten. Das betrifft insbesondere die Einbeziehung der kommunalen Ebene. Hier besteht in der Tat eine Strafbarkeitslücke, die es verdient, geschlossen zu werden. Richtig finde ich auch, dass das unter Beibehaltung der bisherigen Struktur des § 188 StGB geschieht. Das heißt, insbesondere unter Beibehaltung der Eignungsklausel. Das ist aus meiner Sicht auch vorzugswürdig gegenüber der Alternativkonzeption, die das durch das Tatbestandsmerkmal „in Beziehung zu deren politischer Betätigung“ ersetzen möchte. Aus meiner Sicht kann das zu problematischen Verkürzungen des Schutzes führen, nämlich bei ehrenrührigen Tatsachenbehauptungen über private oder berufliche Verfehlungen – berufliche Verfehlungen eben bei Personen, die ehrenamtlich politisch tätig sind. Die würden dann an dieser Stelle wohl von § 188 StGB nicht mehr erfasst. Was man überlegen kann, ist, ob man § 188 StGB noch um § 185 StGB – die Beleidigung – ergänzt. Das erscheint aus meiner Sicht sinnvoll. Grundsätzlich gilt allerdings, dass man an dieser Stelle auch nicht zu viel erwarten darf, weil der weitreichende Vorrang der Meinungsfreiheit nach der Rechtsprechung des Bundesverfassungsgerichts unangetastet bleibt. Kritisch zu sehen



sind aus meiner Sicht zwei Punkte: Einmal bei § 140 StGB – das Billigen auch noch nicht begangener Straftaten. Aus meiner Sicht werden die wirklich strafwürdigen Fälle weitestgehend schon von § 111 StGB, vom Auffordern, erfasst, und es stellt sich auch hier aus meiner Sicht massiv das Problem der Praktikabilität. Bei § 241 StGB sieht es aus meiner Sicht so aus, dass die vorgeschlagenen Änderungen weit in den Bereich der Bagatellkriminalität ausgreifen. Das geht auch über den Schutzzweck der Vorschrift, den Schutz des individuellen Rechtsfriedens vor besonders gravierenden Beeinträchtigungen, doch weit hinaus. Deshalb ist aus meiner Sicht hier nur eine deutlich restriktivere Erweiterung des Tatbestands angezeigt. Vielen Dank.

Der **stellvertretende Vorsitzende**: Danke. Als Nächster hat das Wort Herr Hartleb.

SV Klaus-Dieter Hartleb: Die vorliegenden Gesetzesentwürfe sind im Grundsatz zu begrüßen. Ich will mich hier vorab auf einige wesentliche Punkte beschränken. Zum Bedrohungstatbestand: Äußerungen wie „ich breche dir die Beine“ oder „ich schlage dich krankenhausreif“ sind künftig zurecht als Bedrohung strafbar. Ich habe als Staatsanwalt sehr häufig die Situation erlebt, den Opfern solcher massiver Bedrohungen erklären zu müssen, warum diese keine Bedrohung im Rechtssinn darstellen. Dies fiel natürlich schwer. Die Gesetzesänderung ist deshalb zu begrüßen. Abstand nehmen sollte man allerdings etwa von der Forderung, dass mindestens mit einer gefährlichen Körperverletzung gedroht werden muss, denn dann blieben z. B. die eben genannten Drohungen wie „ich breche dir die Beine“ oder „ich schlage dich krankenhausreif“ weiterhin straffrei, denn es handelt sich um eine einfache Körperverletzung. Zu § 140 StGB, Belohnung und Billigung von Straftaten: Die Änderung ist ebenfalls zu begrüßen. Ein erheblicher Anteil der Hasskommentare im Internet besteht in dem Gutheißen von Mord und Totschlag, etwa durch Äußerungen, jemand gehöre an die Wand gestellt, in die Gaskammer, oder Ähnlichem. Dies vergiftet das gesellschaftliche Klima außerordentlich. Vielfach mussten Ermittlungsverfahren wegen solcher Äußerungen in der Vergangenheit eingestellt werden, denn in der Regel sind sie nicht von dem bestehenden Straftatbeständen, insbesondere der Aufforderung zu oder der

Androhung von Straftaten, der Volksverhetzung oder der Bedrohung umfasst. Es ist deshalb gut und richtig, dass die bestehende Strafbarkeitslücke geschlossen wird. Zu den Beleidigungsdelikten: Hier gehen die Gesetzesentwürfe nicht weit genug. Zwar ist es zu begrüßen, dass nunmehr auch kommunalpolitisch tätige Personen eindeutig in den Schutzbereich des § 188 StGB einbezogen werden. Dies greift aber zu kurz, da dieser Tatbestand aufgrund der engen Voraussetzungen so gut wie nie zur Anwendung kommt. Zur vorgesehenen Meldepflicht: Die Einführung der Meldepflicht gemäß § 3a NetzDG ist zu begrüßen. Sie stellt erstmals eine Verpflichtung der Anbieter sozialer Netzwerke dar, entsprechende Hate-Speech-Straftaten den Strafverfolgungsbehörden anzuzeigen, anstatt die Posts lediglich zu löschen. So wird sich die Zahl der Ermittlungsverfahren erhöhen, was gut ist, denn eins der größten Probleme bei der Bekämpfung von Hate Speech ist, dass es sich zwar objektiv um ein Massenphänomen handelt, die Anzahl der Ermittlungsverfahren aber immer noch relativ gering ist. Ein Beispiel: In Bayern wurden ja bei jeder Staatsanwaltschaft Hate-Speech-Sonderdezernate eingerichtet. Die Zahl der eingegangenen Ermittlungsverfahren im ersten Quartal 2020 bei den insgesamt 31 Sonderdezernaten lag bei nur 356. Dies dürfte sich mit der neuen Regelung nun ändern. Allerdings sollte man keinesfalls den Fehler machen, auf halbem Wege stehen zu bleiben. Es wäre fatal, zwar viele Verfahren zu generieren, die dann aber vielfach eingestellt werden müssten. Diese Gefahr besteht aber nach der gegenwärtigen Fassung der Gesetzesentwürfe. So wird die Verpflichtung der Netzbetreiber, lediglich den Inhalt, die IP-Adresse und die Portnummer mitzuteilen, in vielen Fällen für eine erfolgreiche Strafverfolgung nicht ausreichend sein. Es müssten zudem sowohl die URL als auch die ID des Posts sowie ein sekundengenauer Zeitstempel übermittelt werden, zudem die hinterlegten Bestandsdaten. Danke.

Der **stellvertretende Vorsitzende**: Vielen Dank. Als Nächster hat das Wort Herr Hartmann.

SV Markus Hartmann: Herr Vorsitzender, meine Damen, meine Herren, herzlichen Dank für die Möglichkeit, zu den Gesetzentwürfen Stellung zu nehmen. Meine Dienststelle, die Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen,



ist bereits seit 2016 in ganz unterschiedlichen Zuständigkeiten mit der Verfolgung digitaler Hasskriminalität befasst. Ich möchte mich deswegen in meiner Stellungnahme auf Praxiserfahrungen konzentrieren. Vorab eine ganz kurze Anmerkung zu der Grundannahme der vorliegenden Gesetzentwürfe: Die gehen im Kern davon aus, dass es ein Defizit bei der Anzeigenerstattung gibt und deswegen eine Meldepflicht eingeführt werden müsse. Nach unseren Erfahrungen ist nicht nur die Quantität der Ermittlungsverfahren bislang defizitär, sondern vor allen Dingen deren Qualität. In viel zu wenigen Fällen können wir im Ergebnis Täterinnen und Täter ermitteln, obschon uns ein Posting bekannt ist oder angezeigt wurde. Und dem daraus entstehenden Eindruck, das Internet sei ein strafverfolgungsfreier Raum, in dem man sagen und posten könne, was immer man wolle, dem wird man am wirkungsvollsten generalpräventiv entgegenzutreten können durch eine Steigerung der Qualität der Ermittlungen, also ein Mehr an Identifikation von Tatverdächtigen. Es hätte sich aus meiner Sicht da durchaus empfohlen, auch über Alternativmodelle zu einer Meldepflicht – etwa die Bildung operativer Sondereinheiten von Polizei und Justiz unter Zuweisung auskömmlicher Ressourcen – nachzudenken. Der Gesetzgebungsprozess hat in Teilen eine etwas andere Akzentuierung vorgenommen, weswegen ich vor allen Dingen zu den praktischen Auswirkungen der vorliegenden Entwürfe Stellung nehmen möchte. Ich habe – lassen Sie mich das so offen formulieren – die große Sorge, dass die neue Gesetzeslage eine Flut von Vorgängen, aber nur ein kleines Rinnsal an Verurteilungen hervorbringen wird. Die Strafverfolgungsbehörden werden die Menge an auf sie zukommenden Verfahren nur unter äußersten Anstrengungen und der Zuweisung erheblicher zusätzlicher Ressourcen bewältigen können. Die Schätzung der zusätzlichen Arbeitsaufkommen in den Entwürfen ist allenfalls aus meiner Sicht eine Minimalannahme. Die erwartbaren Verfahrenszahlen sind eher knapp angesetzt. Die Bedarfsberechnungen lassen etwa den Bereich der Rechtspflege und der Unterstützungskräfte in den Staatsanwaltschaften gänzlich außer Acht. Landespolizeiliche Bedarfe sind nicht erwähnt. Auswirkungen der deutlich erweiterten materiell-rechtlichen Grundlagen –

wir haben einiges in den vorangegangenen Beiträgen gehört – sind nicht abgeschätzt und berücksichtigt. Ganz praktisch: Für NRW hieße die vorgeschlagene Gesetzeslage, eine mittelgroße Staatsanwaltschaft komplett neu zu schaffen. Deswegen wird man auch berücksichtigen müssen, dass allein Stellen, die zugewiesen werden, noch keine Akten bearbeiten. Ob und in welchem Zeithorizont überhaupt geeignete Einstellungen vorgenommen werden können, ist aus meiner Sicht ebenso offen. Deswegen halte ich es für zwingend erforderlich, lange Umsetzungsfristen oder eine stufenweise Einführung der Meldepflicht in Erwägung zu ziehen. Im Rechtlichen möchte ich nur auf einen Aspekt kurz eingehen. Der Gesetzentwurf ist an einer aus meiner Sicht wesentlichen Stelle sehr unklar. Insbesondere hinsichtlich der Rolle des BKA – wie genau dessen Tätigwerden rechtlich einzustufen ist, strafprozessual oder im Rahmen einer allgemeinen Zentralstellenstätigkeit – sollte es Klarstellungen geben, um eine Handlungssicherheit für alle Beteiligten zu schaffen. Ganz zum Schluss möchte ich noch kurz darauf hinweisen, dass die erfolgreiche Strafverfolgung vor allem dann gelingt, wenn den Strafverfolgungsbehörden alle erforderlichen Informationen zeitgerecht zur Verfügung stehen. Das ist bislang in wesentlichen Fällen nicht der Fall, da die international aufgestellten Dienstanbieter – durchaus nachvollziehbar – bei unterschiedlichen Konstellationen auf den justiziellen Rechtsweg verweisen. Ohne eine Pflicht zur umfassenden inhaltlichen Beauskunftung von Ersuchen der Strafverfolgungsbehörden unter Zugrundelegung des Marktortprinzips werden wir auch zukünftig, auch bei Einführung einer Meldepflicht, in zahlreichen Fällen die weiteren erforderlichen Auskünfte der sozialen Netzwerke nicht zeitgerecht erhalten, so dass sich dieser Umstand aus meiner Sicht als fortdauerndes und wesentliches Hemmnis der Strafverfolgung erweisen wird. Vielen Dank.

Der **stellvertretende Vorsitzende**: Vielen Dank, Herr Hartmann. Als Nächster hat das Wort Herr Lesch.

SV Henning Lesch: Vielen Dank. Vielen Dank auch für die Einladung und die Gelegenheit zur Stellungnahme. Ich denke, hier besteht Konsens und Einigkeit darüber, dass konsequent gegen



Straftaten und Hasskriminalität im Internet vorzugehen ist. Umstritten ist also nicht das Ob, sondern allein das Wie. Im Eingangsstatement möchte ich ein paar Problempunkte ansprechen. Das Gesetzespaket sieht eine Herausgabepflicht von Passwörtern sowie die Neuregelung der Auskunftspflicht über Bestands- und Nutzungsdaten bei Telemediendiensten vor. Diese Regelung betrifft alle Anbieter von Telemediendiensten – E-Mail-Anbieter, Webseiten-Betreiber, Forenbetreiber, soziale Netzwerke, Chatdienste, Messenger, Online-Shopping, Cloud-Services. Geschätzt ist davon auszugehen, dass in Deutschland ungefähr 2,3 Millionen Unternehmen als geschäftsmäßige Anbieter von Telemedien gelten. Die Neuregelung führt damit also zu einer massiven Ausweitung der Auskunftsansprüche über Bestands- und Nutzungsdaten gegenüber den Strafverfolgungsbehörden, den Sicherheitsbehörden und den sonstigen berechtigten Stellen – dies sowohl nach Bundesrecht als auch nach Landesrecht und natürlich auch nach allgemeinem Polizei- und Ordnungsrecht. Diese Neuregelung hat damit eine immense, sowohl qualitative als auch quantitative, Dimension. Ich denke, diese Tragweite darf man nicht unterschätzen. Eine weitere Regelung ist die Herausgabepflicht von Passwörtern bei den Telemediendiensten. Diese Regelung wurde jetzt im Verlauf des Verfahrens nachgebessert. Es wurde klargestellt, dass eine Verschlüsselung unberührt bleiben soll, sowie die Eingrenzung mit Straftatenkatalog oder einem Richtervorbehalt. Nach wie vor bestehen aber immer noch ungeklärte Fragen an dieser Regelung. Dabei ist, glaube ich, in diesem Kontext die bisherige Diskussion sehr stark auf Passwörter fokussiert. Die Regelung bezieht sich aber auf Passwörter und andere Zugangsdaten, mit denen ein Zugriff ermöglicht wird. Hinzu kommt, dass für die Auskunftserteilung sämtliche unternehmensinternen Datenquellen zu berücksichtigen sind. Ein weiterer Punkt: Die Meldepflicht im Netzwerkdurchsetzungsgesetz für die Betreiber sozialer Netzwerke ist sicherlich eine der zentralen Regelungen des Gesetzesvorhabens. Problematisch an der Meldepflicht: Wir haben eine proaktive Ausleitung von Inhalts- und Nutzerdaten, IP-Adressen und Portnummern an das BKA. Dabei findet keinerlei vorhergehende einzelfallbezogene Prüfung, entweder durch ein

Gericht oder eine Staatsanwaltschaft, statt. Ein Richtervorbehalt ist ebenfalls nicht vorgesehen. Damit haben wir große Probleme, schon in der Grundkonzeption. Wir sehen einen Konflikt verfassungsrechtlicher Art in Bezug auf den Datenschutz – Datenschutz Deutschland, Datenschutz-Grundverordnung (DSGVO) in Europa. Wir sehen einen Konflikt mit der E-Commerce-Richtlinie, dem Herkunftslandprinzip und der E-Evidence-Richtlinie. Ich glaube, was oft vergessen wird – das Gesetz zielt ja in erster Linie auf große soziale Netzwerke und damit im Ausland ansässige Unternehmen ab. Hier entsteht und droht ein Konflikt mit den Rechtsvorschriften des Heimatstaates, z. B. amerikanischem oder irischem Recht sowie internationalem Recht und internationalen Verträgen. Damit besteht auch gleichzeitig die Gefahr, dass sich diese Unternehmen durch die Meldepflicht in ihrem Heimatland strafbar machen können. Die proaktive Ausleitung von Inhalts- und Nutzerdaten ist im Grunde genommen ein Systembruch. Sie erfolgt nicht auf ein Ersuchen von Behörden, sondern es findet eine proaktive Meldung bei potenziellen oder möglichen Straftaten statt. Ein weiterer grundsätzlicher Kritikpunkt, Herr Bäcker hat es ja angesprochen: Die aktuellen Entwicklungen auf der EU-Ebene wurden überhaupt nicht berücksichtigt. Die EU-Kommission hat bereits eigene Aktivitäten angekündigt und entsprechende Rechtsvorschriften in Aussicht gestellt. Vielen Dank.

Der **stellvertretende Vorsitzende**: Vielen Dank, Herr Lesch. Dann kommt als Nächster Herr Lübking als zweiter Vertreter der kommunalen Spitzenverbände. Herr Lübking, Sie haben das Wort.

SV Uwe Lübking: Vielen Dank, Herr Vorsitzender, meine Damen und Herren Abgeordnete, ich glaube, ich brauche meine Zeit nicht auszuschöpfen, da wir innerhalb der kommunalen Familie eine große Einmütigkeit in der Beschreibung der Situation und auch in der Bewertung der Gesetzentwürfe haben. Frau Bastians hat beschrieben, wie die Situation in den Kommunen ist, wie viele Kommunalpolitikerinnen und Kommunalpolitiker, aber auch Amtsträgerinnen und Amtsträger sich diesen Tatbeständen ausgesetzt sehen und beklagen, dass diese Taten



im Augenblick nicht ausreichend verfolgt werden und verfolgt werden können. Deshalb begrüßen wir den Gesetzentwurf insgesamt. Allerdings möchten wir auch darauf hinweisen, dass die Strafverfolgungsbehörden natürlich so ausgestattet sein müssen, dass das Gesetz auch tatsächlich umgesetzt werden kann, und auch nicht vergessen werden sollte, dass wir, um insgesamt dem Phänomen Hasskriminalität und Rechtsextremismus begegnen zu können, auch Präventions- und Sensibilisierungsarbeit brauchen. Auch das muss ausgebaut werden, Frau Bastians hat das auch schon erwähnt. Allein mit den mit dem Strafrecht kann man diesem Phänomen nicht begegnen. Hier brauchen wir weitere Maßnahmen. Was die Tatbestände im Einzelnen angeht: Die Ergänzung des § 46 Abs. 2 S. 2 StGB um antisemitische Beweggründe begrüßen wir als Klarstellung. Die Erweiterung des nach § 115 Abs. 3 vor Widerstandshandlungen und tätlichen Angriffen geschützten Personenkreises um Hilfeleistende eines ärztlichen Notdienstes oder einer Notaufnahme begrüßen wir auch. Es ist leider festzustellen, dass auch dieser Personenkreis sich zunehmend Angriffen ausgesetzt sieht. Es ist insgesamt eine mehr als bedenkliche Entwicklung, dass man hierauf tatsächlich auch mit strafrechtlichen Mitteln antworten muss. Auch die Änderung in § 140 StGB wird von uns begrüßt, ebenso die Erweiterung des § 241 StGB. Was die Änderung des § 188 StGB angeht: Da regen wir allerdings an, ob man den Formulierungsvorschlag des Bundesrates folgen sollte, weil er aus unserer Sicht eine Klarstellung gegenüber dem vorliegenden Gesetzestext darstellt. Und zum Schluss regen wir auch an, über die von uns unterstützte Regelung in § 51 Bundesmeldegesetz hinaus auch zu prüfen, ob § 38 GVG geändert werden kann, weil wir bei der Auslegung der Schöffenlisten auch Erfahrungen machen, dass es hier zu Bedrohungen und Ähnlichem kommt, weil auch hier die Abgleiche erfolgen. Vielen Dank.

Der **stellvertretende Vorsitzende**: Vielen Dank, Herr Lübking. Als Nächster hat das Wort Herr May. Bitte schön.

SV **Andreas May**: Vielen Dank. Sehr geehrter Vorsitzender, sehr geehrte Damen und Herren, viele von den Dingen, die ich mir vorgenommen hatte, zu sagen, haben bereits meine Kollegen von

den anderen Zentralstellen gesagt, so dass ich mich auf zwei Kernpunkte beschränken will. In diesem Gesetzgebungsverfahren sind in den letzten Wochen sehr viele Detailfragen geklärt worden. Es ist sehr viel Detailarbeit verrichtet worden, und dieser Detailarbeit mag ich mich gar nicht zuwenden. Ich möchte vielmehr Stellung nehmen zu ganz grundlegenden Dingen, die mich und uns in der Zentralstelle beschäftigen. Uns muss klar sein: Ziel des Gesetzes ist effiziente strafrechtliche Verfolgung, das heißt, eine Strafverfolgung, bei der die Verantwortlichen letztendlich zur Rechenschaft gezogen werden können. Die Frage ist, ob dieses Gesetz die Voraussetzungen hierfür schafft. Wir müssen uns vergegenwärtigen, wir haben es mit immensen Verfahrenszahlen zu tun, 250.000 Verfahren – das ist eine Hausnummer, das muss man ehrlich sagen. Wir kennen Massenverfahren und können damit umgehen. Aber Massenverfahren hier heißt: besondere Flüchtigkeit der Daten. Wir haben es mit Internetermittlungen zu tun. Es wird vieles von der Qualität und von der Zuordnungsfähigkeit der Daten abhängen, die wir erhalten. Hier sehe ich vieles skeptisch. Aber wir müssen uns, wenn wir Massenphänomene zu bearbeiten haben, in einem sicheren Rechtsrahmen, auf einer sicheren Ebene bewegen.

Der Kollege Hartmann hat es bereits angesprochen. Es gab eine Stellungnahme des Bundesrates vom 27. März 2020. Dort wurde eine Frage aufgeworfen, nämlich: Was hat das BKA als Zentralstelle überhaupt für Aufgaben? Darf es beispielsweise überhaupt diese Posts, die zugelieferten Meldungen strafrechtlich bewerten? Ich muss gestehen, ich habe das Ganze erstmal mit einer gewissen Unverständnis zur Kenntnis genommen, weil das BKA ja schon seit vielen Jahren in anderer Form als Zentralstelle tätig wird und für mich selbstverständlich ist, dass natürlich eine strafrechtliche Bewertung dieser Meldungen stattfindet. Vor allen Dingen vor dem Hintergrund, dass nachher qualifizierte Bestandsdaten-anfragen nach § 10 BKA-Gesetz stattfinden sollen, die den Anfangsverdacht einer Straftat voraussetzen. Das ist aus meiner Sicht absolut selbstverständlich, dass natürlich eine strafrechtliche Bewertung stattfinden muss. Der Bundesrat hat dann gleich noch eine zweite Frage aufgeworfen, die sich daran anschließt, nämlich die Frage: Inwieweit spielen in dieser Phase der



Zentralstellentätigkeit des BKA, das hier die Meldungen entgegennimmt, die Staatsanwaltschaften eine Rolle? Müssen in allen Vorgängen, bei allen Meldungen, Ermittlungsverfahren eingeleitet werden? Muss eine Art Zweitbewertung durch eine Staatsanwaltschaft stattfinden? Müssen diese Verfahren, falls die Meldungen nicht strafrechtlich relevant sind, einer Einstellung zugeführt werden? Auch hier kann ich sagen: Wir arbeiten in einem anderen Segment schon sehr lange mit dem BKA in Massenverfahren zusammen, nämlich im Bereich der Bekämpfung der Kinderpornografie. Wir bekommen dort massenhaft Hinweise, die über eine amerikanische gemeinnützige Einrichtung gesteuert werden, NCMEC [National Center for Missing & Exploited Children]. Und hier werden diese Vorgänge zunächst auf deren strafrechtliche Relevanz erstbewertet vom BKA, und dann werden die mitgelieferten IP-Adressen, ähnlich wie in diesem Verfahren, nach dem BKA-Gesetz abgefragt. Und wenn eine Zuordnung möglich ist, werden die Vorgänge dann abgesteuert. Stellt man keine strafrechtliche Relevanz fest, werden diese Vorgänge natürlich nicht an Strafverfolgungsbehörden abgesteuert. Es besteht auch keine Vorlagepflicht bei offensichtlich strafrechtlich nicht relevantem Verhalten. Das muss man sagen. Also, wie gesagt, es wäre wünschenswert, diesen Rechtsrahmen, in dem sich das BKA im Zuge der Zentralstellentätigkeit bewegt, klarzustellen. Die nächste Frage, ganz kurz, ist die Frage: Können wir effiziente Strafverfolgung gewährleisten? Da muss ich sagen: Nein, die Daten, die ausgeliefert werden, sind IP-Adressen. IP-Adressen sind flüchtig. Sie werden nicht gespeichert. IP-Adressen sind ohne dazugehörigen Port bei Nutzung mobiler Endsysteme nicht zuordenbar. Bei den Kinderpornografieverfahren ist es so, dass wir über 50 Prozent der Verfahren von vornherein einstellen müssen, weil die IP-Adressen entweder verfristet oder nicht mehr zuzuordnen sind wegen des sogenannten NAT-Routings. Das heißt, man muss sagen, dass ohne weitere Daten – der Kollege Hartleb hat es angesprochen –, nämlich die Bestandsdaten, eine effiziente Strafverfolgung nicht zu machen sein wird. Vielen Dank.

Der **stellvertretende Vorsitzende**: Vielen Dank, Herr May. Das Bundeskriminalamt wurde öfter angesprochen, aber der Sachverständige sitzt

alphabetisch etwas weiter hinten und kommt jetzt erst dran. Herr Peter, Sie haben das Wort.

SV Jürgen Peter: Ganz herzlichen Dank. Sehr geehrter Herr Vorsitzender, sehr geehrte Damen und Herren, ich möchte anknüpfen an das, was der Kollege May gesagt hat. Wir haben momentan eine Regelung im aktuellen NetzDG, dass die Verursacher dessen, worüber wir reden, in der Regel anonym bleiben und keine Strafverfolgung fürchten. Deswegen muss das Ziel sein, strafrechtlich relevante Sachverhalte künftig qualifiziert und systematisch der Strafverfolgung zuzuführen. Mit der Neuregelung im NetzDG wird die Grundlage geschaffen, die ausgeleiteten Inhalte im Bundeskriminalamt zentral zu sichten und die Voraussetzungen zu schaffen, dass Strafverfolgungsmaßnahmen durch die örtlich zuständigen Behörden eingeleitet werden können. Zuständigkeiten von Polizeien und Justiz der Länder bleiben gewahrt. Das BKA nimmt seine Rolle als Zentralstelle nach § 2 BKA-Gesetz wahr. In Ausnahmefällen ist die dann erforderliche Strafverfolgung durch das BKA selbst genauso gesichert wie die Bewertung, ob Maßnahmen zum Schutz von Verfassungsorganen oder solche zur Abwehr von Gefahren des internationalen Terrorismus zu treffen sind. Gleichwohl möchte ich drei Punkte erwähnen, die aus meiner Sicht zu berücksichtigen sind: Erstens, der Bedarf einer Befugnisnorm im Bundeskriminalamtsgesetz zur aktiven Erhebung der IP-Adresse beim Telemedien dienst im Rahmen seiner Zentralstellenzuständigkeiten. Das BKA muss bei Telemedien diensten die zu Identifizierungszwecken wichtige IP-Adresse aktiv erheben dürfen. Es entstünde sonst ein Widerspruch, wenn das BKA den Urheber eines strafbaren Inhaltes aufgrund einer NetzDG-Meldung ermitteln kann, nicht aber, wenn es bei eigenen Recherchen oder durch Mitteilung Dritter auf strafbare Inhalte stößt. Zweitens: Es ist uns wichtig, die Erhebung der IP-Adresse beim Telemediendienst im Rahmen der Strafverfolgung sowie Zentralstellenaufgaben auch künftig nicht unter Richtervorbehalt zu stellen. Die Erhebung der IP-Adresse ist wesentliche Standardmaßnahme bei Aktivitäten im Internet. Die IP-Adresse selbst gibt keinen Aufschluss über den inhaltlichen Gegenstand der konkreten Inanspruchnahme der Telemediendienstleistung, so dass wir hier von einer sehr



geringen Eingriffstiefe reden und wir im Grunde ein Massengeschäft sonst, mit Richtervorbehalt, nicht decken können. Sie ist zudem Vorstufe der sich anschließenden Bestandsdatenabfrage beim TK-Dienst nach § 100j StPO. Diese Maßnahme steht ebenfalls nicht unter Richtervorbehalt. Drittens eine Anregung eines Straftatbestandes, der bestimmte Fallkonstellationen der sogenannten Feindeslisten erfasst: Die bloße Veröffentlichung einer Liste mit personenbezogenen Daten ohne weitergehende Bedrohung bzw. Billigung einer in § 140 StGB aufgenommenen Katalogtat bliebe in der Regel straffrei, weil diese Handlung von der Rechtsänderung nicht umfasst wird. Es bedarf eines neuen Straftatbestandes, der es unter Strafe stellt, personenbezogene Daten zu veröffentlichen, um bei anderen die Bereitschaft zu wecken, Straftaten gegen die betroffenen Personen zu begehen. Und ich glaube, unter den Abgeordneten sind viele dabei, die auf diversen Listen in der Vergangenheit gestanden haben und die auch vom Bundeskriminalamt über diese Umstände informiert werden. Abschließend von mir: Die im aktuellen Gesetzgebungsverfahren vorliegenden Rechtsänderungen sind aus meiner Sicht erforderlich und geeignet, strafrechtliches Handeln aus der scheinbaren Anonymität des Netzes in die Realwelt unserer Rechts- und Werteordnung zu transportieren. Allein dieser Umstand kann generalpräventiv wirken. Finale Bemerkung – anknüpfend an Herrn May: Wir reden über ein Massengeschäft mit einer ganz hohen Zeitkritikalität der Ermittlungsansätze, die wir so schnell wie möglich umsetzen müssen, damit dieses Gesetz wirken kann. Vielen Dank für die Aufmerksamkeit.

Der **stellvertretende Vorsitzende**: Vielen Dank, Herr Peter. Als Letztes hat das Wort Herr Ritgen. Bitte schön.

SV **Dr. Klaus Ritgen**: Vielen Dank, Herr Vorsitzender, als Vertreter des dritten kommunalen Spitzenverbandes darf ich Ihre Zeit noch stärker schonen als es der Kollege Lübking gemacht hat. Ich kann mich als Vertreter des Landkreistages den Ausführungen des Deutschen Städtetages und des Deutschen Städte- und Gemeindebundes nur anschließen. Wir begrüßen diesen Gesetzentwurf sehr. Wir danken den Fraktionen und der Bundesregierung, dass sie sich dieses Ziels

angenommen haben, und hoffen, dass insbesondere die Vorschläge, die zur Änderung des materiellen Strafrechts unterbreitet worden sind, so verwirklicht werden, wie sie hier vorliegen. Das gilt insbesondere auch für den vorgeschlagenen § 241 StGB. Den Ausführungen von Herrn Hartleb kann ich mich da auch anschließen. Vielen Dank.

Der **stellvertretende Vorsitzende**: Vielen Dank. Damit sind wir am Ende Ihrer Eingangsstatements und kommen in die erste Fragerunde. Da liegen inzwischen einige Wortmeldungen vor. Als erstes möchte ich das Wort Herrn Movassat geben.

Abg. **Niema Movassat** (DIE LINKE.): Vielen Dank für Ihre Inputs. Meine erste Frage richtet sich an Herrn Conen und an Professor Engländer. Sie haben insbesondere auch zu §§ 140 und 241 StGB kritische Punkte angemerkt. Da teilen wir als Fraktion DIE LINKE. auch einiges, insbesondere dass bei der Billigung von Straftaten schon eine Strafbarkeit vorliegt, ohne dass überhaupt eine andere Straftat vorliegt, die man gebilligt hat. Das ist völlig abstrakt, und möglicherweise haben Leute dann auch Angst, etwas zu sagen, weil sie die Sorge haben, dass sie sich strafrechtlich relevant äußern. Und im vorgeschlagenen § 241 StGB muss man schon sagen, dass dadurch, dass auch die Bedrohung der körperliche Unversehrtheit drin ist, auch typische Kneipen- oder Schulhofsprüche relativ schnell in den Anwendungsbereich fallen könnten. Die Gefahr der Überlastung der Staatsanwaltschaften wurde ja auch angesprochen. Vielleicht könnten Sie beide nochmal zu diesen Fragen etwas sagen, insbesondere auch zu der Vorverlagerung der Strafbarkeit und dem ultima-ratio-Prinzip? Das sind Punkte, die für mich interessant wären.

Der **stellvertretende Vorsitzende**: Vielen Dank, dann Herr Jung.

Abg. **Ingmar Jung** (CDU/CSU): Vielen Dank, Herr Vorsitzender. Ich bin jetzt seit zweieinhalb Jahren im Bundestag und etwas irritiert, dass ich zum ersten Mal in dieselbe Richtung frage wie Herr Movassat. Das ist uns beiden noch nie passiert, glaube ich. In der Tat sind das die beiden Punkte, bei denen ich auch noch eine Nachfrage hätte an Herrn Professor Engländer. Sie haben am Ende Ihrer Stellungnahme zwei kritische Punkte aus Zeitgründen wahrscheinlich nur noch verkürzt



ansprechen können, deswegen möchte ich da nochmal kurz nachfragen. Zunächst bei § 140 StGB. Mir geht es darum, was das bedeutet, wenn man eine Tat, die möglicherweise tatsächlich noch nicht begangen oder versucht wurde, billigen muss. Da frage ich mich, was muss man dafür tun? Ich brauche irgendwie eine öffentliche Friedensstörung. Wenn ich das im Internet lese und dann zu Hause laut jubele und klatsche, wird es wohl noch nicht reichen, aber wie weit muss das nach außen treten? Reicht da der Like unter dem Facebook-Post? Muss ich das noch besonders begründen? Muss ich noch mehr zeigen? Also, wie wäre Ihre Einschätzung? Wie weit muss man gehen, um dieses Tatbestandsmerkmal an der Stelle zu erfüllen? Beim vorgeschlagenen § 241 StGB haben Sie auch angedeutet, dass Sie sich eine etwas restriktivere Ausgestaltung gewünscht hätten. Wie würden Sie vorschlagen, dort vorzugehen? Auch da frage ich mich ein Stück weit, was bedeutet das denn eigentlich, zu drohen mit Straftaten gegen körperliche Unversehrtheit und Sachen von bedeutendem Wert? Ist damit wirklich schon der klassische Satz „lass mal vor die Türe gehen“ gemeint oder „ich zerkratze dir dein Auto“, oder meinen Sie auch, dass man dort mehr braucht, um den Tatbestand zu erfüllen?

Der **stellvertretende Vorsitzende**: Vielen Dank, als nächstes Herr Fechner.

Abg. **Dr. Johannes Fechner** (SPD): Vielen Dank, Herr Vorsitzender. Auch von mir Dank an alle Sachverständigen. Ich hätte eine Frage, die würde ich gerne an Frau Ballon und Herrn Hartmann richten, weil sie beide dieses Thema schon angesprochen hatten, aber wegen der Zeit nicht allzu viel dazu sagen konnten. Ein Thema, das ich auch als zentrales Problem ansehe, dass nämlich viele Unternehmen unter Verweis auf internationales Recht die Behörden nicht beauskunften und damit vieles ins Leere läuft. Da würde mich Ihre Praxiserfahrung interessieren. Ist das ein Problem? Vielleicht können Sie es auch mit Zahlen belegen? Und was wäre aus Ihrer Sicht dann die Lösung, wie könnten wir das Marktortprinzip hier bei uns verankern?

Der **stellvertretende Vorsitzende**: Vielen Dank, Herr Hoffmann.

Abg. **Alexander Hoffmann** (CDU/CSU): Vielen Dank, Herr Vorsitzender. Ich habe zwei Fragen. Eine zunächst an den Herrn Professor Engländer: Sie haben vorhin ausdrücklich begrüßt, dass eine Erweiterung auf die kommunalpolitische Ebene stattfindet, speziell auch im Rahmen des § 188 StGB. Da würde mich jetzt die Frage interessieren, ob aus Ihrer Sicht die Erweiterung bei § 188 auf die kommunalpolitische Ebene doch eigentlich nichts an der praktischen Bedeutungslosigkeit der Norm ändert. Die zweite Frage würde ich gerne an Herrn Hartleb stellen. Herr Hartleb, Sie wissen, dass es einen Vorschlag aus dem bayrischen Justizministerium gibt, der eine grundlegende Reform der Beleidigungsdelikte vorsieht. Die Idee ist, das alles in § 188 StGB zu bündeln. Mich würde interessieren, ob Sie das nicht für praxistauglich halten – ich habe vorhin so im Unterton eine gewisse Kritik rausgehört am aktuellen Entwurf – und wäre es nicht sinnvoll, genau das in den aktuellen Entwurf zu integrieren? Danke.

Der **stellvertretende Vorsitzende**: Vielen Dank, Frau Künast.

Abg. **Renate Künast** (BÜNDNIS 90/DIE GRÜNEN): Danke, Herr Vorsitzender. Lassen Sie mich vorab zwei Dinge antippen. Einmal, ich bedauere, dass der Bundesdatenschutzbeauftragte nicht hier ist, der hätte meines Erachtens hierher gehört, auch vor die Klammer. Zweitens, ich werde mich jetzt nicht weiter zu Strafrechtsfragen äußern, weil wir einen Änderungsantrag gemacht haben, der liegt vor, der strikt nach dem Ultima-Ratio-Grundsatz geht und Vorschläge von Bundesrat, DRV und aus Bayern aufnimmt – was eine Schnittmenge mit einigen Sachverständigen hier hat bezüglich der Anregungen zu verschiedenen Straftatbeständen. Meine beiden Fragen gehen an Herrn Bäcker und Herrn Peter. Ich will mich konzentrieren auf die Frage der Meldepflicht und wie das Verfahren ausgestaltet ist. Wie muss die Meldepflicht eigentlich genau ausgestaltet sein im Mindeststandard, damit sie rechtsstaatlich einwandfrei und zugleich effektiv ist? Das sind ja zwei Dinge, unter denen das Ganze nur Sinn macht. Zweitens, speziell zum Schutz der gemeldeten Daten beim BKA – Sie haben gesagt: zu früh, zu viel, aber unabhängig von der Frage, ich meine auch zu früh, zu viel, Zweistufensystem wäre besser –



aber, wenn die Daten da sind, was ist die konkrete Aufgabe des BKA? Wie geht die Löschung nach Aufarbeitung? Zu welchen Analysen darf man die Daten benutzen? Wie geht die Weiterleitung an die Länder? Ich frage das insbesondere, weil ja die Frage ist, selbst bei Strafverfahren, die auch irgendwann Löschungsfristen haben, wie viel bleibt davon beim BKA? Oder, wenn man keinen Tatverdacht annimmt, aber jemand sich in rechtsextremen Kreisen aufhält? Bleiben die Daten dann da oder werden die gelöscht? Was meine Erwartung wäre. Deshalb also: welche Aufarbeitung, welche Analyse, welche Weiterleitung und Löschung? Danke.

Der **stellvertretende Vorsitzende**: Vielen Dank. Herr Post.

Abg. **Florian Post** (SPD): Danke, Herr Vorsitzender. Meine Frage bezieht sich auch auf die Meldepflicht. Eine Frage an Herrn Hartmann und die zweite Frage an Frau Ballon. Die erste Frage an Herrn Hartmann: Kollegin Künast hat es erwähnt und Sie haben es auch begrüßt, von verschiedenen Seiten wird ein zweistufiges Verfahren vorgeschlagen. Das heißt, zunächst Inhalt an Strafverfolgungsbehörden weiterleiten, und erst wenn der Anfangsverdacht vorliegt, dann Ermittlungen aufnehmen und dann auch IP-Adresse und Portnummer übermitteln. Wie bewerten Sie das? Es wurde auch schon von Kollegen von Ihnen angesprochen, das Stichwort „Aktualität der IP-Adresse“. Kann dann überhaupt noch eine effektive Strafverfolgung stattfinden? Und natürlich auch speziell zur Prozessökonomie bei diesem Vorschlag, wenn Sie sich dazu nochmal äußern würden. An Frau Ballon habe ich die Frage: Wie würde sich ein solches zweistufiges Verfahren Ihrer Ansicht nach auswirken auf die Erhöhung der Strafverfolgung? Auch datenschutzrechtliche Aspekte würden mich da interessieren, wie Sie die aus Ihrer Sicht beurteilen. Und wie wirkt sich ein solches Verfahren hinsichtlich der Akzeptanz aus? Danke.

Der **stellvertretende Vorsitzende**: Vielen Dank, Herr Post. Und als nächstes steht auf meiner Liste Herr Reusch.

Abg. **Roman Reusch** (AfD): Vielen Dank. Ich habe eine Frage an die Herren Hartleb und Hartmann. Das betrifft die zahlenmäßige Verteilung der Delikte, nach Ihrer praktischen Erfahrung,

zwischen den reinen Beleidigungsdelikten und den weiteren hier in Rede stehenden Tatbeständen.

Der **stellvertretende Vorsitzende**: Vielen Dank. Herr Martens, bitte schön.

Abg. **Dr. Jürgen Martens** (FDP): Vielen Dank, Herr Vorsitzender. Ich habe auch noch zwei Fragen an Herrn Lesch. Wie auch bei Frau Künast geht es um die Meldepflichten. Wir haben die Meldepflicht nach § 3a im Netzwerkdurchsetzungsgesetz, die scheint nicht ganz unproblematisch zu sein aus Sicht der Betreiber. Wo könnte es denn praktisch haken bei der Erfüllung der Meldepflicht? Zweitens gibt es den § 15b des Telemediengesetzes. Da gab es ja auch heftige Kritik an der Konstruktion der Regelung, das heißt, jetzt sollen nicht die verschlüsselten Daten, sondern nur die anderen Daten gemeldet werden, und ein Straftatenkatalog soll das Ganze begrenzen, und ein Richtervorbehalt soll das einschränken. Reicht das jetzt aus, um die geäußerten Bedenken aus Sicht der Betreiber auszuräumen?

Der **stellvertretende Vorsitzende**: Vielen Dank. Dann haben wir jetzt das Ende der ersten Fragerunde und kommen zur Beantwortung der Fragen. Als erstes, wenn wir rückwärts alphabetisch vorgehen, wäre hiernach Herr Peter mit der Antwort auf die Frage von Frau Künast an der Reihe. Bitte schön, Sie haben das Wort.

SV **Jürgen Peter**: Ja, das mache ich gerne. Ich will vorweg stellen, dass wir allen Bedarfen dessen, was Datenschutz formuliert, in vollem Umfang Rechnung tragen. Das tun wir in dem bereits von Herrn May erwähnten NCMEC-Prozess. Und die Regelungen, unter denen das Bundeskriminalamt sowohl als Strafverfolgungsbehörde als auch als Zentralstelle Daten weiterverarbeiten und speichern darf, ergeben sich aus den jetzigen Regelungen des BKA-Gesetzes und werden auch künftig keine anderen sein. Das heißt, im Kern ist die Weiterverarbeitung der Daten als Zentralstelle im § 18 erwähnt. Die Rolle des BKA im Zusammenhang mit noch feiner zu definierenden Schwerpunktstaatsanwaltschaften – zwei sitzen hier – wird gerade modelliert. Das heißt, die Rolle des BKA im ersten Angriff ist, mittels Content und der weiteren ausgeleiteten Daten möglichst schnell zu identifizieren, um einen Gerichtsstand feststellen zu können, weil wir ansonsten in die



Polizei- und Justizzuständigkeiten der Länder nicht vordringen. Das heißt, die weitere Verarbeitung der Daten in strafprozessualer und kriminalpolizeilicher Hinsicht erfolgt durch die dann beauftragten Polizeibehörden der Länder, wiederum im Rahmen ihrer Befugnisse. Das Datenvolumen, das bei uns bleiben wird, das sind im Grunde genommen Metadaten auf der Vorgangsebene oder solche Inhaltsdaten, die wir weiter verarbeiten, weil in der Erstbearbeitung im BKA möglicherweise Kreuztreffer erzielt worden sind. Das ist für uns wichtig, weil der Gesamtbekämpfungsansatz PMK –rechts [Politisch motivierte Kriminalität – rechts] nicht nur aus der Änderung des NetzDG besteht, sondern auch aus dem personenbezogenen Ansatz und dem System der Netzwerkerkennung. Ich mache es konkret: Wenn anhand eines „Nicknames“ und möglicherweise anhand eines ermittelten Namens ein Kreuztreffer in Dateien des Bundeskriminalamtes im Bereich der politisch motivierten Kriminalität festgestellt wird, dann ist es selbstverständlich so, dass dieser Vorgang dort beigespeichert wird. Auf der anderen Seite werden all die Vorgänge, die strafrechtlich als völlig irrelevant bewertet werden, auch keiner weiteren Verarbeitung unterzogen. Das ist die Grundrichtung, die im BKA-Gesetz geregelt ist, die wir in dem Prozessverfahren – wo wir das mit einem ausgewählten Anbieter in einem Pilotverfahren modellieren werden, um dann künftig weitere Anbieter anzufanschen, um diesen Geschäftsprozess sukzessive in Gang zu setzen, wo wir das eine oder andere auch an Erfahrungen sammeln. Wir können momentan noch nicht alle praktischen Fragen des Workflows beantworten. Wir haben aber einen sehr gut modellierten Prozess, den wir zusammen mit der ZIT [Zentralstelle zur Bekämpfung der Internetkriminalität] in Frankfurt und der ZAC [Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen] in Köln bereits in Abstimmung haben und der sehr stark auf Automatisierung unter Einhaltung aller datenschutzspezifischen Forderungen besteht.

Der **stellvertretende Vorsitzende**: Vielen Dank, Herr Peter. Als nächstes Herr Lesch mit den beiden Antworten auf die Fragen von Herrn Martens.

SV **Henning Lesch**: Vielen Dank für die beiden Fragen. Starten wir mal mit der Problematik der

sogenannten Meldepflicht. Ich hatte das ja im Eingangsstatement bereits grundsätzlich angesprochen. Es findet keine Vorabprüfung durch eine Behörde, sei es Staatsanwaltschaft oder ein Gericht, statt. Die Entscheidung obliegt allein den Unternehmen, was sie melden und wie sie diese Inhalte bewerten. Das heißt aber, gleichzeitig schauen wir uns die Taten an, die gemeint sind. Es geht um Hassrede, es geht um Beleidigung, es geht um Verleumdung, das heißt, wir sind auch immer in der Abwägung mit Meinungsrelevanz oder mit dem Grundrecht aus Artikel 5 Grundgesetz. Das heißt, auch beispielsweise Satire oder ähnliches muss einbezogen werden, dann wäre es wiederum in Ordnung und dürfte nicht gemeldet und gelöscht werden. Die Problematik ist, es handelt sich ja nicht nur um offensichtliche Fälle, sondern gerade auch um Grenzfälle. Die Entscheidung der Bewertung dieser Inhalte, sei es Bild, Ton oder Video, obliegt den Unternehmen. Auf Basis dieser Entscheidung werden dann die Meldungen an das BKA gemacht. Das ist eine Kernproblematik, die dieser Regelung immanent ist. Die Meldepflicht allein wird ja auch nicht zu einer effektiven Bekämpfung von Rechtsextremismus oder Hass im Internet beitragen. Ich glaube, man muss auch berücksichtigen, im Fokus stehen ja drei große Anbieter. Zahlen waren schon verschiedentlich in der Öffentlichkeit, den Medien zu entnehmen. Wir gehen davon aus – drei große Unternehmen. Geschätzt dürfte das nach der jetzigen gesetzlichen Meldeverpflichtung zu etwa einer Millionen Meldungen im Jahr führen. Es stellt sich die Frage: Wie will man dann effektiv und effizient mit diesen Meldungen bei den Staatsanwaltschaften, beim BKA und bei den Gerichten umgehen? Ich glaube, klar wird damit: Was eigentlich fehlt, ist ein stimmiges Gesamtkonzept, wie wir die Hasskriminalität im Netz effektiv und auch nachhaltig bekämpfen können. Dazu gehört sicherlich auch, dass die Straftaten zur Anzeige gebracht werden, dass sie konsequent verfolgt werden, und natürlich auch, dass die Täter vor das Gericht gestellt und damit geahndet werden für ihre Taten. Ich denke, das ist wichtig. Und dementsprechend ist es auch wichtig, die Strafverfolgungsbehörden personell und technisch angemessen auszustatten. Das ist rechtspolitisch notwendig und auch aus Gründen der Spezial- und Generalprävention geboten. Was sollte



geändert werden? Vielleicht sollte man die Meldepflicht eingrenzen auf besonders demokratieschädliche Straftatbestände – Volksverhetzung, Propaganda verfassungswidriger Organisationen. Gleichzeitig keine proaktive Ausleitung von Inhaltsnutzerdaten, IP-Adressen und Ortnummern. Hier sollte sichergestellt sein, dass vorher eine Prüfung durch Gericht oder Staatsanwaltschaft stattfindet. Es wurde auch angesprochen, Schwerpunktstaatsanwaltschaften beispielsweise für Hasskriminalität. Hier wurde bereits die ZAC erwähnt. Es gibt auch Initiativen in Nordrhein-Westfalen, die löschen und verfolgen. Das sind gute Ansätze, und die Erfahrung von uns damit ist bislang auch sehr gut. Was sollte noch passieren? Die Erstattung von Strafanzeigen sollte einfacher werden und leichter. Beispielsweise die Möglichkeit, online Strafanzeige zu erstatten, und entsprechende Musterformulare. Das würde vieles vereinfachen. Das zu dieser Frage. Ich hatte noch die Frage nach der Regelung mit den Passwörtern. Eingangs hatte ich bereits erwähnt, dass die Diskussion um die Passwörter sehr stark allein darauf fokussiert. Ich hatte auch angesprochen, dass es sich nicht nur auf Passwörter bezieht, sondern auch auf andere Zugangsdaten, mit denen Zugriff auf Endgeräte oder Speicherungseinrichtungen genommen werden kann. Genutzt werden dabei auch, so sieht es das Gesetz vor, unternehmensinterne Datenquellen. Die Regelung ist problematisch, weil sie eben nicht nur den Zugriff auf den Account und seinen Inhalt, sondern eigentlich auch gleichzeitig die komplette Übernahme der Online-Identität des Betroffenen ermöglicht. Das ist eigentlich wie eine virtuelle Hausdurchsuchung. Aber nicht nur das, es ermöglicht ja auch gleichzeitig den Zugriff auf sämtliche Kommunikation und Inhalte. Und wer die Identität übernommen hat, kann diese Inhalte auch verändern. Was sollte gemacht werden? Ich denke, es sollte klargestellt werden, dass die Diensteanbieter keine Mitwirkungspflicht bei der Entschlüsselung von Passwörtern haben, dass sie keine Informationen über eingesetzte Verschlüsselungsverfahren offenbaren müssen und auch klargestellt werden, dass sie nicht zu einem Zurücksetzen des Passworts verpflichtet sind. Gleichzeitig sollten die sogenannte Nutzung der sämtlichen unternehmensinternen Datenquellen für die Ausleitung und die Vorschrift § 15b

gestrichen werden, da sehen wir den Verweis auf den Straftatenkatalog von § 100b Absatz 1 StPO, darauf wird Bezug genommen. Die Regelung in § 15b TMG Absatz 2 Nr. 1 verweist aber nur auf § 100b Absatz 2 der StPO und damit auf die Onlinedurchsuchung und den dortigen Straftatenkatalog, aber eben nur auf den Straftatenkatalog. Es wäre gut und wichtig, ebenfalls auf § 100b Absatz 1 StPO Bezug zu nehmen, damit würde eine Subsidiarität gewährleistet sein. Das heißt, diese Daten sind nur dann herauszugeben oder die Regelung darf nur benutzt werden, wenn keine anderen Maßnahmen erfolgversprechend sind oder keine Aussicht auf Erfolg besteht oder wenn keine anderen Ermittlungsmaßnahmen möglich sind und gleichzeitig der Tatverdacht für das Vorliegen einer besonders schweren Straftat besteht. Das wäre konsistent und würde sich sehr stark an der Online-Durchsuchung orientieren und deren Maßstäbe ansetzen. Vielen Dank.

Der stellvertretende Vorsitzende: Vielen Dank, Herr Lesch. Als nächstes hat das Wort Herr Hartmann mit den Antworten auf die Fragen von Herrn Fechner, Herrn Post und Herrn Reusch. Bitte schön.

SV Markus Hartmann: Vielen Dank. Ich beginne genau in dieser Reihenfolge. Zunächst auf die Frage von Herrn Dr. Fechner, ob wir Praxiserfahrungen zu den Auslandsbezügen haben. Ja, wir haben versucht, die uns vorliegenden Verfahren statistisch auszuwerten. Ich muss einräumen, ob das statistisch wissenschaftlich valide ist, vermag ich nicht zu beurteilen. Es gibt aber einen sehr konkreten Anhalt über die Situation, und danach zeigt sich, dass wir in 98 Prozent der Verfahren Auskünfte der Netzbetreiber benötigen. Im Grunde kann man sagen, ohne entsprechende Auskünfte sind erfolgreiche Ermittlungen nicht zu führen. Wir haben solche Auskunftersuchen auch regelmäßig gestellt bzw. so lange gestellt, bis sie sich ersichtlich als fruchtlos erwiesen haben. Diese Ersuchen sind im Wesentlichen an unterschiedliche US-amerikanische Provider gegangen. Beim Auskunftsverhalten haben wir unterschiedliche Ergebnisse gesehen. In der Praxiserfahrung sind von Google sehr viele Ersuchen beantwortet worden, bei Facebook war es gelegentlich der Fall; im Übrigen sind die Ersuchen nicht beantwortet



worden. Insgesamt, rein statistisch, ist nur jedes 20. Ersuchen, das wir im Rahmen der statistischen Auswertung einbezogen haben, von den Netzwerkbetreibern beantwortet worden. Der wesentliche Grund, warum nicht geantwortet wird, ist nicht der Unwille der Provider, sondern der Hinweis darauf, dass nach der rechtlichen Auffassung der Provider der Datenspeicherort im Ausland belegen und insofern ein förmliches Rechtshilfeersuchen erforderlich sei. Das korrespondiert oft auch mit der Vorschrift der derzeitigen Fassung von § 5 Absatz 2 Satz 2 NetzDG, die eben nur vorsieht, dass die Medien oder die sozialen Netzwerke antworten müssen, aber nicht, dass sie inhaltlich qualifiziert Auskünfte erteilen müssen. Das führt in einer Vielzahl von Fällen zu einem – ich will es ganz deutlich sagen – „Vor-die-Wand-Laufen“ der Ermittlungen, weil Antworten im justiziellen Rechtshilfewege allenfalls nach Monaten zu erlangen sind. Im Ergebnis sind damit die Spuren im Internet kalt und Ermittlungsverfahren nicht mehr erfolgreich zu Ende zu führen. Ich hatte in meinem Eingangsstatement als Lösungsansatz auf das Marktortprinzip hingewiesen. Mir sind die europarechtlichen Komplikationen durchaus bewusst, und wir sehen ja auch am NetzDG-Änderungsentwurf Teil 2, der ja auch in der Entwurfsfassung schon präsent ist, dass dort Anpassungen eher hinsichtlich des Herkunftslandprinzips, etwa bezüglich der Videoplattformen, vorgenommen werden sollen. Deswegen muss ein Lösungsansatz sein, eine europarechtliche oder europäisch vereinheitlichte Lösung zu finden, einen Rechts- und Handlungsrahmen. Wir haben bei der – noch andauernden – Diskussion zu den E-Evidence-Vorschlägen der Kommission dazu einiges gesehen. Mir sind die Komplikationen und die langen Verfahrensdauern durchaus klar, aber wir brauchen mittelfristig sicher einen eindeutigen, europarechtlich zumindest tragfähigen Rahmen über das Europarecht hinaus. Der Cloud Act der Vereinigten Staaten sieht ja auch Kooperationsmöglichkeiten vor. Wir werden im Ergebnis ohne eine direkte Zugriffsmöglichkeit auf die Daten der Provider, unabhängig von deren physischem Besitz, wenn man so will, oder dem physischen Datenspeicherort in vielen Fällen nicht weiterkommen. Der zweite an mich gerichtete Fragenkomplex war der von Herrn Abgeordneten

Post im Hinblick auf die Zweistufigkeit der Verfahren, ob das unter prozessökonomischen Gesichtspunkten denkbar ist. Lassen Sie mich vielleicht erstmals ganz grundsätzlich sagen, der schon öfter angesprochene Bereich der Zeitkritikalität ist auch hier für Ermittlungserfolge entscheidend. Insofern ist jede zusätzliche Hürde, die wir aufstellen, erstmal ein Schritt weg von erfolgreicher Ermittlungsfähigkeit. Das heißt, es wird bei der Ausgestaltung vor allen Dingen darauf ankommen, dass wir sehr effektive Verfahren sehen. Ich sehe ein großes Gewicht darin, dass die praktische Ausgestaltung des Verfahrens eine umfassende Digitalisierung aller Vorgänge vorsehen muss. Wenn wir nach klassischer Justizart Papierakten und Aktenwagen heranziehen wollen, um diese Verfahren zu bearbeiten, werden wir nicht erfolgreich sein. Das heißt umgekehrt aber, wir haben Deliktsbereiche, wo wir im Rahmen der Meinungsfreiheit natürlich auch grundrechtliche Positionen von sehr hoher Bedeutung tangieren. Deswegen, möchte ich umgekehrt auch unterstreichen, müssen wir uns auch nicht nur prozessökonomischen Grundsätzen stellen, sondern auch entsprechende Ausgleichsfunktionen finden. Deswegen glaube ich, dass wir mehrere Maßnahmen vornehmen können, die, wenn nicht das klassische zweistufige Modell – Stichwort Doppeltür – umsetzen, so doch einen hohen Standard in diese Richtung etablieren können. Das kann etwa ein hohes Maß an Integration polizeilicher und justizieller Arbeit etwa in Schulungen und Kategorisierungen sein. Vereinfacht gesagt, nicht jedes dieser Delikte ist höchst kompliziert. Etwa im Bereich des Verwendens von Kennzeichen verfassungswidriger Organisationen ist es relativ kategorisierbar, ob ein angezeigtes Symbol strafbar ist oder nicht. Wir können durch sorgfältige Vorbereitung – was Herr Peter angesprochen hat, da sind wir ja auch gemeinsam mit der ZIT und dem BKA schon dabei – sehr vieles handlungssicher machen. Ich persönlich habe auch eine hohe Sympathie für das auch schon mal angeklingene Quick-Freeze-Verfahren, weil es natürlich keine echte Zweistufigkeit, aber einen Zwischenschritt bedeutet. Die Daten werden angeliefert, sie werden aber nur dann strafprozessual verwertbar zugeordnet, wenn tatsächlich ein Anfangsverdacht nach diesen geschulten Prüfkriterien besteht. Ich kann mir



durchaus vorstellen, dass man über diese rechtliche Neuerung dann auch einen effektiven Ausgleich zwischen Prozessökonomie und den Erfordernissen, die die Meinungsfreiheit uns vorgibt, schaffen kann. Also Digitalisierung, Schulung, Quick Freeze sind sicher Maßnahmen, mit denen wir einen Ausgleich aller beteiligten Interessen schaffen können, ohne allzu viel an Prozessökonomie aufzugeben. Die letzte Frage betraf die zahlenmäßige Verteilung der Verfahren in den unterschiedlichen hier diskutierten Deliktssklassen. Da muss ich leider mangels statistischer Daten eine Antwort schuldig bleiben. Wir sind als Zentralstelle nicht flächendeckend für alle Delikte im Bereich der digitalen Hasskriminalität zuständig, sondern nur für das, was die unterschiedlichen, uns die Aufgaben zuweisenden Erlasse als sogenannte herausgehobene Verfahren qualifizieren. Im Übrigen läuft die Verfolgung bei den Staatsanwaltschaften vor Ort. Das sind allein für Nordrhein-Westfalen 19 Behörden, zu denen mir keine statistischen Erhebungsdaten vorliegen, wie sich die Delikte insgesamt im Bereich der politisch motivierten Kriminalität verteilen. Deswegen vermag ich die dritte Frage nicht valide aus eigener Sachkunde zu beurteilen. Danke sehr.

Der **stellvertretende Vorsitzende**: Vielen Dank, Herr Hartmann. Der Hinweis, dass der Aktenwagen nicht benötigt wird, heißt sicher nicht, dass die Staatsanwaltschaft Köln ihre Raumanforderungen herabsetzt?

SV **Markus Hartmann**: Ich würde das sogar anders sehen wollen, weil die vielen neuen Kollegen, die ja hoffentlich dazukommen, irgendwo sitzen müssen.

Der **stellvertretende Vorsitzende**: Vielen Dank, Herr Hartmann. Als nächstes hat das Wort Herr Hartleb mit den Antworten auf die Fragen von Herrn Hoffmann und Herrn Reusch.

SV **Klaus-Dieter Hartleb**: Danke. Zunächst zur Frage des Herrn Hoffmann. Der bayerische Diskussionsentwurf, der macht im Wesentlichen einen Unterschied in Bezug auf § 188 StGB, in dem der Entwurf weitergeht. Der Gesetzesentwurf sagt da an einer Stelle, diese Vorschrift sei bedeutungslos. Es seien lediglich bundesweit fünf Verurteilungen in den Jahren 2015 bis 2017 erfolgt. Das, denke ich, trifft zu, das deckt sich

auch mit meiner Erfahrung. In 16 Jahren ausschließlich staatsanwaltlicher oder Tätigkeit als Amtsrichter habe ich nicht eine Anklage, Verurteilung oder Strafbefehl in diesem Bereich gesehen. Würde sich jetzt mit den vorliegenden Gesetzesentwürfen etwas an der Bedeutungslosigkeit ändern? Ein bisschen, denn man macht ja hier das absolute Antragsdelikt zu einem relativen Antragsdelikt, und es zeigt sich ja auch, dass Politiker oft auf die Stellung eines Strafantrags verzichten. Das greift aber trotzdem zu kurz, weil der Tatbestand meines Erachtens zu eng gefasst ist. Warum? Erstmal ist er nur auf die üble Nachrede und die Verleumdung, nicht aber auf die Beleidigung gemünzt. Die Beleidigung umfasst in dem Bereich aber die Vielzahl der Ehrverletzungsdelikte zum Nachteil von Politikern. Dann haben wir noch in der Vorschrift ein Merkmal, dass das öffentliche Wirken der Betroffenen Personen erheblich erschwert werden muss. Das engt den Tatbestand auch erheblich ein, da haben wir einen unbestimmten Rechtsbegriff, mit dem natürlich Bewertungsunsicherheiten einhergehen. Außerdem haben wir da noch eine Rechtsprechung aus den achtziger Jahren, die sagt, es kommt allein auf den Inhalt dieses Posts an und es kommt nicht auf die Begleitumstände an. Es ist egal, welche Verbreitung dieser Post etwa erfährt. Das ist natürlich heute, im Zeitalter der sozialen Medien, der massenhaften Verbreitung solcher Beleidigungsdelikte nicht mehr zeitgemäß. Da können auch niederschwellige Äußerungen, wenn sie in Massen auftreten, geeignet sein, das öffentliche Wirken eines Politikers erheblich zu erschweren. Man denke nur an den Fall eines Shitstorms oder eines orchestrierten Shitstorms. Da ist jeder Kommentar an sich möglicherweise nicht so erheblich, aber in der Gesamtheit sind die dann schon erheblich. Dieses Merkmal sollte, meines Erachtens, in Wegfall geraten, um hier einen besseren Schutz der Politiker und Kommunalpolitiker herbeizuführen. Insgesamt zu dem Diskussionsentwurf – den kann ich natürlich in der Kürze der Zeit nicht umfassend würdigen. Der geht von dem Grundsatz aus, dass ein modernes Beleidigungsstrafrecht zu schaffen sei, denn es ist nicht mehr zeitgemäß. In der Tat wurden die zentralen Regelungen – Beleidigung, Verleumdung und üble Nachrede – seit 150 Jahren nicht mehr verändert. Das sehen wir auch in unserer täglichen Arbeit,



dass sie da in gewissen Bereichen der Realität hinterherhängen. Früher gab es die überkommene Vorstellung einer Beleidigung im Zwei-Personen-Verhältnis, heute passiert es im Internet massenhaft. Durch die Funktion Kommentare, Likes, Retweets erfährt eine Beleidigung eine massenhafte Verbreitung. Das muss man sehen. Insofern hat dieser Gesetzentwurf wirklich drei Bereiche herausgenommen, die angehangsbedürftig sind. Erstmal die große Verbreitung – gut, das wurde in den Gesetzentwurf, den wir hier vorliegen haben, übernommen. Dann diese Thematik, Hate Speech und Cybermobbing – das sind auch zwei drängende Probleme der Zeit im Internet: Hate Speech – die gruppenbezogene Menschenfeindlichkeit, Cybermobbing – eher die individuelle Menschenfeindlichkeit. Also, starker Bezug dann auch zu Hate Speech hat das Cybermobbing, so dass ich das letztlich schlüssig finde. Der Schutz der Kommunalpolitiker ist meines Erachtens, wie ich gerade ausgeführt habe, besser gemacht. Allerdings denke ich, dass man hier dem Vorschlag des Bundesrates doch näher treten sollte und eine Konkretisierung machen müsste, wer ist eine politisch, auch kommunalpolitisch, im Leben des Volkes stehende Person ist. Da, denke ich, müsste schon Klarheit geschaffen werden. Das lädt auch zum Missbrauch ein, indem Mitglieder von Bürgerinitiativen, das will ich nicht schlechtreden – die sollten ja nicht vom Schutz umfasst sein. Man denke auch an rechte oder rechtsradikale Bürgerinitiativen, die sich dann nach dem Motto: „Wir sind das Volk“ auf diese Vorschrift berufen, was dann erhebliches Missbrauchspotential – oder da müssten wir bei der Staatsanwaltschaft sehr viele Einstellungsbegründungen machen, die gut begründen und das gibt erhebliches Konfliktpotential. Zur Frage des Herrn Reusch: Da geht es mir wie dem Herrn Hartmann, da kann ich valide Zahlen derzeit nicht präsentieren. Nur ganz allgemein: In der PKS 2017 bis 2019 in Bayern ist die Volksverhetzung prominent unter den Hate-Speech-Tatbeständen, mit 80 Prozent. Wir haben jetzt Anfang des Jahres in Bayern, wie gesagt, 31 Sonderdezernate eingerichtet. Am Ende des Jahres wird man da eine validere Bewertungsgrundlage haben, indem ich das dann einzeln bewerten kann, welche Delikte hier aufgelaufen sind. Aber derzeit kann ich dazu leider nicht dezidiert Stellung nehmen.

Der **stellvertretende Vorsitzende**: Vielen Dank, Herr Hartleb. Als nächstes hat das Wort Herr Engländer mit den Antworten auf die Fragen von Herrn Jung, Herrn Movassat und Herrn Hoffmann.

SV Prof. Dr. Armin Engländer: Ich fange an mit dem § 140 StGB – mit dem Billigen. Da war die Frage, was gehört eigentlich zum Billigen dazu? Zum Billigen selbst erst einmal nicht allzu viel. Die Anforderungen sind ausgesprochen gering. Billigen heißt einfach Gutheißen der Tat. Das kann natürlich auch ohne weiteres vorliegen durch den berühmten Facebook-Like – Daumen nach oben –, durch das Beifallklatschen. All das erfüllt unproblematisch den Begriff des Billigen. Jetzt war ja die Frage, was passiert, wenn jemand das zu Hause im stillen Kämmerlein macht? Das ist natürlich dann kein Problem, weil der § 140 StGB insoweit noch die zusätzliche Anforderung hat, dass das Ganze öffentlich, in einer Versammlung oder durch das Verbreiten von Schriften geschehen muss. Aber die Voraussetzung ist natürlich, wenn wir etwa an den Facebook-Like denken, auch einigermaßen schnell erfüllt. Solange ich keine sehr kleine, abgegrenzte Gruppe habe, sind wir dann schnell in diesem Bereich der Öffentlichkeit drin. Insoweit würde das genügen. Und dann hängt die Strafbarkeitsrestriktion an der Stelle an dem sehr unbestimmten Begriff der Störung des öffentlichen Friedens. Das im Hinblick auf ein Verhalten, das weit im Vorfeld einer möglichen Straftat liegt – einer Straftat, die wohlmöglich niemals begangen wird, die im Übrigen dann auch an dieser Stelle gar nicht weiter spezifiziert werden müsste im Hinblick auf die einzelnen Modalitäten. Deshalb sehe ich das doch als recht problematisch an. Wie gesagt, vor dem Hintergrund, dass es ja für die strafwürdigen Fälle auch noch den § 111 StGB gibt. Klar, auffordern ist mehr als billigen. Aber jedenfalls einen weiten Bereich des strafwürdigen Verhaltens wird der § 111 StGB schon abdecken.

§ 241 StGB – wie sieht es hier mit dem Bedrohen aus? Was zählt als Bedrohen? Auch da sind die Anforderungen, die die höchstrichterliche Rechtsprechung stellt, nicht so besonders hoch. Klar, reine Angebereien, ein bloßer Spruch genügt an der Stelle sicherlich nicht. Andererseits kommt es aber auch nicht darauf an, ob der Betroffene das wirklich ernst nimmt. Es kommt auch nicht



darauf an, ob der Täter das wirklich ernst meint, ob er also wirklich bereit ist, das in die Realität umzusetzen. Relevant ist einzig und allein, dass der Bedrohte das Ganze ernstnehmen soll. Und wenn man den § 241 StGB so weit fasst, wie das im Augenblick im Entwurf vorgesehen ist, dann werden nicht nur gesteigerte Formen der Körperverletzung erfasst, sondern auch Ankündigungen wie „ich verpasse dir eine Ohrfeige“ oder „ich weiß wo du wohnst“. Wenn aus der Sicht desjenigen, der das sagt, die Intention besteht, dass der Betroffene das tatsächlich ernst nimmt. Und auch, wenn man die Sachbeschädigung einbezieht. Die Aussage: „Ich weiß wo dein Auto steht“ fiel dann auch unter den so erweiterten § 241 StGB. Und dann stellt sich doch die Frage, ob man an der Stelle, weil es hier um ein Vorfeldverhalten geht, nicht die Strafbarkeit zu weit ausdehnt. Auch mit all den Problemen der realen Strafverfolgung, die das mit sich bringt.

§ 188 StGB – das ist in der Tat eine gute Frage, warum spielt diese Vorschrift eigentlich bisher eine so untergeordnete Rolle? Aus meiner Sicht gibt es ein paar Faktoren. Der erste Faktor ist hier schlichtweg nicht zu beeinflussen, und zwar ist das die Rechtsprechung des Bundesverfassungsgerichts – gerade wenn es um Äußerungen im politischen Bereich geht, dass hier die Meinungsfreiheit ein sehr starkes Gewicht bekommt, dass der Meinungsfreiheit einen sehr weitgehenden Vorrang eingeräumt wird. Und alle Bemühungen, hier für einen erhöhten Schutz zu sorgen, müssen einfach diese Einschränkung durch die Rechtsprechung des Bundesverfassungsgerichts zur Kenntnis nehmen und akzeptieren. Der zweite Grund, der für eine praktische Bedeutungslosigkeit spricht, ist, dass es sich bisher bei § 188 um ein reines Antragsdelikt handelt. Darüber hinaus auch noch um ein Privatklagedelikt. Insbesondere an das erste – reines Antragsdelikt – geht der Entwurf aus meiner Sicht richtigerweise heran – dass das umgestaltet werden soll zu einem relativen Antragsdelikt. Der dritte Grund, der für die praktische Bedeutungslosigkeit sicherlich eine Rolle spielt, Herr Hartleb hat es auch richtigerweise schon erwähnt, das ist der § 185 StGB, der bisher nicht einbezogen ist. Und hier kann ich mich in der Tat nur anschließen, habe das ja auch in meinem schriftlichen Gutachten gesagt, dass

man doch erwägen sollte, § 185 noch in die Vorschrift des § 188 aufzunehmen, hier zu integrieren.

Die spannende Frage ist schließlich: Bringt der Bayern-Entwurf tatsächlich noch einen höheren Schutz, weil hier auf die Eignungsklausel verzichtet wird? Wobei – nur beiläufig gesagt – solche Eignungsklauseln haben wir an verschiedenen Stellen ohne dass hierdurch die Strafverfolgungsorgane, insbesondere die Gerichte, vor allzu große Schwierigkeiten bei der Interpretation gestellt werden. Ich sehe, wie gesagt, das Problem des Bayern-Entwurfs an anderer Stelle: dass meines Erachtens nicht der Schutz ausgeweitet wird, sondern ganz im Gegenteil der Schutz, jedenfalls was Teile angeht, verengt wird. Also, wenn etwa Aussagen getroffen werden, der Abgeordnete misshandelt seine Partnerin, seinen Partner – das würde dann wohl nicht mehr darunter fallen. Dass Äußerungen etwa über berufliches Fehlverhalten, wie „er hat in die Kasse gegriffen“ – dass hier dann der Bezug zur politischen Tätigkeit fehlt. Das würde auch nicht mehr von § 188 erfasst. Und die Frage ist, will man das? Will man solche Äußerungen aus dem Anwendungsbereich des § 188 herausnehmen? Drittes Problem: dass bestimmte Personen-gruppen, die bisher von § 188 erfasst werden – Verfassungsrichter beispielsweise oder Gewerkschaftsführer – dass die dann auch nicht mehr darunter fielen, weil sie nicht im engeren Sinne politisch tätig sind. Richtig ist vielleicht, dass man über den Punkt nachdenken kann, ob bei den Personen, die im politischen Leben des Volkes stehen, insbesondere wenn man über die kommunale Ebene redet – ob man das präziser fasst, um an der Stelle gewisse Auslegungsschwierigkeiten in den Griff zu bekommen. Hierfür hat der Bundesrat ja einen Vorschlag vorgelegt. Zwingend notwendig ist das aus meiner Sicht nicht, aber gleichwohl ist das etwas, was man ohne weiteres tun kann und worüber man vielleicht zumindest noch einmal nachdenken sollte.

Der stellvertretende Vorsitzende: Herr Engländer, vielen Dank. Als nächstes hat das Wort Herr Conen mit der Antwort auf die Frage von Herrn Movassat.

SV Stefan Conen: Vielen Dank. Mein Vorredner, Professor Engländer, hat ja zu den Fragen schon



Stellung genommen. Ich will probieren, das nur zu ergänzen und nicht zu doppeln. Was die Frage angeht – Billigung Strafbarkeit, Belohnung Strafbarkeit, strafbare Delikte nach § 140 StGB. Da muss man sagen, das ist in der Literatur weitgehend, auch zu Recht, kritisiert worden – dass das in der Nähe des Gesinnungsstrafrechts ist. Es gibt eine Entscheidung des Bundesgerichtshofs aus dem Jahre 1978, wo ein Verleger nach dieser Norm bestraft worden ist, weil er ein Buch eines Straftäters verlegt hat, der über seine Straftaten schrieb. Das reicht für Billigung aus. Wenn man das jetzt für die zukünftigen Straftaten ausdehnt, dann ist das eigentlich keine neue Idee, die man hier in dem Gesetzentwurf formuliert hat, sondern das gab es schon mal, und zwar in einem alten § 88 des Strafgesetzbuches, der von 1976 bis 1981 galt. Und warum hat man den abgeschafft? Der Bundestag hat damals in der Begründung der Abschaffung formuliert, dass dieser Paragraph für das Ansehen des Strafrechts und des Staates mehr Schaden als Nutzen angerichtet hat. Es gab nur eine einzige Verurteilung in den fünf Jahren. Und die negativen Wirkungen der Vorschrift, insbesondere auf das geistige Klima und die Gefahren für die Meinungsfreiheit, stünden in keinem Verhältnis zum kriminalpolitischen Nutzen. Das war die Begründung der Abschaffung. Es gab einen Versuch, diesen Paragraphen oder die darunter liegende Idee noch einmal zu reaktivieren, in der 11. Legislaturperiode – ich glaube, es war § 130b –, was damals aus diesen Erwägungen auch nicht durchgegangen ist, so dass man sich fragen kann, was man sich davon verspricht, wenn man das auf das Internet mit den begrenzten Ressourcen der Strafverfolgung überträgt. Zumal richtig ist, wie Herr Engländer schon gesagt hat, dass die entscheidenden Strafbarkeitslücken gar nicht da sind, weil sie zum Beispiel vom § 111 StGB aufgefangen werden.

Zu § 241 StGB, der Ausweitung der Bedrohung: Mein Vorredner hat es schon einmal formuliert. Ich stelle mir das so vor, es muss ja nicht immer „wo dein Auto steht“ sein, es reicht dann zukünftig, vom sachbedeutenden Wert her, „ich weiß, was deine Stoßstange gekostet hat“. Im Jugendstrafrecht, wo Bedrohungen noch ein bisschen ubiquitärer sind in der Pubertät als es bei einem Erwachsenen der Fall sein sollte – wenn man überlegt, was das heißen kann, wenn auf

jedem Schulhof „ich glaube, du willst ein paar aufs Maul“ oder Ähnliches eine Straftat darstellt, dass da der Lehrer, der die Pausenaufsicht hat, in erster Linie potenziell zum Strafverfolger wird, wenn er das alles notieren muss – da weiß ich auch nicht, ob das angemessen ist. Wir haben das Glück in dieser Republik, dass die Jugendkriminalität stark im Sinken ist. Wenn diese Verbaldelikte, die häufig ja nur pubertäres Imponiergehabe sind, in dem Bereich alle strafbar werden, werden wir einen Anstieg haben, der die Gesellschaft meines Erachtens grundlos besorgen wird. Das wären meine Antworten dazu, danke.

Der stellvertretende Vorsitzende: Vielen Dank. Als nächstes Frau Ballon mit den Antworten auf die Fragen von Herrn Fechner und Herrn Post.

SVe Josephine Ballon: Ich möchte auch nichts wiederholen, was Herr Hartmann schon gesagt hat zum Thema „Heimatlandprinzip vs. Marktortprinzip“. Darauf läuft es ja hier hinaus bei dieser Diskussion. Ich möchte vielleicht einfach daran anknüpfen und kurz etwas zu den Plattformen selbst sagen. Die sozialen Netzwerke, die beauskunfteten leider höchst uneinheitlich, was unvermeidbar den Eindruck der Willkür erweckt. Man kann nicht umhinkommen, als irgendwie den Eindruck zu haben, dass kein richtiges System dahintersteht, dass sich das gesamte Auskunftsverhalten vor allem nach internen Richtlinien richtet und eben nicht nach unseren nationalen Gesetzen. Es mag sein, dass die Beauskunftung von zum Beispiel Morddrohungen oder Volksverhetzungen sich mittlerweile etwas gebessert hat, aber für andere Delikte, den weitaus überwiegenden Teil anderer Delikte, gilt das nicht. Es ist leider so, dass offensichtlich wenig Bereitschaft besteht, dieser Verantwortung, die die sozialen Netzwerke nun mal haben – schon aufgrund der Bedeutung, die sie in unserer Gesellschaft haben – nachzukommen, obwohl das ja zum Beispiel über Nutzungsrichtlinien oder Ähnliches sehr leicht zu lösen wäre. Man beruft sich bei der Begründung, dass keine Beauskunftung erfolgt, vor allem auf interne Risiken rechtlicher Natur im Verhältnis zu den Nutzern, wie auch immer die geartet sein sollen. In erster Linie natürlich auch mit dem Argument, dass die Daten, die beauskunftet werden sollen, im Ausland liegen und deswegen eine Beauskunftung wahrscheinlich sogar gegen Gesetze verstoßen



würde. Es ist sogar so, dass mir bekannt ist, dass derzeit auch schon geprüft wird, ob, wenn eine nationale Auskunftspflicht, zum Beispiel über den jetzt geplanten Gesetzentwurf, käme – ob dann überhaupt eine Verpflichtung bestünde, dem nachzukommen, weil es ja immer noch Daten sind, die im Ausland gespeichert werden. An diesem Fakt hat sich dadurch nichts geändert.

Die zweite Dimension, die man sehen muss, sind die Betroffenen selbst. Wie Herr Hartmann schon gesagt hat, wird die überwiegende Zahl der Ermittlungsverfahren wahrscheinlich eingestellt. Einfach aus dem Grund, dass die Identität der Täterinnen oder Täter nicht ermittelt werden konnte, weil keine Auskunft erfolgt ist. Das ist natürlich aus Sicht der Betroffenen ziemlich frustrierend und führt dann wieder zu diesem altbekannten Rückschluss – die Frage nämlich, warum sagen die Strafverfolgungsbehörden, dass wenig Anzeigen eingehen, und warum sagen die Betroffenen, dass sie keine Anzeigen erstatten wollen. Nämlich in erster Linie, weil, wenn sie es tun, nur Einstellungsbescheide dabei rauskommen. Und wenn sie besonderes Pech haben, werden die sogar noch den Täterinnen oder Tätern zugestellt, sofern sie denn ermittelt werden konnten. Natürlich muss man auch berücksichtigen, dass es eine europarechtliche Ebene gibt. Es wird ja zurzeit am Digital Services Act gearbeitet, und es sieht danach aus, als würde das Heimatlandprinzip dort eher noch bestärkt werden. Was natürlich sehr schade ist. Deswegen kann man hier nicht einfach nur die nationale Ebene sehen, sondern muss das Ganze in einem größeren Kontext betrachten und vor allem die Entwicklungen, die dort stattfinden, auch berücksichtigen.

Zum zweiten Punkt würde ich hier gerne sagen, dass die Einführung dieser Meldepflicht grundsätzlich zu begrüßen ist, weil sie geeignet ist, um die Strafverfolgung zu intensivieren. Wenn mehr Strafanzeigen erstattet werden, dann wird wahrscheinlich auch mehr strafverfolgt werden. Das ist grundsätzlich zu begrüßen. Allerdings darf das nicht um jeden Preis geschehen, denn die schon vorhin angesprochenen Weiterverarbeitungsvorschriften, die sich im BKA-Gesetz finden, die sind vorhanden, und die Ausnahmen, die dort vorgesehen sind, die eine Weiterverarbeitung dieser Daten zulassen, die sind gar nicht so unerheblich. Zum Beispiel ist eine Weiterver-

arbeitung dann gestattet, wenn es um die Wahrnehmung gleichgearteter Interessen geht, wenn nämlich zum Beispiel gleichartige Rechtsgüter betroffen sind oder gleiche Straftaten. Deswegen sollte man hier dringend daran denken, dieses zweistufige Prinzip – wie auch immer es ausgestaltet sein könnte – in irgendeiner Form zu berücksichtigen. Ich sehe vor allem das Problem darin, dass das BKA zumindest nach seiner in § 2 BKA-Gesetz ausgestalteten Zentralstellenfunktion keine strafrechtliche Prüfung vornehmen kann. Das sind schlicht Befugnisse, die sich zumindest daraus nicht ergeben. Und ich weiß auch nicht, woher sie sich sonst ergeben sollen.

Der zweite Punkt ist, dass ich befürchte, dass die große Problematik des Ganzen weniger in den Fällen liegen wird, in denen offensichtlich gar keine Strafbarkeit vorhanden ist, sondern in den Fällen, wo es gerade schwieriger wird. Wenn wir nämlich zum Beispiel daran denken, dass es auch Fälle gibt, in denen zum Beispiel Satire eine Rolle spielt, in denen Karikaturen eine Rolle spielen, dann ist einfach zu sagen, dass den Netzwerken diese höchst komplexe Einordnung überhaupt gar nicht zuzumuten ist. Das wird dazu führen, dass Daten abgefragt werden, die dann in Datenbanken landen. Und wie alle wissen, ist die Netzgemeinschaft sehr datensensibel. Und es wird dazu führen, dass die Menschen Bedenken haben, möglicherweise in den Datenbanken des BKA zu landen, was für einige Menschen, auch wenn sie sich möglicherweise nichts vorzuwerfen haben, schlicht nicht erwünscht ist. Das heißt, wir haben dann wieder einen Effekt in die andere Richtung, dass die Meinungsfreiheit für die Menschen eingeschränkt wird, deren Schutz dieser Gesetzentwurf gerade dient. Das wird im Endeffekt auch dazu führen, dass die Akzeptanz dieses Gesetzes nicht besonders hoch sein wird und es aktuell aus diesem Grund auch nicht ist. Sicherlich ist die Intention, die dahintersteht, nämlich die Prozessökonomie zu verbessern und auch die Geschwindigkeit der Datenabfrage zu gewährleisten, durchaus ersichtlich und auch sinnvoll, allerdings muss man sehen, dass irgendwie ein Ausgleich geschaffen wird, wie ihn Herr Hartmann ja auch schon angesprochen hat.

Einen Punkt würde ich gerne noch erwähnen, und zwar noch einmal zum Thema, was passiert mit der Einschätzung durch die sozialen Netzwerke,



wenn sie falsch ist? Wenn eine falsche Einschätzung vorliegt und dennoch ein Ermittlungsverfahren eingeleitet wird, muss man berücksichtigen, dass die dahinterstehenden Personen, die möglicherweise dem Kreis der Menschen zuzurechnen sind, die gerade hierdurch geschützt werden sollen, in einer unverhältnismäßigen Weise eingeschränkt werden. Deswegen plädieren wir dafür, ein zweistufiges Verfahren einzurichten. Danke.

Der **stellvertretende Vorsitzende:** Frau Ballon, vielen Dank. Und als letztes Herr Bäcker, der uns zugeschaltet ist, mit der Antwort auf die Frage von Frau Künast.

SV Prof. Dr. Matthias Bäcker: Vielen Dank. Mir sind zwei Fragen gestellt worden. Die eine betraf noch einmal dieses Zwei-Stufen-System, über das ja jetzt schon viel gesagt worden ist. Worum es geht, denke ich, ist, dass man hier unterscheiden muss zwischen der Abklärung, ob ein Tatverdacht überhaupt besteht, und allen weiteren Schritten. Das BKA soll hier nach meinem Verständnis im NetzDG mit so einer Art Vorermittlungsverfahren, wie man das in der strafprozessreinen Terminologie nennen würde, betraut werden. Es soll also klären, ob überhaupt ein Tatverdacht besteht, und wenn ja, welche Strafverfolgungsbehörde zuständig ist, an die wir die Sache abgeben können. Diese beiden Stufen sollten auseinandergehalten werden. Es sollte zunächst mal der Tatverdacht geklärt werden. Das kann man, ohne notwendiger Weise den sich Äußernden zu identifizieren, weil es um die Äußerung geht, nicht um die dahinterstehende Person. Nur wenn ein Tatverdacht bejaht wird, nur dann sollten tatsächlich auch Personen Daten verarbeitet werden, um zu einer Zuständigkeitsklärung zu kommen. Das ist, denke ich, das Anliegen hierbei. Da sind jetzt unterschiedliche Vorgehensweisen denkbar, die alle ihre Vor- und Nachteile haben. Man könnte also sagen, die Identifikationsdaten werden zunächst vom Telemedienanbieter bevorratet. Es ist praktisch ein Quick Freeze beim Telemedienanbieter. Und wenn das BKA einen Tatverdacht bejaht, dann werden die Zugangsdaten möglichst schnell an das BKA geschafft, vielleicht auch über eine elektronische Schnittstelle, damit eine Personenidentifikation erfolgen kann. Das birgt natürlich das Problem einer gewissen zeitlichen Verzögerung, die in einem solchen zeitkritischen

Ermittlungsfeld durchaus hohe Schwierigkeiten für die wirksame Strafverfolgung bewirken kann. Man muss allerdings auch sehen, das hat nicht nur Nachteile. Denn in der Zeit zwischen der Meldung des Inhalts und der Entscheidung des BKA, ob hier ein Tatverdacht vorliegt, ja oder nein, ist es ja möglich, dass sich die betreffende Person wieder bei dem Netzwerk anmeldet, dann wieder mit einer neuen IP-Adresse, zu deren Mitschniden man den Netzbetreiber auch verpflichten könnte, so dass man möglicherweise in bestimmten Fällen hier sogar aktuellere Daten rauskriegt, als bei dem Verfahren, das das Gesetz im Moment vorsieht. Eine andere Möglichkeit, die ich auch für vertretbar halten würde, würde so aussehen, dass die zur Identifikation erforderlichen Daten gleich an das BKA gehen, vom BKA aber lediglich an den Telekommunikationsanbieter weitergeleitet werden, der dann eine Identifizierung vornimmt, aber die Identifikationsdaten noch nicht an das BKA zurückmeldet, sondern bei sich behält. Also wäre das eine Art Quick Freeze, aber dieses Mal nicht beim Telemedienanbieter, sondern beim Telekommunikationsanbieter. Wichtig scheint mir aber in jedem Fall, dass eine Identifizierung, eine Zusammenführung von Inhalt und Person beim BKA nicht erfolgen sollte, solange die Frage des Anfangsverdachts nicht geklärt ist. Das führt auch schon zur zweiten Frage, nämlich der nach der Weiterverarbeitung der Daten. Hier muss man nämlich zunächst mal sehen, diese Betrauung des BKA mit Vorermittlungen ist eigentlich etwas, was für die Zentralstellenaufgabe ziemlich untypisch ist. Das ist auch verschiedentlich, bei verschiedenen Stellungnahmen hier angeklungen. Normalerweise beinhaltet die Zentralstellenaufgabe nicht, dass das BKA bei konkreten einzelnen Strafverfolgungsverfahren vorklärend tätig wird, sondern normalerweise ist die Zentralstellenfunktion mehr so eine Art Servicefunktion, wo das BKA Informationen sammelt, bündelt, aufbereitet, in anderer Weise Strafverfolgungsbehörden unterstützt. Ich halte es aber trotzdem für vertretbar, das der Zentralstellenaufgabe insgesamt noch zuzuschlagen. Wenn man das aber tut, ist natürlich die nächste Frage – kann denn das BKA die Daten, also die Inhalte, möglicherweise auch die Identifikationsdaten, die es einmal erhalten hat – kann es die jetzt auch im Rahmen seiner normalen Zentral-



stellenaufgaben, also als Informationsknoten und Serviceeinrichtung, benutzen? Und da scheint mir ganz klar zu sein, dass das geht. Das BKA-Gesetz ermöglicht das. Das hat Herr Peter ja auch gesagt. Er hat auch § 18 des BKA-Gesetzes genannt. Ich sehe also überhaupt keinen Grund, warum das nicht möglich sein soll. Deswegen fand ich es ein bisschen erstaunlich, dass es in der Begründung des Entwurfs heißt, das BKA wird die Daten löschen, sobald es die Zuständigkeit geklärt und den Vorgang weitergegeben hat. Ich halte es für viel naheliegender, dass in vielen Fällen das nicht geschehen wird. Gerade im Bereich Rechtsextremismus, Hate Speech – in diesem ganzen Thema, gerade hier werden enorme Forschungsanstrengungen, gerade auch unter Beteiligung von Polizeibehörden und auch vom BKA, unternommen, um große Massen von Daten auszuwerten, um Lagebilder zu zeichnen, Radikalisierungsverläufe nachzuzeichnen oder sogar zu prognostizieren, gefährliche Strukturen, örtliche Cluster oder so etwas zu entwickeln, und auf diese Weise möglichst dem Phänomen vorauszukommen, insbesondere dem Umschlag von verbaler Übergriffigkeit in physische Gewalt vorauszukommen, zu dem es in der Vergangenheit immer wieder gekommen ist. Ich fände es total fernliegend, die Daten, die im Rahmen des NetzDG übermittelt werden, nicht für so etwas zu nutzen. Das fände ich auch rechtspolitisch und polizeitaktisch fahrlässig, wenn das nicht möglich wäre. Und es ist auch möglich. Und ich würde davon ausgehen, dass es auch geschehen wird. Ich habe damit auch kein grundlegendes Problem, man muss aber sehen – und das ist ein Webfehler des BKA-Gesetzes, der mit den Regelungen, die Gegenstand der Anhörung sind, gar nicht unmittelbar zusammenhängt –, dass diese Weiterverarbeitungsregelungen im BKA-Gesetz teilweise viel zu weit gefasst sind. Und das will ich nur an einem Beispiel festmachen, um das zu illustrieren. Wir haben jetzt schon viel darüber gehört, dass es Fälle geben wird, in denen die Netzwerke einen Inhalt melden und sich dann aber herausstellt, dass der Inhalt tatsächlich nicht strafbar ist. Das BKA verneint also einen Anfangsverdacht. Was kann das BKA jetzt machen? Herr Peter hat gesagt, wenn es strafrechtlich völlig irrelevant ist, löschen wir den Inhalt. Davon gehe ich aus. In vielen Fällen ist das aber nicht völlig irrelevant in dem Sinne, dass das

ein glasklarer Fall ist, sondern die Delikte, die hier zu melden sind, von denen ist ein großer Teil hochgradig pathologisch, erfordert sehr schwierige Subsumptionen, Abwägungen. So etwas wie Volksverhetzung, das ist ein Albtraum, von der Handhabung her. Ich habe selber als wissenschaftlicher Mitarbeiter im Bundesverfassungsgericht immer wieder Volksverhetzungsfälle zu bearbeiten gehabt. Da habe ich jedes Mal gekreisch, wenn wieder so eine Akte auf meinen Tisch kam, weil die so unangenehm sind, und weil sich da immer wieder so schwierige Probleme stellen. Der § 86a – Verwenden von Kennzeichen verfassungswidriger Organisationen –, der hier als unproblematisch bezeichnet wurde – da würde ich nur mal illustrativ darauf hinweisen, dass der Bundesgerichtshof als Revisionsinstanz erstmals entscheiden musste, dass es nicht strafbar ist, ein T-Shirt zu produzieren, auf dem ein durchgestrichenes Hakenkreuz, das in einen Mülleimer geworfen wird, mit der Bildunterschrift „Nazis raus“ abgebildet ist. Die Vorinstanzen hielten das für einen strafbaren Verstoß gegen diese Vorschrift. Das ist keineswegs trivial. Was bedeutet das für das BKA? § 18 BKA-Gesetz ermöglicht dem BKA, Daten personenbezogen auch dann weiterzuverarbeiten, wenn es um Daten sogenannter Anlasspersonen geht. Das sind Personen, gegen die kein Tatverdacht besteht, bei denen aber das BKA aufgrund tatsächlicher Anhaltspunkte annimmt, dass sie in naher Zukunft Straftaten begehen werden. Ich halte es für durchaus vorstellbar, dass man aufgrund von Inhalten, die für sich genommen noch zulässig sind, trotzdem auf einen bevorstehenden Radikalisierungsverlauf, bevorstehende Äußerungsdelikte oder Schlimmeres schließt, und dass dann durchaus Datenspeicherungen auch in Fällen erfolgen werden, wo ein Tatverdacht nicht besteht. Das würde ja nicht jeder in jedem Einzelfall verteuflern, aber das Gesetz ist hier schlicht zu weit gefasst. Wie gesagt – das Kind ist sozusagen im Brunnen. Wenn Sie jetzt nicht im Rahmen dieses Gesetzgebungsverfahrens das BKA-Gesetz noch einmal aufbohren wollen, dann sollten Sie dafür sensibilisiert sein, dass das solche Auswirkungen haben kann und wahrscheinlich auch haben wird. Wirklich etwas daran ändern können Sie nicht, wenn Sie nicht Abstand nehmen von einem Vorhaben, das für sich



genommen auch viel für sich hat, nämlich diese Meldepflicht. Herzlichen Dank.

Der stellvertretende Vorsitzende: Vielen Dank, Herr Bäcker. Jetzt schaue ich auf die Uhr. Wir haben noch sieben Minuten, haben fünf weitere Fragen. Mein Vorschlag ist, dass ich die fünf Frager bitte, ganz kurz eine Frage zu stellen, denn das könnten wir mit etwas Beschleunigung hier durchbekommen. Das hängt damit zusammen – was wir auch vorhergesehen haben –, dass wir eine viel größere Zahl als Sachverständige als sonst haben. Deshalb haben wir ja schon gesagt, bitte die Redezeit etwas begrenzen. Das ist aber nur sehr beschränkt geschehen und die Zeit ist an anderer Stelle schon ausgeschöpft worden. Als erstes dann Carsten Müller mit einer kurzen Frage. Bitte.

Abg. Carsten Müller (Braunschweig) (CDU/CSU): Vielen Dank, Herr Vorsitzender. Eine kurze Frage an Herrn May: Welche Vorkehrungen treffen Sie denn jetzt im Hinblick auf personelle und sachliche Ressourcen? Es ist ja nicht vollkommen unwahrscheinlich, dass dieses Gesetz Mehrheiten im Bundestag finden wird, mit hilfreichen Anmerkungen, die wir heute aufgenommen haben. Und wie kann es gelingen, diese große Aufgabe relativ schnell zu erfolgreichen Verfahren zu führen?

Der stellvertretende Vorsitzende: Vielen Dank für die knappe Frage. Herr Zimmermann.

Abg. Dr. Jens Zimmermann (SPD): Vielen Dank. Ich möchte Herrn Hartmann noch einmal nach seiner hohen Sympathie für das Quick-Freeze-Verfahren befragen. Mich würde interessieren, was sehen Sie da für notwendige Änderungen am Gesetzesvorschlag, insbesondere auch im Hinblick auf die Frage „IP-Adresse“? Da könnte man ja die Anbieter auch verpflichten, dann, sofern vorhanden, die aktuelle IP-Adresse, wenn das Ermittlungsverfahren beginnt, noch einmal nachzureichen.

Der stellvertretende Vorsitzende: Vielen Dank. Frau Künast.

Abg. Renate Künast (BÜNDNIS 90/DIE GRÜNEN): Danke. Eine Frage an Herrn Peter, gerade jetzt nach Herrn Bäcker. Ich würde gerne noch einmal genauer verstehen, wie Sie mit diesen Anlasspersonen umgehen. Um welche Fälle geht

es? Weil ich finde, dass man da eine Abgrenzung braucht – was ist meinerseits rechtsextremes Netzwerk und was ist weit im Vorfeld, wo jemand vielleicht nur einmal – Ich würde es gerne genauer und präziser verstehen. Was sind die Personendaten, die Sie trotz fehlender Strafbarkeit für Ihre Netzwerkanalysen benutzen? Wer würde darunter fallen? Wen würden Sie löschen?

Der stellvertretende Vorsitzende: Vielen Dank. Herr Maier.

Abg. Jens Maier (AfD): Ich habe eine Frage an Frau Dr. Bastians. Der wissenschaftliche Dienst des Deutschen Bundestages hatte 2016 in seiner Veröffentlichung „Aktueller Begriff – Hass und Hetze im Strafrecht“ darauf hingewiesen: „Während das Strafrecht als schärfste Sanktionsmöglichkeit des Staates mithin dazu dienen kann, als ultima ratio bestimmte Erscheinungsformen von Hetze als Symptom von Hass zu bekämpfen, erscheint es als grundlegendes Mittel gegen Hass und seine Ursachen kaum geeignet.“ Und daher auch die Frage an Frau Dr. Bastians: Meinen Sie, dass innerhalb Ihres Verantwortungsbereiches – also Kommunalpolitiker beispielsweise dadurch jetzt eine Entspannung erfahren, eine Besserstellung durch diese Regelung, dass es wirklich ein Ende hat oder zumindest reduziert wird, welche Erwartungen haben Sie da?

Der stellvertretende Vorsitzende: Vielen Dank. Als Letzter Herr Schipanski.

Abg. Tankred Schipanski (CDU/CSU): Vielen Dank, Herr Vorsitzender. Eine Frage mit zwei Handlungssträngen an den Sachverständigen May. Zum einen wurde jetzt mehrmals gesagt, dass die Daten, die die sozialen Netzwerke herausgeben, nicht praktikabel und effektiv für die Strafverfolgung sind. Vielleicht können Sie noch einmal ganz konkret sagen, für die Qualität der Strafverfolgung, welche Datensätze werden da benötigt? Das ist der erste Strang. Und der zweite Strang ist das Zwei-Stufen-Verfahren, das der Sachverständige Bäcker vorgestellt hat. Das ist ja das, was der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) in seiner Stellungnahme (Anlage) vorgeschlagen hat. Der Sachverständige Bäcker hat auf die zeitlichen Verzögerungen hingewiesen. Was würde das für die Praxis bedeuten? Ist das dennoch praxistauglich, was hier auf dem Tisch liegt?



Der **stellvertretende Vorsitzende**: Vielen Dank. Als erstes in der Antwortrunde – wir gehen jetzt alphabetisch vor – hat Frau Bastians das Wort. Und jetzt möglichst schnell.

SVe **Dr. Uda Bastians**: Ich werde mich kurzfassen. Vielen Dank, Herr Maier. Wir sehen mit dem Gesetzentwurf deutliche Verbesserungen, und zwar nicht nur für den kommunalpolitischen Bereich, sondern auch für die Kommunalbeschäftigten. Wenn die Mitarbeiterin im Jobcenter oder im Meldeamt sich sagen lassen muss, „ich breche dir die Beine“, und vor ihr steht ein Kampfsportler, dann ist eine Reaktion des Staates da wirklich unausweichlich. Und die ist künftig möglich. Im Moment ist es quasi straflos. Das kann so nicht bleiben. Da müssen wir auch den öffentlichen Dienst schützen, und da müssen wir auch die Ehrenamtlichen und amtlich tätigen Kommunalpolitiker schützen. Und deswegen begrüßen wir die Ausweitung des § 241 StGB ausdrücklich und halten das für einen wichtigen Verbesserungsschritt.

Der **stellvertretende Vorsitzende**: Vielen Dank. Herr Hartmann mit der Antwort auf die Frage von Herrn Zimmermann.

SV **Markus Hartmann**: Wenn ich die Sympathie präzisieren kann, hinsichtlich der beiden Alternativen, die Herr Professor Bäcker aufgezeigt hat, dann glaube ich, ist die erste Alternative die dogmatisch klarste, aber in der Praxis nicht umsetzbar, weil sie zu hohe zeitliche Verzögerungen mit sich bringen wird. Die zweite Alternative, also nicht Quick Freeze bei den sozialen Medien, sondern Quick Freeze bei den Telekommunikations Providern, halte ich unter der Voraussetzung, dass das Gesamtverfahren komplett digitalisiert wird, für durchaus umsetzbar. Insoweit werden wir auch meines Erachtens keinen Mehrwert durch eine weitere IP-Adresse haben, weil zum Zeitpunkt der Anlieferung der Daten ein sofortiges Quick Freeze ja identifizierungsfähige Datensätze festhalten würde. Ist also mit der IP-Adresse der Tatverdächtige oder die Tatverdächtige identifiziert, dann wird wohl der Zeitpunkt nach hinten verlagert, in dem das BKA – nämlich nach Bejahung eines Anfangsverdachts – auf diese Daten dann Zugriff nimmt. Insofern, glaube ich, ist das ein tragbarer Preis für die Ermittlungen, der den grundrechtlichen

Interessen insofern ein etwas höheres Schutzniveau zubilligen kann.

Der **stellvertretende Vorsitzende**: Vielen Dank, Herr Hartmann. Und Herr May als nächstes mit den Antworten auf die Fragen von Herrn Müller und die Zwei-Stränge-Frage von Herrn Schipanski.

SV **Andreas May**: Ganz kurz zur Frage des Herrn Müller. Vielen Dank, Herr Müller. Man muss, um das Verfahren zu verstehen, wissen, dass das BKA in allen Fällen, in denen die Täter oder die Beschuldigten nicht identifizierbar sind, diese Verfahren an Staatsanwaltschaften geben wird mit der Bitte um weitere Identifizierungen im Rahmen der StPO. Wir haben für diesen Bereich und dieses Haushaltsjahr zehn Stellen zur Verfügung, die sich nur mit der Identifizierung der unbekannt gebliebenen Verantwortlichen beschäftigen werden. Das ist die Stellensituation momentan bei uns. Wie gesagt, zehn Stellen, die geschaffen werden nur für die Bekämpfung. Zur Datenqualität ist es eigentlich sehr einfach. Eine IP-Adresse alleine, wie das Gesetz es vorsieht, nützt heute nichts mehr zur Zuordnung. Die sozialen Netzwerke werden in aller Regel mit mobilen Endgeräten bedient. Man nutzt mobile Endgeräte. Das heißt, man braucht eine IP-Adresse und einen Port, man braucht eine Verpflichtung des sozialen Netzwerkes zur Ausleitung der Port-Adresse, sonst nützt es schon nichts. Und auf der anderen Seite, quasi als Gegenstück, natürlich auch eine Verpflichtung der Speicherung von Access-Providern, das heißt den Zugangs Providern, zur Speicherung des Port-Schlüssels. Ansonsten ist eine Zuordnung ohnehin nicht möglich. Ganz kurz noch die Frage zu Quick Freeze und Zeitverzögerungen. Auch da muss ich ehrlich sagen, der Verlust der Daten droht sehr schnell. Es gibt viele Provider, die überhaupt keine Daten speichern. Es gibt eine Menge Provider, die beaskunften nicht, während ich den Dienst nutze. Selbst dann ist eine Beaskunftung derzeit bei diesen Providern nicht möglich. Das heißt, jeder Zeitverzug – und dieser Zeitverzug wird bei Quick Freeze entstehen – wird zu einem weiteren massiven Datenverlust führen. Das vielleicht in aller Kürze. Und dann wird es für die Ermittlungsbehörden unheimlich schwierig, weil mit der StPO weiterzukommen, mit dem Rechtshilfeweg weiterzukommen,



Bestandsdaten-, Nutzerdaten-anfrage im Rechtshilfewege zu tätigen, das ist aus meiner Sicht nahezu aussichtslos.

Der **stellvertretende Vorsitzende**: Vielen Dank, Herr May. Und als letzter Herr Peter mit der Antwort auf die Frage von Frau Künast.

SV **Jürgen Peter**: Kurz zu der Frage von Frau Künast. Der § 18 BKA-Gesetz liefert eine sehr hohe Hürde für die Weiterverarbeitung von Daten sogenannter Anlasspersonen. Ich will das kurz zu Protokoll geben. Wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die betroffenen Personen in naher Zukunft Straftaten von erheblicher Bedeutung begehen werden. Das ist die Definition, die bedarf einer sehr gründlichen Negativprognose, die auch dokumentiert wird. Bezogen auf die NetzDG-Volumen vielleicht mal ein Beispiel. Ein Post oder ein Inhalt, der ausgeleitet wird, der haarscharf – weil die Täter oft clever sind – an der Strafbarkeitsschwelle vorbeirauscht, würde im BKA im Rahmen der Erstbearbeitung zuzuordnen sein einem politisch rechtsmotivierten Straftäter, der bereits als Gewalttäter, wegen fremdenfeindlicher Straftaten oder Sonstigem bekannt ist und mehrere Fundstellen im polizeilichen System hat, in denen bewiesen ist, dass Straftaten von erheblicher Bedeutung begangen wurden und die Prognose es auch zulässt, dass er sie weiter begehen wird. Das wäre ein Fall der Weiterspeicherung.

Weil ich viele Kommentare jetzt gehört habe zur Rolle des BKA und doch wohl einige Missverständnisse im Raum sind, möchte ich festhalten, das BKA ist eine Polizeibehörde des Bundes. Und wir diskutieren über Kriminalpolizei und Polizei. Ich möchte, sehr geehrter Herr Vorsitzender, anbieten, dass die Prozessschritte, die wir bereits in Vorbereitung haben, zur Umsetzung dessen,

was wir zum NetzDG hier diskutieren – dass wir das gerne mit einer Einladung flankieren und dem Ausschuss anbieten, dass Mitglieder des Ausschusses sich zu den Vorbereitungshandlungen, die wir bisher schon getroffen haben und den Prozessschritten im BKA ein Bild machen.

Der **stellvertretende Vorsitzende**: Vielen Dank, Herr Peter. Diese Anregung greifen wir gerne auf und werden sie diskutieren. Denn ich sage mal so, der technische Sachverstand bei manchen dieser Sachen ist ein Teil des Problems, das ich aus der Diskussion mit Juristen kenne, wenn es dann heißt, die Richter sollen das alles entscheiden und die Richter die Datenzugänge nicht haben. Wir sehen das ja jetzt auch hier, die Erfahrungen mit Webex usw. An welchen Stellen es dann scheitert und hapert und das sind dann nicht die Rechtsfragen, die wir aber eigentlich als erstes zu beantworten haben.

Herzlichen Dank auch, dass Sie sich in der letzten Runde so kurz gefasst haben. Damit haben wir fast eine Punktlandung hinbekommen. Herzlichen Dank vor allen Dingen an Sie, die Damen und Herren Sachverständigen, an die Kolleginnen und Kollegen, auch schließlich an die Gäste auf der Besuchertribüne, die ja heute nicht nur Besucher, sondern auch Mitarbeiter und Abgeordnete sind. Wir werden das, was Sie hier vorgetragen haben, in unsere Erwägungen aufnehmen, weiterüberlegen und dann zu einem Ergebnis kommen. Das Bundesministerium der Justiz und für Verbraucherschutz hat freudig mitgeschrieben, auch wenn Staatssekretär Lange jetzt nicht mehr da war. Aber die Fachabteilung macht ja erst einmal die Arbeit, auch dafür herzlichen Dank.

Herzlichen Dank nochmals, dass Sie da waren. Ich schließe die Sitzung. Die nächste Sitzung hier in einer Stunde, die nächste Anhörung. Bis dahin – alles Gute!

Schluss der Sitzung: 13:04 Uhr

Dr. Heribert Hirte, MdB
Stellvertretender Vorsitzender



Anlagen:

Stellungnahmen der Sachverständigen

Prof. Dr. Matthias Bäcker, LL.M.	Seite 36
Josephine Ballon	Seite 55
Dr. Uda Bastians	Seite 77
Stefan Conen	Seite 80
Prof. Dr. Armin Engländer	Seite 93
Klaus-Dieter Hartleb	Seite 102
Markus Hartmann	Seite 111
Henning Lesch	Seite 125
Uwe Lübking	Seite 132
Andreas May	Seite 152
Jürgen Peter	Seite 160
Dr. Klaus Ritgen	Seite 166
Ausschussdrucksache 19(6)134	Seite 170
Ausschussdrucksache 19(6)121	Seite 186

JOHANNES GUTENBERG-UNIVERSITÄT MAINZ - 55099 Mainz

FACHBEREICH 03

JURA

Lehrstuhl für Öffentliches Recht
und Informationsrecht, insbe-
sondere Datenschutzrecht

Universitätsprofessor
Dr. Matthias Bäcker

Johannes Gutenberg-
Universität Mainz
Jakob-Welder-Weg 9
55128 Mainz

Tel. +49 6131 39 28173
Fax +49 6131 39 28172

matthias.baecker@uni-mainz.de
www.baecker.jura.uni-mainz.de/

Stellungnahme

zu dem Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus
und der Hasskriminalität
(BT-Drs. 19/17741)

Gliederung

Ergebnisse	3
I. Meldung strafbarer Inhalte an das Bundeskriminalamt	4
1. Keine grundlegenden verfassungsrechtlichen Bedenken	4
2. Verfassungs- und unionsrechtliches Gebot einer zweistufigen Ausgestaltung	5
3. Weiterverarbeitung der übermittelten Daten	6
II. Übermittlung von und Zugriff auf Telemediendaten	7
1. Vorfragen	7
a) Doppeltürmodell und grundrechtliche Regelungsverantwortung	7
b) Differenzierung und Abgrenzung von Telemedien und Telekommunikation	8
c) Kategorien von Telekommunikations- und Telemediendaten	10
2. Übermittlung von und Zugriff auf Bestandsdaten	13
3. Übermittlung von und Zugriff auf Nutzungsdaten	14
4. Inhaltsüberwachung von Telemedien	15
5. Übermittlung von und Zugriff auf Zugangsdaten	17
6. Zitiergebot	18

Ergebnisse

1. Die in § 3a NetzDG-E vorgesehene Pflicht zur sofortigen Übermittlung von Identifikationsdaten an das Bundeskriminalamt verletzt höherrangiges Recht. Eine solche Pflicht ist nur in einem zweistufigen Verfahren als zweiter Schritt verhältnismäßig, nachdem das Bundeskriminalamt in einem ersten Schritt die übermittelten Inhalte geprüft und einen strafprozessualen Anfangsverdacht bejaht hat.
2. Die vorgesehene Ermächtigung des Bundeskriminalamts zum Zugriff auf Telemedien-Bestandsdaten in § 10 Abs. 1 Satz 1 Nr. 1, Satz 2 BKAG-E geht weiter als die zugehörige Übermittlungserlaubnis in § 15a Abs. 2 Satz 1 TMG-E, da sie einen Zugriff auch im Vorfeld von präventivpolizeilicher Gefahr und strafprozessuellem Anfangsverdacht zulässt. Sie verletzt zudem das Recht auf informationelle Selbstbestimmung, da sie den Eingriffsanlass weder in tatsächlicher noch in materieller Hinsicht näher konturiert und qualifiziert.
3. § 15a Abs. 4 Satz 1 und § 15b Abs. 3 Satz 1 TMG-E verletzen die bundesstaatliche Kompetenzordnung, soweit diese Vorschriften eine Pflicht zu Datenübermittlungen auch in Fällen normieren, in denen die Regelungskompetenz für den behördlichen Datenzugriff bei den Ländern liegt. Im Übrigen sind die Vorschriften weitgehend redundant, da sich Übermittlungspflichten zumeist auch im behördlichen Fachrecht finden. Sie können und sollten ersatzlos gestrichen werden.
4. Die in § 15a Abs. 2 Satz 1 TMG-E enthaltene Übermittlungserlaubnis für Telemedienanbieter ist zu weit gefasst und unverhältnismäßig, soweit sie sich auf Telemedien-Nutzungsdaten erstreckt. Gegen die vorgesehene strafprozessuale Zugriffsermächtigung in § 100g Abs. 1 Satz 2 StPO-E bestehen gleichfalls verfassungsrechtliche Bedenken, da sie der potenziellen besonderen Sensibilität dieser Datenkategorie nicht vollumfänglich Rechnung trägt.
5. In dem Entwurf fehlt eine strafprozessuale Ermächtigung zur Inhaltsüberwachung von Telemedien. Entgegen der Entwurfsbegründung ist eine solche Ermächtigung nicht deshalb entbehrlich, weil eine solche Überwachung auf die Ermächtigung zu Telekommunikationsüberwachungen in § 100a StPO gestützt werden könnte. Dieser Ansatz birgt erhebliche Rechtsunsicherheit und Risiken für die Effektivität der Strafverfolgung.
6. Die Erlaubnis zur Übermittlung von Telemedien-Zugangsdaten in § 15b Abs. 2 Satz 1 TMG-E und die Ermächtigung zum Zugriff auf solche Daten in § 100j Abs. 1 Satz 2 StPO-E sind inkongruent. Wegen der sehr hohen Sensibilität dieser Datenkategorie sollte die Übermittlungsschwelle des § 15b Abs. 2 Satz 1 TMG-E in die strafprozessuale Ermächtigung überführt werden.
7. Die Zitierung des Fernmeldegeheimnisses in Art. 7 des Entwurfs ist selbst dann noch unvollständig, wenn der Änderungsvorschlag des Bundesrates umgesetzt wird. Als Art. 10 GG einschränkende Norm muss auch § 100g StPO-E (Art. 2 Nr. 2 des Entwurfs) zitiert werden, da sich der Schutzbereich des Fernmeldegeheimnisses zumindest auf manche Telemedien-Nutzungsdaten erstreckt.

⁴ In der knappen Zeit, die mir zur Verfügung stand, war mir eine umfassende Stellungnahme zu allen verfassungsrechtlichen und gesetzgebungstechnischen Fragen, die der Entwurf aufwirft, nicht möglich. Ich beschränke mich darum im Folgenden auf zwei Themenkomplexe: die Pflicht bestimmter Netzbetreiber zur Meldung bestimmter Inhalte an das Bundeskriminalamt (unten I) sowie die Regelungen zur Übermittlung von Telemediendaten an Sicherheitsbehörden und zum behördlichen Zugriff auf diese Daten (unten II). Außen vor bleiben damit insbesondere die vorgesehenen Änderungen im materiellen Strafrecht, die gleichfalls teilweise erhebliche Probleme bergen.¹ Hierzu kann ich gegebenenfalls in der Anhörung mündlich Stellung nehmen.

I. Meldung strafbarer Inhalte an das Bundeskriminalamt

Gegen die vorgesehene Pflicht von Netzbetreibern, bestimmte mutmaßlich strafbare Kommunikationsinhalte an das Bundeskriminalamt zu melden (§ 3a NetzDG-E), bestehen keine fundamentalen verfassungsrechtlichen Bedenken.² Allerdings reicht diese Pflicht hinsichtlich der mit zu übermittelnden Identifikationsdaten teils zu weit. Folgefragen wirft die Weiterverarbeitung der übermittelten Daten durch das Bundeskriminalamt auf.

1. Keine grundlegenden verfassungsrechtlichen Bedenken

Im Grundansatz ist die in § 3a NetzDG-E enthaltene Meldepflicht verfassungskonform. Insbesondere wird hiermit nicht etwa in rechtsstaatlich bedenklicher Weise eine genuin hoheitliche Tätigkeit an Private delegiert. Die Meldepflicht fügt sich vielmehr in ein Gefüge vergleichbarer Pflichten marktmächtiger Unternehmen ein, mit denen diese zur Unterstützung hoheitlicher Aufsichts- und Sanktionsaufgaben in Dienst genommen werden.

Meiner Ansicht nach ist es auch vertretbar, die Bearbeitung der Meldungen unter die Zentralstellenaufgabe des Bundeskriminalamts zu subsumieren, wenngleich es sich um einen Grenzfall handelt. Die Meldepflicht soll dazu dienen, dass das Bundeskriminalamt – in strafprozessualer Terminologie – in den Meldefällen Vorermittlungen anstellt, um das Vorliegen eines Anfangsverdachts zu prüfen und eine zuständige Landesstraßverfolgungsbehörde zu ermitteln. Eine solche Tätigkeit weicht von den üblicherweise unter den Zentralstellenbegriff subsumierten Service- und Koordinationstätigkeiten³ deutlich ab und nähert sich einer operativen Aufgabe zumindest an. Die Zuständigkeit der Zentralstelle lässt sich aber mit der in der Gesetzesbegründung vorgebrachten Erwägung begründen, dass sich bei den in § 3a Abs. 2 Nr. 3 NetzDG-E genannten Kommunikationsdelikten im Internet eine zuständige Strafverfolgungsbehörde nicht ohne weite-

¹ Vgl. die Stellungnahme des Sachverständigen Prof. Dr. Engländer.

² Nicht erörtert werden im Folgenden die allgemeinen Bedenken, die gegen das NetzDG insgesamt aus der bundesstaatlichen Ordnung der Gesetzgebungskompetenzen sowie aus dem Unionsrecht, insbesondere der E-Commerce-Richtlinie, abgeleitet werden. Diese Bedenken sind nicht neu und werden durch den Entwurf meines Erachtens zumindest nicht verschärft.

³ Näher zu diesem Begriff aus kompetenzrechtlicher Sicht Bäcker, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. 2018, Rn. B 127 ff.

⁵ res bestimmen lässt. Insbesondere kann – entgegen einer Tendenz in der früheren Rechtsprechung – nicht einfach auf die bundesweite Zugänglichkeit der Inhalte abgestellt werden, um eine Zuständigkeit aller Staatsanwaltschaften in Deutschland zu begründen.⁴

2. Verfassungs- und unionsrechtliches Gebot einer zweistufigen Ausgestaltung

Jedoch reicht die Meldepflicht inhaltlich zu weit bzw. ist zu undifferenziert ausgestaltet. Sie verletzt darum in ihrer derzeit vorgesehenen Ausgestaltung höherrangiges Recht.

Gemäß § 3a Abs. 4 NetzDG-E soll der Netzanbieter verpflichtet sein, dem Bundeskriminalamt neben dem mutmaßlich strafbaren Inhalt die letzte IP-Adresse und Portnummer des betroffenen Nutzers mitzuteilen. Hierbei handelt es sich um personenbezogene Daten, da mit ihrer Hilfe die Lokalisierung und Identifikation des Nutzers ermöglicht wird und auch werden soll.⁵ Die Meldepflicht greift daher zum einen in das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ein. Zum anderen ist sie als gesetzliche Datenverarbeitungspflicht, die eine Zweckänderung der übermittelten Daten bewirkt, an Art. 6 Abs. 1 Satz 1 lit. c, Abs. 3 sowie Art. 6 Abs. 4 i.V.m. Art. 23 Abs. 1 lit. d DSGVO zu messen.⁶ Diese höherrangigen Regelungen verlangen übereinstimmend, dass die durch die Meldepflicht vorgegebene Datenübermittlung erforderlich ist, um das Ziel der Verfolgung bestimmter Straftaten zu erreichen.

Dies ist jedoch nicht durchweg der Fall. Die Prüfung des übermittelten Inhalts durch das Bundeskriminalamt kann und wird in vielen Fällen ergeben, dass dieser Inhalt entgegen der Ansicht des Netzbetreibers keinen Straftatbestand erfüllt. Hiervon geht ersichtlich auch die Entwurfsbegründung aus, die eine weit höhere Zahl von Meldungen (250.000) als von anschließenden Ermittlungsverfahren (150.000) erwartet.⁷ In einem solchen Fall ist eine Identifizierung des Nutzers, der den Inhalt veröffentlicht hat, nicht angezeigt und werden die Identifikationsdaten nicht benötigt. Verfassungsrechtlich unzulässig wäre insbesondere eine tatverdachtsunabhängige vorsorgliche Identifikation aller Nutzer, deren Inhalte gemeldet werden, durch Bestandsdatenabrufe auf der Grundlage von § 10 Abs. 1 Nr. 1, Abs. 2 BKAG i.V.m. § 113 Abs. 1 Satz 3 TKG. Diese Normen setzen bei verfassungskonformer Auslegung den Anfangsverdacht einer Straftat voraus⁸ und ermöglichen daher keinen Datenabruf zu einem Zeitpunkt, in dem gerade noch nicht geklärt ist, ob ein Anfangsverdacht besteht oder nicht. Erforderlich ist die Übermittlung

⁴ Näher zum Problem der für die Zuständigkeit maßgeblichen Bestimmung des Tatorts bei Internetstraftaten, die – wie zumindest die Mehrzahl der in § 3a Abs. 2 Nr. 3 NetzDG-E genannten Tatbestände – weder als Erfolgs- noch als konkrete Gefährdungsdelikte ausgestaltet sind, Heintschel-Heinegg, in: BeckOK StGB, Stand 2020, § 9 Rn. 19 ff.; Eser/Weißer, in: Schönke/Schröder, StGB, 30. Aufl. 2019, § 9 Rn. 7 ff.; Ambos, in: MüKo StGB, 3. Aufl. 2017, § 9 Rn. 26 ff.; Kudlich/Berberich, NStZ 2019, S. 633 ff.

⁵ Vgl. BT-Drs. 19/17741, S. 44 f.

⁶ Ich gehe hier davon aus, dass eine zweckändernde Datenverarbeitung sowohl einer Verarbeitungs- als auch einer Zweckänderungserlaubnis bedarf, wie hier etwa Buchner/Petri, in: Kühling/Buchner, DS-GVO/BDSDG, 2. Aufl. 2018, Art. 6 DSGVO Rn. 181 ff. Die folgenden Ausführungen ließen sich allerdings auch auf der Grundlage der Gegenposition begründen, nach der Zweckänderungserlaubnis die Verarbeitungserlaubnis mitumfasst.

⁷ BT-Drs. 19/17741, S. 29.

⁸ Vgl. BVerfGE 130, 151 (206).

- ⁶ der in § 3a Abs. 4 Nr. 2 NetzDG-E genannten Daten daher nur, wenn die Prüfung durch das Bundeskriminalamt den Anfangsverdacht einer Straftat ergibt.

Hieraus folgt, dass die Meldepflicht zweistufig auszugestalten ist. Zunächst darf der Netzwerkanbieter nur zur Übermittlung des mutmaßlich strafbaren Inhalts verpflichtet werden. Erst nach einer inhaltlichen Prüfung, die einen Anfangsverdacht ergibt, darf er auch zur Übermittlung der Identifikationsdaten auf Anforderung des Bundeskriminalamts verpflichtet werden. Zulässig und sinnvoll ist es darüber hinaus, den Netzwerkanbieter zu verpflichten, gleichzeitig mit der Übermittlung des Inhalts die in § 3a Abs. 4 Nr. 2 NetzDG-E genannten Identifikationsdaten zu speichern und bis zu einer Rückmeldung des Bundeskriminalamts aufzubewahren („quick freeze“). Mit dem Erforderlichkeitsgrundsatz vereinbar und zudem möglicherweise sogar wirkungsvoller als die in § 3a Abs. 4 Nr. 2 NetzDG-E vorgesehene Meldepflicht wäre es darüber hinaus, den Netzwerkanbieter auch zu verpflichten, bis zur Rückmeldung des Bundeskriminalamts gegebenenfalls weitere Identifikationsdaten zu speichern, die bei einer zwischenzeitlichen Nutzung des Netzwerks durch den fraglichen Nutzer anfallen. Zur Beschleunigung der Identifizierung könnten die Netzwerkanbieter schließlich verpflichtet werden, die Identifikationsdaten mittels einer technischen Schnittstelle zum jederzeitigen automatisierten Abruf durch das Bundeskriminalamt vorzuhalten.

3. Weiterverarbeitung der übermittelten Daten

Hinweisen möchte ich darauf, dass das Bundeskriminalamt die aufgrund von § 3a NetzDG-E übermittelten Daten nicht nur zur Einleitung einzelner Strafverfahren bzw. zur Abwehr konkreter Gefahren nutzen darf, sondern eine einzelfallübergreifende, strategisch ausgerichtete Weiterverarbeitung zulässig ist und kriminalistisch naheliegt. Dies wird aus der Entwurfsbegründung nicht deutlich, in der es heißt, die Daten seien „regelmäßig... nach Übermittlung der betreffenden Daten an die zuständige Strafverfolgungsbehörde“ zu löschen.⁹ Bei Meldungen, zu denen das Bundeskriminalamt einen Tatverdacht bejaht, liegt nach meiner Einschätzung nahe, dass im Gegenteil die umgehende Löschung faktisch eher den Ausnahmefall darstellen wird.

Die Inhalte und ggfs. Identifikationsdaten werden dem Bundeskriminalamt in seiner Zentralstellenfunktion übermittelt. Sie können daher, ohne dass eine besonders legitimationsbedürftige Zweckänderung vorläge, im Rahmen der Zentralstellenaufgabe gemäß § 16 Abs. 1 i.V.m. § 12 Abs. 1 Satz 1 BKAG sowie ggfs. aufgrund von § 18 Abs. 1 Nr. 3 BKAG weiterverarbeitet werden. Der Begriff der Weiterverarbeitung schließt insbesondere eine Bevorratung der Daten im Informationssystem des Bundeskriminalamts (§ 13 BKAG) ein, um die Daten in späteren, noch nicht zwangsläufig absehbaren polizeilichen Verfahren nutzen zu können. Die Daten könnten etwa in Lagebilder bestimmter Phänomenbereiche oder in Analysen von Diskurszusammenhängen zur Früherkennung von Radikalisierungsprozessen und Gewaltereignissen einfließen. Die in § 3a Abs. 2 NetzDG-E für die Übermittlung vorgesehene Zweckbestimmung der „Ermöglichung der Verfolgung von Straftaten“ steht einer solchen Weiterverarbeitung nicht entgegen, da sie sprach-

⁹ BT-Drs. 19/17741, S. 15.

⁷ lich zwanglos auch auf die Verfolgung zukünftiger, noch nicht absehbarer Straftaten (sog. Verfolgungsvorsorge) bezogen werden kann. Aus höherrangigem Recht bestehen hiergegen angesichts der begrenzten Eingriffsintensität der Weiterverarbeitung der übermittelten Daten keine prinzipiellen Bedenken.

Kritisch zu sehen wäre hingegen eine Weiterverarbeitung in Fällen, in denen das Bundeskriminalamt einen Tatverdacht verneint, weil es den gemeldeten Inhalt für (noch) zulässig hält. Für eine derartige Weiterverarbeitung ließen sich allerdings durchaus Rechtsgrundlagen finden. Neben der schon genannten Ermächtigung aus § 16 Abs. 1 i.V.m. § 12 Abs. 1 Satz 1 BKAG, die weder einen Tatverdacht noch eine auf die betroffene Person bezogene Kriminalprognose voraussetzt, kommt hierfür insbesondere § 18 Abs. 1 Nr. 4 BKAG in Betracht. Anknüpfungspunkt der Kritik müssen dementsprechend weniger die im Gesetzentwurf vorgesehenen Regelungen als die verfassungsrechtlich sehr zweifelhaften Bestandsnormen im BKAG sein. Ich sehe aus diesem Grund davon ab, die Kritik hier zu vertiefen.¹⁰

II. Übermittlung von und Zugriff auf Telemediendaten

Der Entwurf sieht eine Reihe von Regelungen vor, welche die Übermittlung von Telemediendaten an Sicherheitsbehörden und den behördlichen Zugriff auf solche Daten rechtssicher ermöglichen sollen. Dieses Ziel wird allerdings nicht vollumfänglich erreicht. Insbesondere aufgrund einiger konzeptioneller Unklarheiten gibt der Entwurf die Datenverarbeitung teils in zu weitem Umfang frei und weist einige Lücken auf.

1. Vorfragen

Bevor die einzelnen vorgesehenen Regelungen näher erörtert und kritisiert werden können, bedarf es konzeptioneller Vorklärungen. Diese betreffen zum einen die juristische Konstruktion des sicherheitsbehördlichen Zugriffs auf gesellschaftliche Datenbestände, zu denen auch Telemediendaten zählen, zum anderen die Definition und Abgrenzung der für den Entwurf relevanten Datenkategorien.

a) Doppeltürmodell und grundrechtliche Regelungsverantwortung

Der sicherheitsbehördliche Zugriff auf gesellschaftliche Datenbestände wird datenschutzrechtlich als zweiaktiger Vorgang konstruiert: Das private Unternehmen, das bestimmte Daten an eine Sicherheitsbehörde transferiert, benötigt hierfür eine Übermittlungserlaubnis. Die Sicherheitsbehörde benötigt zur Entgegennahme und zum weiteren Umgang mit den Daten einer Zugriffsermächtigung. Das Bundesverfassungsgericht verwendet für diese Regelungsstruktur das

¹⁰ Gegen die genannten Normen ist seit Mai 2019 eine von mir als Prozessbevollmächtigtem vertretene Verfassungsbeschwerde bei dem Bundesverfassungsgericht anhängig (Az. 1 BvR 1160/19), über die noch nicht entschieden und die zumindest bislang auch nicht zugestellt wurde. Der Text meiner Beschwerdeschrift ist abrufbar unter <https://freiheitsrechte.org/home/wp-content/uploads/2019/10/2019-05-21-BKA-Gesetz-VB-anonymisiert.pdf>.

⁸ Bild einer Doppeltür.¹¹ Das originär datenschutzrechtliche Doppeltürmodell ist in zweifacher Hinsicht verfassungsrechtlich bedeutsam:

Erstens ist die Gesetzgebungskompetenz für den Datentransfer anhand dieses Modells zu differenzieren.¹² Die Kompetenz für die Übermittlungserlaubnis liegt bei dem Gesetzgeber, der das Datenschutzrecht für die übermittelnde Stelle regeln darf. Für den Telemediendatenschutz ergibt sich aus Art. 74 Abs. 1 Nr. 11 GG eine konkurrierende Gesetzgebungskompetenz des Bundes.¹³ Die Kompetenz für die Zugriffsermächtigung richtet sich hingegen nach der Gesetzgebungskompetenz für die jeweilige Sicherheitsbehörde, der ein Zugriff erlaubt werden soll. Dies führt wegen der differenzierten Kompetenzrechtslage für das Sicherheitsrecht zu einer zwischen Bund und Ländern aufgeteilten Regelungsbefugnis. So ist der Bund für die Regelung strafprozessualer Zugriffe gemäß Art. 74 Abs. 1 Nr. 1 GG zuständig, während Zugriffe durch die Landespolizeibehörden von den Ländern zu regeln sind.

Zu beachten ist, dass die Regelungsbefugnis des Gesetzgebers der Übermittlungserlaubnis lediglich die Erlaubnis, nicht aber die Pflicht zur Übermittlung umfasst. Das Bundesverfassungsgericht hat hierzu ausgeführt, eine Pflicht der Unternehmen zur Datenübermittlung sei als Teil des Abrufs kompetenziell den Gesetzgebern der Zugriffsermächtigungen zugewiesen, also in weitem Umfang den Ländern.¹⁴

Zweitens sind die materiellen verfassungsrechtlichen Anforderungen an den Gesamtvorgang zwischen den beiden Regelungen zu verteilen. Nach der Rechtsprechung des Bundesverfassungsgerichts trifft den Gesetzgeber, der für die Übermittlungserlaubnis zuständig ist, eine grundrechtliche Regelungsverantwortung für den Umgang mit den übermittelten Daten. Er muss die Zwecke der zulässigen Übermittlungen normenklar bestimmen und durch hinreichend strenge Tatbestandsvoraussetzungen gewährleisten, dass diese Übermittlungen den Verhältnismäßigkeitsgrundsatz wahren.¹⁵ Bedeutsam ist dies insbesondere, wenn die Regelungskompetenzen für die Übermittlungserlaubnis und die Zugriffsermächtigung auseinanderfallen. In einem solchen Fall muss zwingend bereits die Übermittlungserlaubnis eine hinreichende tatbestandliche Übermittlungsschwelle errichten.

b) Differenzierung und Abgrenzung von Telemedien und Telekommunikation

Die vorgesehenen Regelungen beruhen auf der in § 1 Abs. 1 Satz 1 TMG i.V.m. § 3 Nr. 24 TKG geregelten Differenzierung zwischen Telemedien- und Telekommunikationsdiensten. Weil es sich um rechtlich getrennte Arten von Kommunikationsdiensten handelt, sollen auch die Übermittlung der bei der Dienstleistung anfallenden Daten an Sicherheitsbehörden sowie der behördliche Zugriff auf diese Daten ausdrücklich voneinander unterschieden werden.

¹¹ Grundlegend BVerfGE 130, 151 (184); daran anknüpfend BVerfGE 141, 220 (333 f.); 150, 244 (278); 150, 309 (335).

¹² BVerfGE 130, 151 (200 ff.).

¹³ Vgl. Heintzen, in: v. Mangoldt/Klein/Starck, GG, 7. Aufl. 2018, Art. 73 Rn. 76.

¹⁴ BVerfGE 130, 151 (201).

¹⁵ Vgl. BVerfGE 125, 260 (344, 346); 130, 151 (201); 141, 220 (333 f.).

⁹ Die Differenzierung zwischen beiden Dienstetypen hat eine Wurzel im Unionsrecht, da der Begriff des Telekommunikationsdienstes durch Art. 2 lit. c der derzeit noch geltenden Rahmenrichtlinie für die elektronische Kommunikation¹⁶ vorgeprägt wird. Der Gerichtshof der Europäischen Union hat diese Norm kürzlich eng ausgelegt, so dass zahlreiche verbreitete internet-basierte Kommunikationsdienste nicht unter den unionsrechtlichen Begriff des elektronischen Kommunikationsdienstes fallen, da sie nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen. Konkret entschieden hat der Gerichtshof dies für E-Mail-Dienste.¹⁷ Ebenso dürften zahlreiche weitere sogenannte Over-the-Top-Dienste zu behandeln sein, etwa Messengerdienste wie WhatsApp oder Soziale Medien wie Facebook (letztere auch insoweit, als sie Funktionen für den Nachrichtenaustausch zwischen Individuen enthalten). Solche Kommunikationsdienste sind dementsprechend nach deutschem Recht als Telemediendienste einzustufen.

Die Übermittlungserlaubnisse für Diensteanbieter, die das Telekommunikationsrecht enthält, können nicht auf Telemedienanbieter angewandt werden. Zudem beschränkt sich der Anwendungsbereich einiger Überwachungsermächtigungen im Sicherheitsrecht auf Datenerhebungen mit Bezug zur Telekommunikation im telekommunikationsrechtlichen Sinne. Es bedarf daher für telemedienbezogene Überwachungsmaßnahmen spezifischer Rechtsgrundlagen, welche die Übermittlung von Telemediendaten an Sicherheitsbehörden und den behördlichen Zugriff auf solche Daten regeln. Der Entwurf soll solche Regelungen schaffen und dabei einen prinzipiellen Gleichlauf zwischen telekommunikations- und telemedienbezogenen Überwachungsmaßnahmen herstellen.

Die Begrifflichkeiten könnten sich in naher Zukunft verschieben. Der bis Ende des Jahres in deutsches Recht umzusetzende Kommunikationskodex¹⁸ fasst den Anwendungsbereich des europäischen Kommunikationsrechts neu. Gemäß Art. 2 Nr. 4 Kommunikationskodex umfasst der zentrale Begriff des elektronischen Kommunikationsdienstes fortan unter anderem alle interpersonellen Kommunikationsdienste, die über elektronische Kommunikationsnetze erbracht werden. Es kommt danach – anders als nach geltendem Recht – nicht darauf an, ob solche Dienste ganz oder überwiegend in der Übertragung von Signalen bestehen. Mit der Umsetzung des Kommunikationskodex wird sich – unterstellt, es bleibt bei der aktuellen Terminologie im deutschen Recht – der Begriff des Telekommunikationsdienstes erweitern und der Begriff des Telemediendienstes entsprechend verengen.¹⁹ Dementsprechend könnten die Übermittlung von und der behördliche Zugriff auf Daten aus interpersonellen Over-the-Top-Kommunikationsdiensten ab diesem Zeitpunkt auf die Regelungen zu stützen sein, die sich auf Telekommunikationsdaten

¹⁶ Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie), ABl. L 108 vom 24. April 2002, S. 33, zuletzt geändert durch die Richtlinie 2009/140/EG vom 25. November 2009, ABl. L 337 vom 18. Dezember 2009, S. 37.

¹⁷ EuGH, Urteil vom 13. Juni 2019, Rs. C-193/18 – Google LLC gegen Bundesrepublik Deutschland.

¹⁸ Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation, ABl. L 321 vom 17. Dezember 2018, S. 36.

¹⁹ Kiparski, CR 2019, S. 179 (180).

¹⁰ beziehen. Die praktische Relevanz der im Entwurf vorgesehenen Rechtsänderungen würde sich damit erheblich vermindern.

Zwingend wäre diese Schlussfolgerung allerdings nicht. Insbesondere enthält der Kommunikationskodex keine Regelungen zu der im vorliegenden Zusammenhang besonders relevanten Rechtsmaterie des Telekommunikations-Datenschutzes. Eine angestrebte Neuregelung dieser Materie ist bislang nicht gelungen. Bis auf Weiteres bleibt daher die alte Richtlinie über den Datenschutz bei der elektronischen Kommunikation maßgeblich. Da deren sachlicher Anwendungsbereich sich nach der Rahmenrichtlinie bestimmt, könnte es in Zukunft dazu kommen, dass ein regulierungsrechtlicher und ein datenschutzrechtlicher Telekommunikationsbegriff zu unterscheiden sind. Es erschiene dann naheliegend, für die Übermittlung von Kommunikationsdaten an Sicherheitsbehörden und den behördlichen Zugriff auf diese Daten auf den engeren datenschutzrechtlichen Telekommunikationsbegriff abzustellen.

Letztlich wird die Frage nach der zukünftigen Reichweite der auf Telemedien bezogenen Übermittlungs- und Überwachungsregelungen mittelbar vom deutschen Gesetzgeber zu beantworten sein, wenn er den Kommunikationskodex umsetzt. Meine Stellungnahme beschränkt sich im Folgenden auf den gegenwärtigen, möglicherweise kurzlebigen Rechtsstand.

c) Kategorien von Telekommunikations- und Telemediendaten

Der Entwurf verfolgt erkennbar den Regulierungsansatz, Telekommunikations- und Telemediendienste hinsichtlich der Übermittlung von Kommunikationsdaten an Sicherheitsbehörden und des behördlichen Zugriffs auf solche Daten gleichzubehandeln. Eine solche Parallelisierung fand sich schon bislang (zumindest teilweise) in einigen Fachgesetzen der Sicherheitsbehörden.²⁰ Ihre Überzeugungskraft hängt allerdings maßgeblich davon ab, inwieweit sich für Telekommunikations- und Telemediendienste vergleichbare Datenkategorien bilden lassen, hinsichtlich derer einem behördlichen Zugriff jeweils eine gleichartige Eingriffsintensität zukommt.

Das Telekommunikations- und das Telemedienrecht kennen gleichermaßen die Datenkategorie der Bestandsdaten.²¹ Hierbei handelt es sich jeweils um Daten, die für „die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses“ zwischen dem Diensteanbieter und dem Nutzer benötigt werden. Bestandsdaten sind mithin Basisdaten eines Nutzungsvertrags, die sich nicht auf einen konkreten Kommunikationsvorgang beziehen. Beispiele bilden Name, Anschrift oder Bankverbindung des Nutzers. Die Sensibilität von Telekommunikations-Bestandsdaten und Telemedien-Bestandsdaten erscheint ohne weiteres vergleichbar, so dass sich eine Gleichbehandlung hinsichtlich der Übermittlung und des behördlichen Zugriffs aufdrängt.

Einen Sonderfall der Bestandsdaten bilden die bisher nur im Telekommunikationsrecht ausdrücklich erwähnten Zugangsdaten. Hierbei handelt es sich um „Daten, mittels derer der Zugriff

²⁰ Vgl. beispielhaft für den Zugriff auf Telekommunikations-Verkehrsdaten und Telemedien-Nutzungsdaten § 52 BKAG. Hingegen enthält das BKAG bislang keine ausdrückliche Ermächtigung zur Erhebung von Telemedien-Bestandsdaten.

²¹ § 3 Nr. 3 TKG; § 14 Abs. 1 TMG.

¹¹ auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird“.²² Die Verarbeitung von Zugangsdaten durch die Diensteanbieter zu eigenen Zwecken wird dabei nicht besonders reguliert. Diese Unterkategorie ist nur für Datenübermittlungen an Sicherheitsbehörden bedeutsam.²³

Im Telekommunikationsrecht werden des Weiteren zwei Kategorien von Daten unterschieden, die sich jeweils auf konkrete Kommunikationsvorgänge beziehen. Dabei handelt es sich zum einen um die Kommunikationsinhalte,²⁴ zum anderen um die Verkehrsdaten. Dies sind Metadaten der Kommunikation, die „bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden.“²⁵ Hierzu zählt beispielsweise die Information, zwischen welchen Rufnummern zu welcher Zeit ein Telefongespräch geführt wurde. Das geltende Sicherheitsrecht stellt an Zugriffe auf beide Datenkategorien teils identische Anforderungen (so etwa § 51 Abs. 1 und § 52 Abs. 1 BKAG). In anderen Regelungswerken wird hingegen der Zugriff auf Telekommunikations-Verkehrsdaten wegen deren – vermeintlich – geringerer Sensibilität unter weniger engen Voraussetzungen ermöglicht als Inhaltsüberwachungen der Telekommunikation (etwa in § 100a Abs. 1 und § 100g Abs. 1 StPO).

Schwieriger und kontroverser ist die Kategorisierung von Telemediendaten. Das Telemedierecht nennt ausdrücklich neben den Bestandsdaten nur die Nutzungsdaten als weitere Datenkategorie. Hierbei handelt es sich gemäß § 15 Abs. 1 TMG um Daten, die erforderlich sind, „um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen“. Beispielhaft nennt das Gesetz Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie den Umfang der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien. Die Telemedien-Nutzungsdaten entsprechen damit – zumindest auf den ersten Blick – den Telekommunikations-Verkehrsdaten. Hiervon geht auch der Entwurf erkennbar aus.

Hingegen findet sich im Telemedierecht keine Datenkategorie, die den Inhalten der Telekommunikation entspräche. Dabei ist offenkundig, dass es auch Telemedieninhalte gibt. Bestellt beispielsweise jemand Waren bei einem Online-Versandhändler, so sind die im Rahmen der Bestellung anfallenden technischen Metadaten (beispielsweise die IP-Adresse, unter der die Bestellung aufgegeben wird, oder die Uhrzeit der Bestellung) Nutzungsdaten. Die Angabe, welche Waren der Nutzer bestellt hat, ist hingegen kein auf das Telemedium (die Website des Versandhändlers) bezogenes Nutzungsdatum, sondern ein über das Telemedium transportiertes Datum, das sich auf den abgeschlossenen Kaufvertrag bezieht. Bei den der Individualkommunikation dienenden Over-the-Top-Diensten wie E-Mail, Chat oder Instant Messaging erscheint es zumindest fragwürdig, ob sich die übermittelten Nachrichten als Nutzungsdaten einordnen lassen.

²² § 113 Abs. 1 Satz 2 TKG; derselbe Wortlaut findet sich in § 15a Abs. 1 Satz 2 und § 15b Abs. 1 Satz 1 TMG-E.

²³ Vgl. zum verfassungsrechtlichen Hintergrund BVerfGE 130, 151 (207 ff.).

²⁴ Vgl. § 88 Abs. 1 Satz 1 TKG.

²⁵ § 3 Nr. 30 TKG.

¹² Wie Telemedien-Inhaltsdaten zu behandeln sind, war lange umstritten. Teils wurde eine direkte oder analoge Anwendung der Vorschriften über Nutzungsdaten vertreten. Nach der Gegenauffassung sollten die Inhaltsdaten nach allgemeinem Datenschutzrecht zu beurteilen sein – mit der Konsequenz eines im Vergleich zu Nutzungsdaten schwächeren Schutzes. Der Streit wird heute vielfach für überwunden gehalten, da Telemediendaten spätestens seit Inkrafttreten des novellierten europäischen Rechtsrahmens generell dem allgemeinen Datenschutzrecht unterfielen.²⁶ Dies mag für Datenverarbeitungen durch den Telemedienanbieter zu eigenen Zwecken zutreffen, gilt jedoch nicht für die zweckändernde Übermittlung von Telemediendaten an eine Sicherheitsbehörde sowie für den sicherheitsbehördlichen Zugriff auf die Daten. Hinsichtlich dieser Datenverarbeitungen bestehen mitgliedstaatliche Regelungsspielräume.²⁷ Zur Ausfüllung dieser Spielräume könnte durchaus zwischen Nutzungs- und Inhaltsdaten differenziert werden.

Die Abgrenzung dieser Datenkategorien bereitet allerdings im Detail erheblich größere Schwierigkeiten als die Abgrenzung zwischen Telekommunikationsinhalten und Telekommunikationsverkehrsdaten. Grund hierfür ist, dass der Telemedienbegriff sich auf eine viel größere Zahl unterschiedlicher Kommunikationsdienste mit unterschiedlichen kommunikativen Funktionen und Wirkungsweisen bezieht. Eine statische Webseite im World Wide Web, die lediglich zum Leseabruf zur Verfügung steht, ist ebenso ein Telemedium wie ein webbasiertes Diskussionsforum, ein E-Mail-Dienst oder ein Online-Shop. Zudem ist der Telemedienbegriff unterschiedlichen Abstraktionsstufen zugänglich und kann darum über- und untergeordnete Dienste gleichermaßen umfassen. Beispielsweise lässt sich ein Soziales Netzwerk ebenso als Telemedium einstufen wie eine einzelne auf diesem Netzwerk betriebene Profilseite eines Unternehmens. Je nach Dienst können Nutzungs- und Inhaltsebene verschwimmen (so beim Abruf der statischen Webseite, je nach Perspektive auch bei der Übermittlung von Nachrichten über Over-the-Top-Dienste). Denkbar ist auch, dieselben Daten für einen Dienst als Nutzungs- und für einen anderen Dienst als Inhaltsdaten einzustufen (so etwa, wenn ein Besucher eine Nachricht auf der Profilseite eines Sportartikelherstellers in einem Sozialen Netzwerk hinterlässt – Inhaltsdatum im Verhältnis zu dem Sportartikelhersteller, möglicherweise Nutzungsdatum im Verhältnis zu dem Netzwerkbetreiber).

Zudem liegt nahe, dass Nutzungs- und Inhaltsdaten je nach Dienst unterschiedlich sensibel sein können. Die Angabe, dass jemand einen bestimmten Dienst genutzt hat, kann aussagekräftiger und für den Betroffenen kritischer sein als die über diesen Dienst vermittelten Inhalte (so etwa bei der Nutzung eines webbasierten Diskussionsforums, bei dem die Inhalte, nicht aber die Nutzungsdaten öffentlich zugänglich sind). In anderen Fällen erscheinen die Inhalte zumindest ten-

²⁶ Schmitz, in: Spindler/ders., TMG, 2. Aufl. 2018, § 15 Rn. 84; Tinnefeld/Buchner, in: BeckOK DatenschutzR, Stand 2019, Syst. I Rn. 91 ff.

²⁷ Für die Übermittlung aus Art. 6 Abs. 1 lit. c, Abs. 3 sowie aus Art. 6 Abs. 4 i.V.m. Art. 23 Abs. 1 lit. a, c oder d DSGVO; für den Datenzugriff – soweit er nicht dem Anwendungsbereich des europäischen Datenschutzrechts vollständig entzogen ist – aus Art. 8 RL (EU) 2016/680.

¹³ denziell sensibler als die Nutzungsdaten (so etwa bei Over-the-Top-Diensten, die der Individualkommunikation dienen, wie E-Mail oder Instant Messaging, sofern hier zwischen Nutzungs- und Inhaltsdaten unterschieden wird).

2. Übermittlung von und Zugriff auf Bestandsdaten

Die vorgesehenen Regelungen über die Übermittlung von und den behördlichen Zugriff auf Telemedien-Bestandsdaten genügen nicht vollständig den verfassungsrechtlichen Anforderungen.

Gemäß § 15a Abs. 1 Satz 1, Abs. 2 Satz 1, Abs. 3 TMG-E darf ein Telemedienanbieter (unter anderem) Bestandsdaten an Sicherheitsbehörden zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung sowie für die Erfüllung nachrichtendienstlicher Aufgaben übermitteln. Diese Übermittlungsschwelle stimmt wörtlich mit dem für Telekommunikations-Bestandsdaten maßgeblichen § 113 Abs. 2 Satz 1 TKG überein. Die tatbestandlichen Voraussetzungen jener Norm hat das Bundesverfassungsgericht wiederum als „verfassungsrechtlich noch hinnehmbar“ bezeichnet.²⁸ Diese Bewertung lässt sich wegen der Strukturgleichheit und gleichartigen Sensibilität von Telekommunikations- und Telemedien-Bestandsdaten ohne weiteres auf die vorgesehene Regelung übertragen. Keine Bedenken bestehen des Weiteren gegen die strafprozessuale Zugriffsermächtigung in § 100j Abs. 1 Satz 1 Nr. 2 StPO-E, die den Zugriff von einem strafrechtlichen Tatverdacht abhängig macht.

Über das verfassungsrechtlich zulässige Maß geht hingegen die vorgesehene Zugriffsermächtigung in § 10 Abs. 1 Satz 2 BKAG-E hinaus, zumindest soweit sie auf § 10 Abs. 1 Satz 1 Nr. 1 BKAG Bezug nimmt.

§ 10 Abs. 1 Satz 2 BKAG-E soll dem Bundeskriminalamt Bestandsdatenzugriffe unter anderem im Rahmen seiner Zentralstellenaufgabe „zur Ergänzung vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung“ ermöglichen. Diese Zugriffsermächtigung ermöglicht dem Bundeskriminalamt Datenerhebungen bereits weit im Vorfeld konkreter Gefahren oder strafprozessualer Ermittlungsverfahren. Das Bundeskriminalamt könnte danach Bestandsdatenzugriffe zur Unterstützung kriminalstrategischer Analysen nutzen, die es unabhängig von konkreten einzelfallbezogenen Verdachtsmomenten durchführt.

Damit sind die Grenzen des verfassungsrechtlich noch Hinnehmbaren auf der Grundlage der Rechtsprechung zu Telekommunikations-Bestandsdaten überschritten. Eine im Vorfeld von konkreter Gefahr oder Tatverdacht angesiedelte Zugriffsermächtigung erscheint zwar – auch angesichts der gemäßigten Eingriffsintensität von Bestandsdatenabfragen – nicht von vornherein ausgeschlossen.²⁹ Sie müsste jedoch zumindest entweder den Eingriffsanlass in tatsächlicher Hinsicht näher konturieren oder Qualifikationen im Hinblick auf das Gewicht drohender Schäden oder begangener Straftaten enthalten, um den grundrechtlichen Anforderungen zu genügen. Die

²⁸ BVerfGE 130, 151 (205 f.).

²⁹ Vgl. zu weitaus eingriffsintensiveren Überwachungsmaßnahmen BVerfGE 141, 220 (269 ff.).

¹⁴ vorgesehene Zugriffsermächtigung enthält hingegen keine besondere tatsächliche Eingriffsschwelle, sondern verweist lediglich auf die Zentralstellenaufgabe und das allgemeine datenschutzrechtliche Erforderlichkeitsgebot. Auch hinsichtlich der zu schützenden Rechtsgüter oder der zu verfolgenden Straftaten fehlt es an qualifizierenden Anforderungen. Dies gilt auch dann, wenn § 10 Abs. 1 Satz 2 BKAG-E im Zusammenhang mit der Aufgabenzuweisung in § 2 Abs. 1, Abs. 2 Nr. 1 BKAG gelesen wird, da der dort verwandte Begriff der „Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung“ wenig restriktiv gefasst ist.

Regelungstechnisch könnte § 10 Abs. 1 Satz 2 BKAG-E verfassungskonform gefasst werden, indem die Abfragebefugnis an das Erfordernis einer konkreten Gefahr oder eines Tatverdachts gebunden wird. Der Sinn der Ermächtigung läge dann vor allem darin, Krisensituationen aufzulösen oder Verdachtsmomenten nachzugehen, auf die das Bundeskriminalamt im Rahmen seiner Auswertungstätigkeit stößt. Eine Nutzung der Bestandsdatenabfrage für kriminalstrategische Analysen im Vorfeld konkreter präventivpolizeilicher oder strafprozessualer Verfahren – also im Rahmen der „Intelligence-Arbeit“ des Bundeskriminalamts – scheidet hingegen aus.

Sollen dem Bundeskriminalamt hingegen Bestandsdatenabfragen gerade auch für kriminalstrategische Auswertungszwecke ermöglicht werden, müsste eine Vorfeldermächtigung geschaffen werden, deren Anwendungsbereich durch geeignete tatbestandliche Einengungen zu begrenzen wäre. Zudem müsste auch § 15 Abs. 2 Satz 1 TMG-E so angepasst werden, dass Datenübermittlungen im Gefahrvorfeld ermöglicht werden.

Schließlich verletzt § 15a Abs. 4 Satz 1 TMG-E teilweise die Kompetenzordnung. Diese Vorschrift sieht eine Übermittlungspflicht der Telemedienanbieter auch insoweit vor, als für die zugehörigen Zugriffsermächtigungen eine Gesetzgebungskompetenz der Länder besteht. Die Regelungsbefugnis für eine solche Übermittlungspflicht folgt jedoch der Regelungsbefugnis für die Abfrageermächtigung. Im Zusammenhang mit den bundesrechtlichen Zugriffsermächtigungen, die der Entwurf enthält, ist § 15a Abs. 4 Satz 1 TMG-E hingegen zwar kompetenzgemäß, aber redundant, da bereits diese Normen – systematisch korrekt – ausdrücklich eine Übermittlungspflicht begründen.³⁰ § 15a Abs. 4 Satz 1 TMG-E sollte daher ersatzlos gestrichen werden.

3. Übermittlung von und Zugriff auf Nutzungsdaten

Zu weit gefasst und darum verfassungswidrig ist die Übermittlungserlaubnis in § 15a Abs. 1 Satz 1, Abs. 2 Satz 1, Abs. 3 TMG-E hingegen insoweit, als sie eine Übermittlung auch von Nutzungsdaten erlaubt. Daten dieser Kategorie sind zumindest in der Regel deutlich sensibler als Bestandsdaten. Eine Übermittlung kann darum nicht generell durch die Zwecke der Verfolgung von (irgendwelchen) Straftaten oder gar Ordnungswidrigkeiten, der Gefahrenabwehr sowie der Wahrnehmung nachrichtendienstlicher Aufgaben legitimiert werden. Vielmehr bedarf es einer materiell qualifizierten Eingriffsschwelle. Diese Eingriffsschwelle muss aufgrund der grund-

³⁰ Vgl. § 100j Abs. 5 StPO-E; § 10 Abs. 5 Satz 2 BKAG-E.

¹⁵ rechtlichen Regelungsverantwortung des Bundes zumindest insoweit zwingend im Telemedienrecht enthalten sein, als es um eine Übermittlung an Landessicherheitsbehörden geht. Diesem verfassungsrechtlichen Erfordernis wird der Entwurf nicht gerecht.

Verfassungsrechtlich problematisch ist darüber hinaus die vorgesehene strafprozessuale Zugriffsermächtigung in § 100g Abs. 1 Satz 2 StPO-E. Die geplante Norm verweist hinsichtlich der Eingriffsschwelle auf die Ermächtigung zum Zugriff auf Telekommunikations-Verkehrsdaten in § 100g Abs. 1 Satz 1 StPO-E. Danach ist der Datenzugriff zulässig zur Verfolgung von Straftaten von erheblicher Bedeutung³¹ sowie von Straftaten, die mittels Telekommunikation begangen wurden. Ob diese recht offen gefasste Ermächtigung der Sensibilität von Telekommunikations-Verkehrsdaten vollauf gerecht wird, ist durchaus zweifelhaft, mag hier aber dahinstehen.³² Beim Zugriff auf Telemedien-Nutzungsdaten verschärfen sich die Zweifel jedenfalls noch, da diese Datenkategorie schwierig abzugrenzen ist und potenziell ein extrem weites Spektrum an Datenarten umfasst, deren Aussagekraft über Telekommunikations-Verkehrsdaten noch deutlich hinausgehen kann. Angesichts dessen halte ich den Regelungsansatz von § 100g Abs. 1 Satz 2 StPO-E, den Zugriff auf Verkehrs- und Nutzungsdaten unter denselben Voraussetzungen zu ermöglichen, allenfalls dann für verfassungsrechtlich vertretbar, wenn Inhaltsdaten als eigenständige weitere Kategorie von Telemediendaten anerkannt werden und diese Kategorie so zugeschnitten wird, dass sie die besonders sensiblen Datentypen umfasst.

4. Inhaltsüberwachung von Telemedien

Sowohl wegen der Interpretationsprobleme im Zusammenhang mit dem Begriff der Nutzungsdaten als auch aus Gründen der Rechtssicherheit ist es misslich, dass der Entwurf keine Regelung über die Überwachung von Telemedieninhalten vorsieht. Dem liegt anscheinend die Erwägung zugrunde, solche Überwachungen könnten auf § 100a StPO gestützt werden, da der dort verwendete Begriff der Telekommunikation auch die Kommunikation mittels Telemedien umfasse.³³ Ob diese Erwägung überzeugt, mag auf sich beruhen. Es ist jedenfalls nicht ratsam, sich bei der Überarbeitung der strafprozessualen Eingriffsermächtigungen an ihr zu orientieren.

Es trifft zwar zu, dass der sicherheitsbehördliche Zugriff auf Inhalte von Telemedien bislang – soweit sie nicht offen zugänglich sind und darum durch eine verdeckte Überwachung beschafft werden müssen – üblicherweise auf § 100a StPO gestützt wird. Dies gilt insbesondere für die Inhaltsüberwachung von Over-the-Top-Diensten, die (primär) der Individualkommunikation dienen.³⁴ Die Einstufung solcher Dienste als Telekommunikation im Sinne von § 100a StPO bedarf jedoch möglicherweise der Revision.

³¹ Der Straftatenkatalog des § 100a Abs. 2 StPO wird lediglich beispielhaft in Bezug genommen.

³² Diese Frage zu der – allerdings noch weiter gefassten – Vorgängerregelung in § 12 FAG a.F. offenlassend BVerfGE 107, 299 (315 f.), vgl. auch ebd., S. 322.

³³ Vgl. BT-Drs. 19/17741, S. 36.

³⁴ Vgl. beispielhaft zu der (im Beschluss nicht problematisierten) Überwachung eines E-Mail-Accounts auf der Grundlage von § 100a StPO BGH, Beschluss vom 11. August 2016 – StB 12/16; ferner BVerfG, Beschluss der 3. Kammer des Zweiten Senats vom 20. Dezember 2018 – 2 BvR 2377/16.

¹⁶ Nach der Rechtsprechung des Bundesgerichtshofs deckt sich der Telekommunikationsbegriff des § 100a StPO mit dem telekommunikationsrechtlichen Telekommunikationsbegriff.³⁵ Aufgrund des Urteils des Gerichtshofs der Europäischen Union zu E-Mail-Diensten steht nunmehr jedoch verbindlich fest, dass Over-the-Top-Dienste zumindest in der Regel gerade keine Telekommunikationsdienste im Sinne des Telekommunikationsrechts sind. Wird die bisherige Rechtsprechung des Bundesgerichtshofs zugrunde gelegt, verengt sich reflexartig auch der strafprozessuale Telekommunikationsbegriff. Die Inhaltsüberwachung von Telemedien kann dann nicht mehr auf § 100a StPO gestützt werden.

In der juristischen Literatur wird allerdings vertreten, der Telekommunikationsbegriff des § 100a StPO sei nicht an dem technisch ansetzenden telekommunikationsrechtlichen Telekommunikationsbegriff, sondern an dem – teils engeren, teils weiterreichenden – Fernmeldegeheimnis des Art. 10 GG zu orientieren.³⁶ Da zugleich aufgrund ausdrücklicher Verweise auf das Telekommunikationsgesetz unstreitig ist, dass der Telekommunikationsbegriff in den Ermächtigungen zur Erhebung von Bestands- und Verkehrsdaten (§ 100g und § 100j StPO) dem telekommunikationsrechtlichen Telekommunikationsbegriff entspricht, hat diese Auffassung zur Folge, dass der Begriff der Telekommunikation in unterschiedlichen strafprozessualen Eingriffsermächtigungen unterschiedlich zu verstehen ist. Hiervon geht auch die Entwurfsbegründung erkennbar aus.

Eine Stellungnahme zu dieser Kontroverse ist hier entbehrlich. In jedem Fall sollte aus Gründen der Rechtssicherheit die Inhaltsüberwachung von Telemedien ausdrücklich in § 100a StPO aufgenommen werden. Hierdurch würde eine ansonsten drohende Begriffsverwirrung vermieden. Zudem wäre klargestellt, dass es für Telemedien neben Bestands- und Nutzungsdaten eine weitere Datenkategorie gibt, deren Erhebung besonders strengen Anforderungen genügen muss. Vor allem aber hat die in der Entwurfsbegründung verfochtene Position missliche Konsequenzen für die Praktikabilität einer Inhaltsüberwachung von Telemedien. Eine solche Überwachung wird oftmals auf eine Mitwirkung des Telemedienanbieters angewiesen sein. Es gibt jedoch keine Vorschrift, die eine solche Mitwirkung eindeutig anordnet. § 100a Abs. 4 StPO verpflichtet zur Mitwirkung an Telekommunikationsüberwachungen die Anbieter von Telekommunikationsdiensten (vgl. zu diesem Begriff § 3 Nr. 24 TKG) und verweist wegen der Reichweite ihrer Mitwirkungspflicht teilweise auf das Telekommunikationsgesetz und die Telekommunikations-Überwachungsverordnung. Damit wird ausdrücklich auf das Telekommunikationsrecht Bezug genommen, dem die Anbieter von Telemediendiensten gerade nicht unterfallen.³⁷ Hieraus resultiert

³⁵ BGH, Urteil vom 14. März 2003 – 2 StR 341/02 –, NJW 2003, S. 2034; Beschluss vom 31. Januar 2007 – StB 18/06, NJW 2007, S. 930 (931 f.).

³⁶ Vgl. zur Diskussion Graf, in: BeckOK StPO, § 100a Rn. 18 ff.; Günther, in: MüKo StPO, 2014, § 100a Rn. 26 ff.

³⁷ Das Bundesverfassungsgericht hat zwar erst in jüngerer Zeit keine verfassungsrechtlichen Bedenken dagegen erhoben, dass einem E-Mail-Anbieter nach § 110 TKG Mitwirkungspflichten auferlegt wurden, vgl. BVerfG, Beschluss der 3. Kammer des Zweiten Senats vom 20. Dezember 2018 – 2 BvR 2377/16 –, NJW 2019, S. 584. Die diesem Beschluss zugrunde liegenden fachgerichtlichen Entscheidungen sind jedoch aufgrund des später ergangenen Urteils des EuGH zur Einstufung von E-Mail-Diensten obsolet. Eine Anwendung von § 110 TKG auf E-Mail-Anbieter ist heute meiner Ansicht nach unabhängig von den verfassungsrechtlichen Maßstäben einfachrechtlich nicht mehr vertretbar.

¹⁷ erhebliche Rechtsunsicherheit, die den Anbietern von Telemediendiensten nicht zumutbar ist und – sofern diese eine Mitwirkung wegen des Wortlauts von § 100a Abs. 4 StPO (meines Erachtens zu Recht) verweigern – die Tätigkeit der Strafverfolgungsbehörden erheblich behindern könnte.

Über die angezeigte Ergänzung von § 100a StPO um die Telemedien-Inhaltsüberwachung hinaus sollte zudem erwogen werden, nach dem Vorbild des Telekommunikationsrechts spezifische technische Vorgaben zu schaffen, um eine wirksame Überwachung zu ermöglichen.³⁸

5. Übermittlung von und Zugriff auf Zugangsdaten

Die auf Telemedien-Zugangsdaten bezogenen Regelungen des Entwurfs sind systematisch nicht schlüssig gestaltet, worauf bereits der Bundesrat hingewiesen hat.³⁹ § 15b Abs. 2 Satz 1 TMG-E errichtet sehr hohe Anforderungen an die Übermittlung solcher Daten, die sich jedoch in der vorgesehenen Zugriffsermächtigung in § 100j Abs. 1 Satz 2 StPO-E nicht wiederfinden. Im Bild der Doppeltür stellt der Entwurf eine Gartenpforte neben ein Scheunentor. Dieser Mangel an Konsistenz ist nicht lediglich ein normästhetisches Problem, sondern begründet erhebliche Anwendungsprobleme. So wird das Gericht, das den Datenzugriff erlaubt (§ 100j Abs. 3 StPO), naheliegenderweise nur prüfen, ob die Voraussetzungen der weit gefassten strafprozessualen Zugriffsermächtigung vorliegen. Der Telemedienanbieter wird dann mit einem gerichtlichen Beschluss konfrontiert, den er zu erfüllen hat, obwohl die Voraussetzungen der für ihn geltenden Übermittlungserlaubnis nicht vorliegen. Die beiden Regelungen sollten daher aufeinander abgestimmt werden.

Damit ist allerdings noch nicht gesagt, wie hoch die einheitliche gesetzliche Eingriffsschwelle angesetzt werden sollte. Im Entwurf finden sich hierzu zwei unterschiedliche Ansätze. § 15b Abs. 2 Satz 1 TMG-E bindet die Datenübermittlung an starre Voraussetzungen, die sich an den verfassungsrechtlichen Anforderungen an Online-Durchsuchungen orientieren.⁴⁰ Hingegen macht § 100j Abs. 1 Satz 2 StPO-E den Datenzugriff davon abhängig, dass die Voraussetzungen für eine strafprozessuale Nutzung der übermittelten Daten vorliegen.

Der starre Ansatz des § 15b Abs. 2 Satz 1 TMG-E ist klar vorzugswürdig. Nur er schafft Rechtsicherheit und gewährleistet zuverlässig, dass der Datenzugriff den verfassungsrechtlichen Anforderungen genügt. Die in § 15b Abs. 2 Satz 1 TMG-E vorgesehene Eingriffsschwelle ist allerdings sehr hoch angesetzt. Dies ergibt dann Sinn, wenn eine Erhebung von Telemedien-Zugangsdaten aus sicherheitsbehördlicher Sicht faktisch nur in Betracht kommt, wenn mit Hilfe der Zugangsdaten die Nutzung eines komplexen Telemediums über einen längeren Zeitraum beobachtet werden soll, so dass die Überwachung als Online-Durchsuchung einzustufen ist. Sollten hingegen auch punktuellere Datennutzungen praktisch bedeutsam sein (etwa die einmalige ge-

³⁸ Sehr unspezifisch sind hingegen die – auf Inhaltsdaten auch nicht anwendbaren – § 15a Abs. 5 und § 15b Abs. 4 TMG-E formuliert.

³⁹ BT-Drs. 19/18470, S. 30.

⁴⁰ BT-Drs. 19/17741, S. 39.

18 zielte Suche nach bestimmten Dateien), so könnte auch überlegt werden, statt einer einheitlichen Zugriffsschwelle den Zugriff auf Zugangsdaten als Annexmaßnahme in den jeweiligen Überwachungsermächtigungen (also etwa in den Ermächtigungen zu Online-Durchsuchungen oder zu Telekommunikationsüberwachungen) mitzuregeln und die Übermittlungserlaubnis entsprechend differenziert zu gestalten.

In diesem Zusammenhang seien zwei Anmerkungen gestattet, die sich nicht unmittelbar auf den geregelten Datenzugriff beziehen, sondern auf vor- und nachgelagerte Fragen:

Erstens erscheint mir zwingend geboten, dass der Zugriff auf Zugangsdaten immer nur in der Form erfolgen kann und darf, in der diese Daten bei den Telemedienanbietern aufgrund einer technisch-organisatorisch ordnungsgemäßen Datenhaltung vorliegen. Da insbesondere die Telemedienanbieter aus Gründen der IT-Sicherheit Zugangsdaten nicht im Klartext oder in einer für sie entschlüsselbaren Form speichern dürfen, können sie lediglich Daten herausgeben (sog. Hashwerte), auf deren Grundlage die Sicherheitsbehörden – gegebenenfalls mit erheblichem Aufwand – die eigentlichen Zugangsdaten (etwa Passwörter) zu ermitteln versuchen können. Eine denkbare Pflicht der Telemedienanbieter, Zugangsdaten im Klartext für sicherheitsbehördliche Zugriffe zu bevorraten, stünde weder mit Art. 32 DSGVO noch mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in seiner objektiv-rechtlichen Dimension in Einklang.

Zweitens bedarf es für die Nutzung der erlangten Zugangsdaten jeweils besonderer Rechtsgrundlagen, die sich im Entwurf nicht finden. Insbesondere ermöglicht das geltende Strafprozessrecht mangels ausdrücklicher Ermächtigung keine Nutzung mit dem Ziel, ein Konto auf einem Telemedium (beispielsweise einem Sozialen Netzwerk) zu übernehmen, um aktiv an Kommunikationsvorgängen mit Dritten teilzunehmen oder solche Kommunikationsvorgänge gar zu initiieren. Die bestehenden Ermächtigungen zu Online-Durchsuchungen und Telekommunikationsüberwachungen ermöglichen lediglich eine passive Beobachtung solcher Kommunikationsvorgänge.

Schließlich verletzt § 15b Abs. 3 Satz 1 TMG-E teils die Kompetenzordnung und ist teils überflüssig. Insoweit gilt das oben unter II.2. zu § 15a Abs. 4 Satz 1 TMG-E Ausgeführte entsprechend.

6. Zitiergebot

Die Zitierung von Art. 10 GG in Art. 7 des Entwurfs bezieht sich lediglich auf Vorschriften, die eine Zuordnung von dynamischen IP-Adressen vorsehen.⁴¹ Auch der Vorschlag des Bundesrats zur Nennung weiterer Vorschriften beruht allein auf diesem Kriterium.⁴² Dieses Kriterium greift jedoch zu kurz und erfasst nicht alle Eingriffe in das Fernmeldegeheimnis, die der Entwurf ermöglicht.

⁴¹ BT-Drs. 19/17741, S. 46.

⁴² BT-Drs. 19/18470, S.30

¹⁹ Das Fernmeldegeheimnis ist als eingeschränktes Grundrecht für alle Regelungen zu zitieren, die einen Eingriff in dieses Grundrecht ermöglichen. Der Schutzbereich von Art. 10 GG reicht teils weiter als der Telekommunikationsbegriff des Telekommunikationsrechts. Er umfasst prinzipiell alle mit der Fernmeldetechnik ausgetauschten Informationen. Dementsprechend hat das Bundesverfassungsgericht bereits mehrfach ausgeführt, dass der Schutz dieses Grundrechts sich auf E-Mails erstreckt,⁴³ die einfachrechtlich als Telemedien- und nicht als Telekommunikationsdienste anzusehen sind. Da zudem das Fernmeldegeheimnis sowohl die Inhalte als auch die Umstände der grundrechtlich geschützten Kommunikation umfasst, kann insbesondere die Erhebung von Telemedien-Nutzungsdaten in Art. 10 GG eingreifen. In Art. 7 muss darum auch noch § 100g StPO-E (Art. 2 Nr. 2) aufgeführt werden.

⁴³ BVerfGE 113, 348 (383); 120, 274 (307); 124, 43 (54); 125, 260 (310 f.).

HateAid gGmbH

Stellungnahme

zum Entwurf des
Gesetzes zur Bekämpfung des Rechtsextremismus und der
Hasskriminalität
(Drs. 19/17741)



Inhalt

A.	Einleitung	3
B.	Meldung von Inhalten an das BKA.....	4
1.	Meldepflicht, § 3a NetzDG	4
2.	Änderung des Bundeskriminalamtgesetzes (BKAG)	6
a)	Meldungen ohne Anfangsverdacht.....	6
b)	Folgeproblem: (un)verhältnismäßige Datenverarbeitung.....	7
3.	Lösungsvorschlag: Quick Freeze	8
c)	Betreiberhaftung	9
d)	Beauskunftung von Bestands- und Nutzungsdaten.....	10
e)	§ 15 b TMG n.F.	13
f)	§ 51 Bundesmeldegesetz n.F.....	13
g)	Sonstige Änderungen und Reformvorschläge	14
1.	Änderung des Strafgesetzbuchs	15
2.	Änderung des Netzwerkdurchsetzungsgesetzes (NetzDG)	19

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 vorrangig 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 Meinungs Austausch 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.pdf>https://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 sein². 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.

²Facebook: 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 Rechnung³. 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.

³Facebook: 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 Auskunftersuchen 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 Verbessierung der Rechtsdurchsetzung insgesamt - losgelöst von den Katalogstraftaten wie §§ 86a, 130 StGB, welche die Meldepflicht betreffen - dringend erforderlich. Die Rechtsdurchsetzung scheitert häufig daran, dass den Auskunftersuchen 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 Officialdelikte 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 Zugangs Providern 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 Auskunftersuche 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

⁴J.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).

⁵Erhardt, 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 Lübke⁶ 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.

⁶Der 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 friedienstörende 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 Officialdelikte 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 Studien⁸, aber auch die Zahlen des BKA⁹ 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.

⁷Institut 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).

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

⁹BKA: 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

¹⁰ARD-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 Gemeindebundes¹¹ 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 Diensteanbietern 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.

Deutscher Städtetag · Gereonstraße 18 - 32 · 50670 Köln

An den
Vorsitzenden des Ausschusses für Recht- und Verbraucherschutz
des Deutschen Bundestages
Herrn Prof. Dr. Heribert Hirte
Platz der Republik 1
11011 Berlin

Per E-Mail:
rechtsausschuss@bundestag.de
Kathrin.schreiber@bundestag.de

Öffentliche Anhörung am 06. Mai 2020

a. Gesetzentwurf der Fraktionen der CDU/CSU und SPD

Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (BT-Drucksache 19/17741)

b. Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (BT-Drucksache 19/18470)

Ihr Schreiben vom 23. April 2020 / Ihr Geschäftszeichen: PA 6-5410-2.2

hier: Stellungnahme

Sehr geehrter Herr Vorsitzender,
Sehr geehrte Damen und Herren,

wir danken Ihnen für die Übersendung des Entwurfs eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität nebst Vorblatt und Begründung und nehmen hierzu wie folgt Stellung:

Wir begrüßen die Zielsetzung des Gesetzentwurfes, mit der erkannte Strafbarkeitslücken geschlossen und die effektive Strafverfolgung der dort aufgeführten Taten verbessert sowie der Eindruck eines rechtsfreien Raums im Internet weiter zurückgedrängt werden sollen. Gerade in der Öffentlichkeit stehende Personen, wie Politikerinnen und Politiker, aber auch Menschen, die sich für das Gemeinwesen einsetzen oder als Teil der öffentlichen Verwaltung den Staat repräsentieren, stehen immer wieder und mit zunehmender Tendenz im Fokus von Beleidigungen, Bedrohungen, Einschüchterungen oder sogar tätlichen Angriffen. Insoweit wird mit dem Gesetzentwurf und seinen

04.05.2020/mq

Kontakt
Gereonstraße 18 - 32
50670 Köln
Telefon 0221 3771-0
Telefax 0221 3771-0

Aktenzeichen
32.15.08 D

Hausvogteiplatz 1
10117 Berlin
Telefon 030 37711-0
Telefax 030 37711-999

Avenue des Nerviens 9 - 31
1040 Bruxelles
Belgien
Telefon +32 2 74016-20
Telefax +32 2 74016-21

www.staedtetag.de

Ergänzungen, vornehmlich den Regelungen des Strafgesetzbuches, ein wichtiges Zeichen gesetzt und gleichsam die Wehrhaftigkeit des Staates gegen derartige Taten im virtuellen Raum und in der realen Welt dokumentiert.

Besonders begrüßen möchten wir den vorgesehenen verbesserten Schutz von Kommunalpolitikerinnen und Kommunalpolitikern durch die Änderung des § 188 StGB (üble Nachrede und Verleumdung gegen Personen des politischen Lebens). Kommunalpolitisch agierende Personen stehen in der öffentlichen Auseinandersetzung besonderes im Fokus der Aufmerksamkeit. Deshalb ist es erforderlich, diese – genau wie Landes- oder Bundespolitikerinnen und -politiker – besonders gegen üble Nachrede und Verleumdung in den Schutzbereich des § 188 StGB einzubeziehen. Der Einsatz für unsere demokratischen Strukturen muss besonders geschützt werden, bis hin zur kommunalen Ebene.

Auch die Erweiterung des Tatbestandes des § 241 StGB (Bedrohung) insoweit, dass künftig auch die Bedrohung mit einer rechtswidrigen Tat gegen die sexuelle Selbstbestimmung, die körperliche Unversehrtheit, die persönliche Freiheit oder gegen eine Sache von bedeutendem Wert vom Tatbestand erfasst ist, ist sehr zu begrüßen. Diese Erweiterung stellt eine erhebliche Verbesserung insbesondere auch für kommunale Bedienstete dar, weil bisher nur die Drohung mit der Begehung eines Verbrechens tatbestandsmäßig war. Damit konnte beispielsweise die Drohung einer Körperverletzung (Vergehen), die gegenüber kommunalen Bediensteten häufig erfolgt, nicht als Bedrohung im Sinne des Gesetzes strafrechtlich geahndet werden. Gleichzeitig ist eine Verschärfung der Rechtsfolgen dergestalt vorgesehen, dass künftig die Höchststrafe für die Bedrohung mit einem Verbrechen von einem Jahr auf zwei Jahre Freiheitsstrafe angehoben werden kann.

Angesichts der vermehrt aufkommenden Angriffe in den Notaufnahmen ist die Ergänzung des § 115 StGB folgerichtig. Wir regen darüber hinaus an zu prüfen, ob nicht der strafrechtliche Schutz von Behördenmitarbeiterinnen und -mitarbeitern auch ohne Vollstreckungsaufgaben generell verbessert werden kann, z.B. durch die Aufhebung der Beschränkung in § 114 StGB auf Vollstreckungsbeamte. Auch Beschäftigte im öffentlichen Dienst ohne Vollstreckungsaufgaben arbeiten für das Gemeinwohl, die zunehmenden Angriffe aus sie dürfen nicht toleriert werden.

Schließlich halten wir die Ausweitung des § 140 StGB (Belohnung und Billigung von Straftaten) auf die Billigung noch nicht erfolgter Straftaten für eine wichtige Änderung, da das Aufgreifen und Befürworten von strafbaren Inhalten in sozialen Netzwerken zahlreich vorkommt und dies neben der Verbreitung dieser Inhalte letztlich auch zu einer fortschreitenden Akzeptanz solcher Äußerungen in der Bevölkerung führt. Allerdings lässt der Gesetzentwurf offen, in welcher Form diese Billigung erfolgen muss. Ist also ein einfaches "Teilen" des Inhalts bereits ein ausreichendes "Gutheißen" oder eine "Kundgabe der Zustimmung" (S. 33 der Begründung) oder muss damit eine weitere Befürwortung des weitergeleiteten Inhalts einhergehen? Eine Konkretisierung wäre aus Gründen der Rechtsklarheit und mit Blick auf die praktische Anwendbarkeit sinnvoll und wünschenswert.

Es ist im Übrigen zu befürworten, dass der Katalog der Strafzumessungsgründe in § 46 StGB ausdrücklich um "antisemitische" Beweggründe ergänzt wird. Auch wenn nach der bereits geltenden Rechtslage antisemitische Beweggründe unter die Formulierung "sonstige menschenverachtende" Beweggründe subsumiert und insoweit bei der Strafzumessung grundsätzlich strafscharfend zu berücksichtigen waren, dient die vorgesehene Ergänzung der Klarstellung. Antisemitische Motive eines Täters oder einer Täterin werden ausdrücklich als weitere Beispiele für menschenverachtende Beweggründe und Ziele genannt und werden bei der Strafzumessung besonders berücksichtigt.

Wir begrüßen grundsätzlich die Änderung des § 51 Abs. 1 Bundesmelderegistergesetz (BMG). Durch diese Änderung wird es insbesondere Personen, die durch ihr berufliches oder ehrenamtliches Engagement in den Fokus gewaltbereiter Personen oder Gruppen geraten sind, erleichtert, eine Auskunftssperre zu

erwirken. Diese Auskunftssperre nach § 51 BMG verhindert die Erteilung einer einfachen Melderegisterauskunft, wenn dadurch eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnlich schutzwürdige Interessen für die nachgefragte Person erwachsen würde. Notwendig für die Einrichtung einer Auskunftssperre ist daher der Nachweis der individuellen und konkreten Gefährdung einer Person. Auf eine subjektive Einschätzung der Person, ob sie zu einem Personenkreis gehört, der sich besonderen Anfeindungen ausgesetzt sieht, kann es dabei nicht ankommen. Möglicherweise wäre es klarer, wenn stattdessen formuliert würde, dass der Personenkreis in verstärktem Maße Anfeindungen oder sonstigen Angriffen ausgesetzt ist.

Der Gesetzentwurf sorgt für einen wesentlich verbesserten Schutz der Betroffenen. Er deckt sich auch überwiegend mit den Erwartungen und Forderungen der Beschlussgremien des Deutschen Städtetages.

Weitergehende Erfordernisse

Gleichwohl ist darauf hinzuweisen, dass die beabsichtigten Änderungen im Strafgesetzbuch für sich allein als Mittel der Bekämpfung von Rechtsextremismus und Hasskriminalität nicht ausreichend sind. Eine effiziente Strafverfolgung kann nur im Rahmen von damit einhergehenden personell und technisch hinreichend ausgestatteten Strafverfolgungsbehörden gewährleistet werden. Angesichts der in der Bundesrepublik seit Jahren personell überlasteten Polizei- und Justizbehörden darf dieser Gesichtspunkt ungeachtet der Zuständigkeiten der Länder nicht vergessen werden. Zudem ist eine konsequente Verfolgung der Straftaten durch die Staatsanwaltschaften dringend geboten. Schwerpunktstaatsanwaltschaften, wie sie in einigen Bundesländern eingerichtet worden sind, können hier helfen. Ebenso sind Richtlinien hilfreich, in denen die Einstellung von Ermittlungsverfahren wegen Geringfügigkeit bei Attacken und Übergriffen gegen Amtsträger, Rettungssanitäter, Polizisten und Hilfeleistende an weitere Kriterien geknüpft wird. Das öffentliche Interesse an Strafverfolgung sollte unabhängig von der Qualifikation einer Straftat als Vergehen gerade bei Straftaten gegen öffentliche Bedienstete und Amts- und Mandatsträgerinnen und -träger nicht verneint werden.

Schließlich regen wir an, in § 46 Abs. 2 StGB bezüglich der Strafzumessungsgründe eine Erweiterung um "frauenverachtende" Beweggründe vorzunehmen. Rechtsextremismus und Hasskriminalität haben auch eine besondere Genderrelevanz.

Wir wären Ihnen dankbar, wenn Sie unsere Hinweise im weiteren Verfahrensgang berücksichtigen könnten.

Referentenentwurf eines Gesetzes zur Bekämpfung der Hasskriminalität und des Rechtsextremismus

Die mit dem Gesetzesentwurf verfolgten Ziele kann man nur begrüßen. Die hierzu angedachten Mittel und die legislative Umsetzung sind jedoch durchgreifenden Einwänden ausgesetzt.

Die Inanspruchnahme der privaten Diensteanbieter als meldepflichtige Vorposten der Strafverfolgung durch das BKA begegnet ebenso Bedenken und ist im Ergebnis abzulehnen wie die tatbestandliche Ausweitung von Strafbarkeiten, etwa bei Bedrohungen iSv § 241 StGB, bzw. der Anhebung von Strafrahmen, zumal die Hoffnung mit letzteren Sozialverhalten steuern zu können nach allen kriminologischen Erkenntnissen der Tatsachenbasis entbehrt.

1. Zur Meldepflicht für Diensteanbieter nach dem NetzDG

a)

Die vorgesehene Novelle des NetzDG sieht in § 3a Abs. 2 Nr. 1 NetzDG-E eine Mitteilungspflicht an das BKA in Fällen vor, in denen der Anbieter aufgrund von Beschwerden mit Löschung oder Sperren reagiert und bei denen konkrete Anhaltspunkte bestehen, dass sie strafrechtlich relevante Inhalte im Sinne eines in § 3a Abs. 2 Nr. 3c NetzDG-E enthaltenen Deliktskatalogs enthalten.

Die Übermittlung an das BKA ist dem Nutzer erst nach 2 Wochen zu melden, sofern das BKA diese Mitteilung nicht zum Schutze des Ermittlungszwecks untersagt.

Zur Gewährleistung eines funktionierenden Ablaufs hat gem. § 3a Abs. 1 der Anbieter eines sozialen Netzwerks Ressourcen für ein wirksames Verfahren vorzuhalten.

b)

Dem Vorschlag ist entgegenzutreten:

aa)

Erfasst sind gemäß § 1 Abs .2 NetzDG-E nur Kommunikationsplattformen, die mindestens 2 Millionen Nutzer haben. Zu besorgen ist mithin, dass gerade diejenigen, denen der Sinn nach Austausch strafrechtlich relevanter Äußerungen steht, sich schlicht auf kleinere, indes immer noch nicht unbedeutende Plattformen mit Nutzern unter 2 Millionen zurückziehen, die den vorgeschlagenen Regelungen gerade nicht unterliegen. Gegebenenfalls machen es sich einschlägige Plattformen sogar zur Regel ihre Teilnehmer unterhalb der gesetzlichen Schwelle zu halten und zum Schaden der Demokratie die Legende zu pflegen, dass allein auf ihrer Ebene die Rede noch „frei“ sei.

bb)

Die vorgesehene Meldepflicht macht private Unternehmen darüber hinaus gleichsam zu Subsumtionswächtern komplizierter strafrechtlicher Tatbestände. Barg das NetzDG schon bisher die Gefahr des sogenannten Overblockings durch „zuviel“ gelöschte Beiträge seitens der verpflichteten Unternehmen, die hierdurch präventiv Haftungsrisiken von bis zu 5 Millionen € zu vermeiden trachten, potenziert sich diese Gefahr durch die vorgesehene Meldepflicht mit weitreichenden Folgen:

Das BKA bekommt neben den beanstandeten Äußerungen die digitalen Adressdaten zur Identifizierung/Verifizierung des Nutzers, und zwar auch dann, wenn sich der Inhalt bei näherer Betrachtung als nicht strafbar erweist. Mit Fug zu befürchten ist, dass hierdurch eine Datenbank beim BKA über Äußerungen entsteht, die ggf. bedenklich, aber nicht strafbar sein mögen. Diese Sorge wird eine unter Nutzern verbreitete sein und diese ggf. auch zur

Selbstzensur nicht strafbarer Äußerungen veranlassen, um nicht in den Fokus von Meldungen an das BKA zu geraten. Der Meinungsfreiheit, die zu schützen der Entwurf sich anschickt, wäre damit kein Gefallen getan.

c)

Nach dem Entwurf ist zudem neben den IP-Adressen dem BKA durch die Betreiber auch die jeweilige Portnummer mitzuteilen. Der Entwurf formuliert zwar in § 3a Abs. 4 Nr. 2 NetzDG, dass dies nur „sofern vorhanden“ gelte. Es steht aber zu besorgen, dass die Plattformen im Rahmen ihrer Compliancebemühungen zu weitreichenden Speicherungen bewegt werden (sollen) und zur Sicherung der Strafverfolgung insoweit ein erneuter Einstiegsversuch in die durch das OVG Münster gegenwärtig als europarechtswidrig verbannte Vorratsdatenspeicherung unternommen werden soll.

d)

Die flankierende Regelung des § 15a TMG-E, welche es künftig im Zusammenspiel mit § 10 BKAG-E gestatten soll, dass das BKA sich den Zugriff auf das Konto eines gemeldeten Nutzers verschafft, verstärkt die angesprochene Besorgnis. Denn § 15a TMG-E verpflichtet die Anbieter u. a. dem BKA auf dortiges Auskunftsverlangen selbst Passwörter und Zugangsdaten herauszugeben. Es liegt alles andere als fern, dass hier – ggf. auch unter der Prämisse der Gefahrenabwehr – der Nutzer auch jenseits beanstandeter Posts ausgeforscht werden soll und dass dieser Zugriff zudem heimlich stattfindet. Es wurden diesbezüglich schon Einwände hinsichtlich der IT-Sicherheit erhoben. Dass Passwörter unverschlüsselt gespeichert oder herausgegeben werden müssten, wurde zwar bislang dementiert. Die Herausgabepflicht für die Behörden nicht zu nutzender, weil verschlüsselter und auch nicht entschlüsselbarer Daten (sog. Hashs) entbehrt dann aber der Sinnhaftigkeit. Der Blick zurück auf die Genese der Gesetzgebung zur sog. Quellen-TKÜ legt es hingegen nahe, dass behördliche Begehrlichkeiten den Gesetzgeber alsbald veranlassen werden auch den Weg zum zweiten Schritt, nämlich zum Dechiffrierungszwang zu ebnen, nachdem der erste, nämlich ein behördlicher Anspruch auf Bestandsdaten normiert worden ist.

e)

Bedenklich ist weiterhin die gesetzlich vorgesehene Heimlichkeit der Ermittlungen:

Mag das Bundesverfassungsgericht bei umstrittenen Äußerungen im Zweifel auch grundrechtsschützend zugunsten der Meinungsfreiheit entscheiden,¹ droht diese Prämisse durch den in Rede stehenden Referentenentwurf, gerade auch durch die Einbindung Privater mit Haftungsrisiken, ausgehöhlt zu werden. Die Folgen sind wie gesagt gravierend. Denn anders als in der „analogen“ Welt schließt sich in der Logik der Novelle an eine – auch fehlerhaft so bewertete – inkriminierte Äußerung nicht etwa ein offenes Verfahren mit rechtlichem Gehör, um die Frage der Legitimität beanstandeten Inhalts an, sondern eher ein heimliches mit ggf. digitalen Durchsuchungen und Durchleuchtungen des Nutzers.

Die Regelungen sind von daher abzulehnen.

2. Ergänzung der Regelungen des StGB mit Bezug zur Hasskriminalität

a) Änderung des § 46 StGB

Der Referentenentwurf schlägt vor, neben festgestellten rassistischen, fremdenfeindlichen und sonst menschenverachtenden Motiven künftig auch antisemitische in die enumerative Aufzählung strafmaßbestimmender Tätermotive aufzunehmen. Der Vorschlag verwundert, da antisemitische Motive sich zwanglos bereits unter die bereits in § 46 StGB benannten menschenverachtenden subsumieren lassen. Eine zu schließende „Strafmaßlücke“ ist eigentlich nicht auszumachen.

Dies konzidiert auch die Begründung des Entwurfs, artikuliert jedoch ein überwiegendes Bedürfnis für auch rein symbolische Gesetzgebung

¹ Vgl. etwa instruktiv *Grimm* NJW 1999, 1697ff.

aufgrund der deutschen Verantwortung für die Shoa sowie angesichts der Zunahme antisemitisch geprägter Taten. So begrüßenswert die Intention des Entwurfs an dieser Stelle ist, steht doch zu besorgen, dass sie ihr Ziel mit der vorgeschlagenen Umsetzung in mehrerlei Hinsicht zu verfehlen droht:

aa)

Dies gilt zunächst systematisch. Die exemplarische Benennung antisemitischer Motive wird absehbar den Auftakt zu einem wachsenden Enumerativkatalog in § 46 StGB bilden. Denn auch andere gesellschaftliche Gruppen, deren Mitglieder aufgrund ihrer Zugehörigkeit Angriffen ausgesetzt sind, werden für diese perspektivisch das in der expliziten Benennung in § 46 StGB besondere Unwerturteil für solche Angriffe einfordern. Zu befürchten ist ein wachsender Katalog, der unbeabsichtigt dazu führen könnte, dass „Hatecrimes“ gegen dort nicht aufgeführte Gruppen analog dem Umgang mit unbenannten Regelbeispielen eher in den Hintergrund geraten, was der Intention der Entwurfsverfasser zuwiderlaufen dürfte. Diese Gefahr wird in der Entwurfsbegründung durchaus erkannt, dort jedoch schlicht durch die normative Behauptung negiert, die Herausnahme antisemitischer Motive aus den „sonst menschenverachtenden“ durch explizite Benennung bedeute keine strukturelle Änderung für § 46 Abs. 2 StGB.² Dies vermag nicht zu überzeugen.

bb)

Dass man dem berechtigten Anliegen des Entwurfs, antisemitisch motivierten Straftaten deutlich entgegenzutreten mit der expliziten Aufnahme des Begriffs der „antisemitischen Motive“ in § 46 StGB einen Gefallen tut, ist aber auch aus anderem Grund zu bezweifeln:

Der Versuch einer strafrechtlichen Definition von Antisemitismus in § 46 StGB-E wird unter dem Regime des im Strafrecht geltenden

² Entwurfsbegründung S. 17.

Bestimmtheitsgrundsatzes sowie den verfassungsrechtlichen Auslegungsgrundsätzen für die Pönalisierung von Äußerungen im Lichte des Art. 5 Abs. 1 GG bereits normativ einen sehr restriktiv ausgelegten Antisemitismusbegriff zeitigen. Hinzu kommt in der Praxis noch der in dubio pro reo Grundsatz auf der subjektiven Ebene.

Es steht demnach zu befürchten, dass ein aus jüdischer Sicht klar als solcher empfundener Antisemitismus, der beispielsweise getarnt als Israel- oder Zionismuskritik daherkommt,³ nach den restriktiven strafrechtlichen Auslegungsmaximen schwerlich zu erfassen sein wird. Absehbar sind Strafurteile, die im Korsett der strafrechtlichen Auslegungsprämissen von der jüdischen Bevölkerung als antisemitisch empfundene Motive nicht als solche iSd § 46 Abs. 2 StGB-E benennen (können).

Schlimmstenfalls und nicht einmal fernliegend könnte dies dazu führen, dass antisemitisch gesonnene Personen danach suchen, die Auseinandersetzung um die Grenzen des Antisemitismusbegriffs unter den für sie günstigen Beweis- und Auslegungsregeln des Straf- und Strafprozessrechts zu führen. Ein strafrechtlich notwendig restriktiver Antisemitismusbegriff könnte zudem in der politischen Diskussion als Referenz dafür missbraucht werden, dass von diesem nicht erfasste Äußerungen – vermeintlich auch gerichtlich anerkannt – nicht antisemitisch seien. Die Gefahr, dass der Vorschlag in der Praxis Ergebnisse zeitigt, die das Gegenteil von dem bedeuten, was der Referentenentwurf intendiert, ist nach alledem nicht von der Hand zu weisen.

b) Erweiterung des Straftatenkataloges des § 126 StGB

§ 126 StGB erweist sich bereits in seiner jetzigen Fassung als Straftatbestand, der „Unsicherheiten in der praktischen Anwendung“ auslöst und dem Einwand begegnet, eine Strafbarkeit von Äußerungen nach Maßgabe moralischer Entrüstung zu bestimmen.⁴ Das

³ Vgl. hierzu auch Beschluss des Bundestages BT.Drucks 19/444

⁴ Fischer, § 126 Rn. 10.

Bundesverfassungsgericht hat zudem „Bedenken“ hinsichtlich der Bestimmtheit des Tatbestandsmerkmals der Störung des öffentlichen Friedens in Tatbeständen angemeldet, die nicht wenigstens durch „andere Tatbestandsmerkmale grundsätzlich tragfähige und hinreichend begrenzte Konturen“ erhalten.⁵

Letzteres ist bei § 224 StGB nicht uneingeschränkt der Fall, wenn sich etwa die Frage der Drohung mit einer „lebensgefährdenden Behandlung“ oder einer gemeinschaftlich (mit Beihilfern) in Aussicht gestellten Aufsuche zu beurteilen ist.

Die Drohung und die Furcht des Bedrohten wird sich regelmäßig auf die Handlungsfolge, also den Taterfolg einer Körperverletzung beziehen, während § 224 StGB zuvörderst *Begehungsweisen*, die generell gefährlicher erscheinen pönalisiert, ohne dass sich diese im Verletzungserfolg niedergeschlagen haben müssen. Die Inkongruenz von Drohungen und den in § 224 StGB genannten Handlungsformen wird besonders deutlich durch die Tatbestandsvariante des § 224 Abs. 1 Nr. 4 StGB illuminiert. Denn in dieser müsste ein hinterlistiger Angriff angedroht werden. Die entsprechende Ankündigung eines solchen Angriffs nach § 126 StGB-E würde allerdings die Hinterlist in § 224 Abs. 1 Nr. 4 StGB ausschließen, weil sie eine auf Verdeckung der wahren Absicht berechnetes Vorgehen verlangt, um dem Gegner die Abwehr des nicht erwarteten Angriffs zu erschweren und eine Vorbereitung auf seine Verteidigung nach Möglichkeit auszuschließen.⁶

Weiterhin gilt, dass sich gerade mit Bezug auf das Internet, wo Menschen sich virtuell und häufig anonym und ohne Absicht, sich jemals real zu begegnen die Frage stellt, inwiefern in solchen, ggf. mehr oder minder geschlossenen Chatforen, der gestörte Friede als „öffentlicher“ im Sinne der Norm verstanden werden kann. Zu bedenken ist, ob nicht gleichsam

⁵ BVerfG 4.11.2009 – 1 BvR 2150/08, JZ 2010, 298 (304); zust. zur Eingrenzung des Schutzzwecks „öffentlicher Friede“ auch Hörnle JZ 2010, 310 (312)

⁶ BGH NSTZ-RR 2013, 173; BGH NSTZ-RR 2009, 77

zwischen „virtuellen“ und „analogen“ Frieden zu differenzieren ist, wobei ersterer sich durchaus auf letzteren auswirken kann, was dann aber für den Einzelfall auch festzustellen wäre. Da indes dem Tatbestandsmerkmal des öffentlichen Friedens wie ausgeführt in seiner jetzigen Interpretation durch die Rechtsprechung gegenwärtig keine tatbestandskonturierende Wirkung zukommt, wird die vorgeschlagene Weiterung zu erheblichen Unsicherheiten und ggfls. konturloser Ausweitung des Deliktsfeldes führen.

c) Gutheißen künftiger Straftaten in § 140 StGB-E

aa)

Der Tatbestand ist bereits in seiner jetzigen Fassung nicht ohne Grund Kritik ausgesetzt, was seine Bestimmtheit und potentielle Nähe zum Gesinnungsstrafrecht⁷ angeht. Das Tatbestandsmerkmal der „Billigung“ erfordert nach der Rechtsprechung entgegen der Annahme der Entwurfsbegründung auf S. 23 auch nicht notwendig eine explizite Kundgabe. Aufgrund seiner mit Blick auf die Rechtsgüter weitreichenden Vorverlagerung der Strafbarkeit gilt die Norm als zudem geeignet, die öffentliche Diskussion und Auseinandersetzung zu beeinträchtigen und erscheint nach Stimmen der Rechtswissenschaft in einer freiheitlich-liberalen Gesellschaft verzichtbar.⁸

Die Unschärfe und Weite des Tatbestands durch konkludentes Gutheißen, illustriert eine Entscheidung, in welcher der BGH die Einschlägigkeit der Norm bereits für den Verleger einer Autobiographie eines Straftäters angenommen hat.⁹ Durch das (vermeintliche) Gutheißen *künftiger* Delikte, würde sich das Problem tatbestandlicher Unbestimmtheit und Weite verschärft stellen.

bb)

⁷ Pointiert Kindhäuser/Neumann/Paeffgen-Ostendorf, § 140 Rz. 5

⁸ SSW-Jeßberger, § 140 Rz. 2

⁹ BGH NJW 1978, 58

Es bestehen darüber hinaus entgegen der Gesetzesbegründung (S. 23) keine tatsächlichen Strafbarkeitslücken, da der sozialschädliche Kern der Befürwortung von und der Anleitung zu Gewalttaten schon hinreichend von anderen Straftatbeständen erfasst wird (insbesondere von § 111 StGB – öffentliche Aufforderung zu Straftaten; § 126 StGB – Störung des öffentlichen Friedens durch Androhung von Straftaten; § 130 StGB – Volksverhetzung; § 131 StGB – Verherrlichung von Gewalt; § 140 StGB – Billigung von Straftaten; § 21 in Verbindung mit § 6 des Gesetzes über die Verbreitung jugendgefährdender Schriften, § 53 Abs. 1 Nr. 5 des Waffengesetzes). Dies hat der Gesetzgeber in früheren Legislaturperioden bereits zutreffend erkannt:¹⁰

So wurde § 88a a.F. StGB, der ebenfalls intendierte, das Gutheißen zukünftiger Straftaten unter Strafe zu stellen bereits fünf Jahre nach seiner Einführung 1976 wieder abgeschafft.

Zur Begründung hieß es damals, die Vorschrift sei praktisch obsolet (in den fünf Jahren gab es nur eine Verurteilung) und habe für das Ansehen des Strafrechts und des Staates mehr Schaden angerichtet als Nutzen gebracht. So hätten sich sogar zuvor dem Inhalt der Äußerungen ablehnend gegenüberstehende Personen mit den Beschuldigten aufgrund der als übergriffig empfundenen Punitivität des Staates solidarisiert.¹¹

Die negativen Wirkungen der Vorschriften, insbesondere auf das geistige Klima, und die Gefahren für die Meinungsfreiheit stünden in keinem angemessenen Verhältnis zum kriminalpolitischen Nutzen.¹² Aus eben diesen Erwägungen wurde später auch dem Versuch eine entsprechende Vorschrift als § 130b StGB wiederzubeleben eine Absage erteilt.¹³ Überzeugende Argumente dafür, dass diese Erfahrungen und Einsichten überholt wären, führt der Entwurf nicht an.

¹⁰ BT-Drs. 9/135.

¹¹ BT-Drs. 9/135.

¹² BT-Drs. 9/135.

¹³ BT-Drs. 11/4359

cc)

Da die Zahl der Verurteilungen schon nach der alten Fassung bis zum Jahre 2013 republikweit jährlich regelmäßig einstellig war,¹⁴ die Unbestimmtheit des Tatbestandes und die Nähe der Norm zum Gesinnungsstrafrecht kaum zu bestreiten sind, steht außerdem zu befürchten, dass die künftige Bedeutung der vorgeschlagenen Fassung rechtstatsächlich mehr in strafprozessualen Ausforschungen mittels digitaler und analoger Durchsuchungen im Ermittlungsverfahren liegen wird, denn in Verurteilungen, die Verletzungen geschützter Rechtsgüter ahnden.

d) Erweiterung des § 241 StGB

Der Entwurf schlägt zudem die Erweiterung der strafbaren Bedrohung um Körperverletzungsdelikte, solche gegen die persönliche Freiheit oder die sexuelle Selbstbestimmung und gar gegen Inaussichtstellung strafbarer Handlungen gegen Sachen von bedeutendem Wert vor. Hier streiten teils ähnliche Bedenken wie bereits oben für § 126 StGB-E unter 2a) formuliert gegen den Vorschlag. Denn auch für § 241 StGB gilt, dass sich die Vereinbarkeit der Deliktsstrukturen von § 241 und § 224 StGB, was die Frage der Drohung mit Handlungsqualifikationen angeht, keineswegs von selbst verstehen.

aa)

Die Einbeziehung der einfachen Körperverletzung wird darüber hinaus zu einer strafrechtlichen Erfassung von sich regelmäßig als niedrighschwelligen Drohungen, gegebenenfalls sogar in der Form rhetorischer Fragen führen,¹⁵ die sich alltäglich auf dem Schulhof oder in der Kneipe finden.¹⁶

¹⁴ Zitiert nach Kindhäuser/Neumann/Paeffgen-Ostendorf, § 140 Rz. 4

¹⁵ BGH v. 16.6.2016 – 3 StR 124/16

¹⁶ So würde künftig das zumeist folgenlose, aber nicht nur in gewissen Kneipen ubiquitäre „Willst’ ein paar auf’s Maul?“ zum Offizialdelikt.

Derartige Äußerungen werden sich durch drohende strafrechtliche Ahndung nicht verhindern lassen, indes zu einer noch weitergehenden Überlastung der Strafverfolgungsbehörden und -justiz führen. Sie werden unfreiwillig außerdem zum unzutreffenden Narrativ vermeintlich kaum beherrschbarer Kriminalitätszunahme gerade auch im Jugendbereich beitragen, die in Wahrheit nur das Resultat der Ausweitung normativer Strafbarkeit durch den Gesetzgeber wäre. Statistisch ist sie sodann aber ohne weiteres geeignet, das subjektive Sicherheitsgefühl der Bevölkerung entgegen den realen Verhältnissen weiter zu untergraben.

bb)

An die Pönalisierung von Verhaltensweisen, die der eigentlichen Rechtsgutsverletzung vorgelagert sind, sollten aufgrund des ultima-ratio Prinzips hohe Anforderungen gestellt werden. Die Beschränkung des § 241 StGB auf Verbrechen war diesem Grundsatz geschuldet, den aufzugeben kein Anlass besteht. Ist indes der Damm einmal gebrochen, scheinen der Bagatellisierung kaum Grenzen gesetzt. Im Referentenentwurf war die Erweiterung noch auf Körperverletzungsdelikte beschränkt. Zu diesen gesellen sich nun angedrohte Straftaten gegen die persönliche Freiheit, sexuelle Selbstbestimmung und gar gegen Sachen von bedeutenden Wert. Warum die nicht nötigende Drohung mit Sachbeschädigungen den gleichen Strafrahmen erfahren soll wie die vollendete Sachbeschädigung (nach dem Entwurf Geldstrafe bis 2 Jahre Freiheitsstrafe, was der vollendeten Sachbeschädigung entspricht) erschließt sich nicht nur vom Gedanken des Rechtsgüterschutzes her nicht, sondern taugt allenfalls als Beleg des Verlusts an Augenmaß bei der Strafbarkeitsausweitung und Aufgabe des ultima ratio Prinzips.

Der Vorschlag ist daher abzulehnen.

- e) Neuer Qualifikationstatbestand im Rahmen der Beleidigung, § 185 StGB sowie Ausweitung des geschützten Personenkreises in § 188 StGB

Die vorgesehenen Änderungen in §§ 185 und 188 StGB-E sollen ausweislich der Problem- und Zielbeschreibung des Entwurfs u. a. in der Öffentlichkeit stehende Personen gegen diffamierende Äußerungen schützen, deren respektlose und herabwürdigende Inhalte für eine breite Öffentlichkeit lange Zeit nicht nur wahrnehmbar, sondern auch geeignet seien, die Hemmschwelle für gleichgerichtete Äußerungen bei potentiellen Nachahmern herabzusetzen.¹⁷

Das Bedürfnis, politisch aktive und von daher in der Öffentlichkeit stehende Personen stärker gegen Angriffe auf ihre Ehre und Verleumdungen zu schützen, ist angesichts mancher Exzesse im Internet ggü. politisch aktiven Personen und nicht zuletzt wegen der Ermordung von Walter Lübcke verständlich. Es stellt sich jedoch als gegenläufig zur verfassungsgerichtlichen Rechtsprechung dar, die den politischen Funktionsträgern im öffentlichen Meinungskampf eine erhöhte Duldung von Ehrangriffen jenseits reiner Schmähkritik abverlangt und droht damit stets in Konflikt mit dieser zu geraten.¹⁸

aa)

Gegen den erweiterten Schutz auch von Kommunalpolitikern, die zumeist ehrenamtlich tätig sind, ist im Grundsatz nichts zu erinnern. Angesichts der bisherigen praktischen Bedeutungslosigkeit von § 188 StGB muss allerdings bezweifelt werden, dass die Novelle insoweit die gewünschte Wirkung entfaltet.

bb)

Gleiches gilt für den Vorschlag, den Qualifikationstatbestand von § 185 StGB für die Fälle der Verbreitung der Beleidigung durch Schriften im Sinne von § 11 Abs. 3 StGB zu erweitern. Der Strafraum für abwertende

¹⁷ Vgl. S. 1 des Referentenentwurfs

¹⁸ S. etwa BVerfGE 61, 1 (11) für Wahlkämpfe, vgl. a. „Vermutung für die freie Rede: BVerfGE 7, 198 (212); 93, 266 (294 f.); BVerfG NJW 2003, 3760; 2006, 3266 (3267); 2009, 3016 (3017); vgl. a. Zusammenfassend „Üble Nachrede und Verleumdung“ – Ausarbeitung Wissenschaftlicher Dienst des Bundestags, S. 6 ff. (<https://www.bundestag.de/resource/blob/407504/dfcdee163a8b5201de6ac33d17bfb524/WD-7-216-13-pdf-data.pdf>)

Werturteile im jetzt geltenden § 185 StGB lässt bereits hinreichend Differenzierungsspielraum, um auch einen hohen Verbreitungsgrad zu pönalisieren. Das Phänomen hoher Verbreitung ist zudem nicht neu, dennoch wurden Beleidigungen, die etwa über Medien verbreitet wurden auch bislang nicht als Qualifikationstatbestand diskutiert. Es ist nicht ersichtlich, dass dies kriminalpolitisch nun aufgrund des Internets Not täte oder geeignet wäre, das dortige Nutzerverhalten zu domestizieren. Da es sich zudem weiterhin um absolute Antragsdelikte handelt, erscheint der Strafraum übersetzt, und zwar nicht nur, weil in der Wissenschaft vor kurzen noch die Abschaffung und Überflüssigkeit strafrechtlicher Ahndung von Verletzungen des unscharfen Ehrbegriffs diskutiert und gefordert wurde.¹⁹

- f) Änderungsvorschlag § 115 Abs. 3 StGB-E, Erweiterung des geschützten Personenkreises um Hilfeleistende

Die Erweiterung des Personenkreises des § 115 III StGB um Hilfeleistende eines ärztlichen Notdienstes und in Notaufnahmen ist für sich genommen aufgrund der Vergleichbarkeit mit den bereits erfassten Hilfeleistenden nachvollziehbar, angemessen und in sich konsequent. An den durch die jüngsten Reformen zuvor entstandenen systematischen Ungereimtheiten der §§ 113 ff.²⁰ vermag dies nichts zu ändern.

Es bestehen insbesondere keine sog. Strafbarkeitslücken. Die nunmehr von §§ 113, 114 i.V.m. § 115 StGB erfassten Verhaltensweisen sind letztlich bereits umfassend von den Beleidigungs-, Nötigungs- und Körperverletzungsdelikten abgedeckt, wobei die Funktion der angegriffenen Person ggf. auf Strafzumessungsebene berücksichtigt werden kann.

¹⁹ Kubiciel/Winter, ZStW 113, 305ff.

²⁰ Dazu umfassend: Stellungnahme des DAV 5/17; s. a. Stellungnahme Nr. 16/2017 der BRAK.



LUDWIG-
MAXIMILIANS-
UNIVERSITÄT
MÜNCHEN

PROF. DR. ARMIN ENGLÄNDER
LEHRSTUHL FÜR STRAFRECHT, STRAFPROZESSRECHT,
RECHTSPHILOSOPHIE UND RECHTSSOZIOLOGIE



LMU · Geschwister-Scholl-Platz 1 · 80539 München

Armin Engländer

Telefon +49 (0)89 2180-9470
Telefax +49 (0)89 2180-99-
9471

Armin.Englaender@jura.uni-
muenchen.de

Postanschrift
Prof.-Huber-Platz 2
80539 München

München, 4. Mai 2010

Stellungnahme zum Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität

I. Gegenstand der Stellungnahme

Der Gesetzentwurf der Bundesregierung eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität konstatiert eine zunehmende Verrohung der Kommunikation im Internet im Allgemeinen und in den sozialen Medien im Besonderen, die sich u.a. durch Einschüchterung, Androhung und Billigung von Straftaten und massive Beleidigungen auszeichne. Dadurch würden nicht nur das allgemeine Persönlichkeitsrecht sowie weitere Rechtsgüter der Betroffenen verletzt, sondern auch der politische Diskurs in der demokratischen und pluralistischen Gesellschaft angegriffen und letztlich die Meinungsfreiheit gefährdet. Ziel des Gesetzesentwurfs ist, mit dem Mittel des Strafrechts dieser Entwicklung gegenzusteuern und Rechtsextremismus und Hasskriminalität insbesondere (aber nicht nur) im Hinblick auf Tatbegehungen im Internet effektiv zu bekämpfen. Hierzu werden eine Reihe von prozessualen Anpassungen in der StPO, dem BKAG, dem TMG und dem NetzDG, aber auch verschiedene Änderungen und Ergänzungen im materiellen Strafrecht vorgeschlagen. Die vorliegende Stellungnahme beschränkt sich auf die vorgeschlagenen Änderungen des StGB.

II. Zusammenfassung

Der Gesetzentwurf der Bundesregierung verdient in seiner Zielsetzung uneingeschränkt Zustimmung. Auch die Umsetzung ist unter Zugrundelegung der soeben skizzierten Grundannahmen des Entwurfs im tatsächlichen Bereich in weiten Teilen schlüssig. Das gilt insbesondere im Hinblick auf die sinnvollen Änderungen und Ergänzungen bei den Beleidigungstatbeständen, die einen der Schwerpunkte des Entwurfs bilden. Zu weit gehen allerdings die vorgesehenen Änderungen bei § 140 StGB und § 241 StGB. Insbesondere bei der Bedrohung lässt sich vor dem Hintergrund des anerkannten Schutzzwecks der Vorschrift kriminalpolitisch allenfalls eine deutlich restriktivere Erweiterung des Tatbestandes legitimieren. Hinzuweisen ist schließlich darauf, dass sich die mit dem Mittel des Strafrechts verfolgten gesetzgeberischen Ziele nur erreichen lassen, wenn die Strafjustiz auch über ausreichende Ressourcen verfügt, die entsprechenden Straftaten zu verfolgen und zu ahnden.

III. Die vorgeschlagenen Änderungen des StGB im Einzelnen

1. Die vorgeschlagene Ergänzung der exemplarisch genannten Beweggründe in § 46 Abs. 2 StGB um die antisemitischen ist zwar nicht notwendig, um diese bei der Strafzumessung strafscharfend berücksichtigen zu können, da sie schon bisher erfasst waren.¹ Insoweit handelt es sich um einen symbolischen Akt. Da dem Strafrecht aber auch eine kommunikative Funktion zukommt, ist es vor dem Hintergrund der deutschen Geschichte und angesichts des Anstiegs von Straftaten aus antisemitischen Motiven rechtspolitisch gut vertretbar, die strafscharfende Bedeutung solcher Beweggründe ausdrücklich hervorzuheben.

Kritisch wäre hingegen eine – im Gesetzentwurf der Bundesregierung freilich nicht vorgeschlagene – Ergänzung der menschenverachtenden Beweggründe um weitere konkretisierende Beispiele zu sehen. Denn sämtliche Ausprägungen gruppenbezogener Menschenfeindlichkeit wird man weder in einem abschließenden Katalog fixieren noch in den Gesetzestext aufnehmen können. Begnügte man sich aber mit einer Auswahl, drohte das von den nicht erwähnten gesellschaftlichen Gruppen mit Diskriminierungserfahrung als Zurücksetzung und fehlende Anerkennung empfunden zu werden.

¹ Miebach/Maier, in MüKo-StGB, 3. Aufl. 2016, § 46 Rn. 187.

2. Die vorgeschlagene Ergänzung in § 115 Abs. 3 S. 1 StGB um Hilfeleistende des ärztlichen Notdienstes und der Notaufnahme ist gemessen an dem schon bislang einbezogenen Personenkreis² gut nachvollziehbar. Die Hilfeleistenden des ärztlichen Notdienstes werden bei Unglücksfällen regelmäßig in den gleichen zugespitzten Gefahrensituationen tätig wie die des Rettungsdienstes und auch beim medizinischen Personal der Notaufnahme kann es zu vergleichbaren konfliktbehafteten Gefahrenlagen kommen.

Wiederum kritisch zu sehen wäre allerdings eine in der rechtspolitischen Debatte gelegentlich geforderte weitergehende Ausdehnung des Tatbestandes auf Fälle jenseits der nötigen Behinderung professioneller Hilfeleistender in zugespitzten Gefahrenlagen. Damit würde die Vorschrift zu einem „Super-Nötigungsdelikt“ umfunktioniert, dessen Legitimation zweifelhaft und dessen Verortung im Abschnitt über den Widerstand gegen die Staatsgewalt verfehlt wäre.

3. Die Ergänzung des Straftatkatalogs des § 126 Abs. 1 Nr. 3 StGB um die gefährliche Körperverletzung ist rechtspolitisch gut vertretbar. Zwar ist der Kritik (vgl. etwa die BRAK-Stellungnahme zum Regierungsentwurf, S. 7) zuzugestehen, dass es sich bei § 224 StGB lediglich um ein Delikt mittleren Schweregrades handelt. Gleichwohl kann aber etwa eine Androhung von Vergiftungen (§ 224 Abs. 1 Nr. 1 Alt. 1 StGB) wie beispielsweise das öffentliche Inaussichtstellen, in ausgewählten Supermärkten verschiedene Lebensmittel mit Gift zu versetzen oder das Ankündigen von mit Waffen begangenen Körperverletzungen (§ 224 Abs. 1 Nr. 2 Alt. 1 StGB) unter Umständen geeignet sein, zu einer besonderen Beunruhigung der Bevölkerung zu führen, also den öffentlichen Frieden zu stören.³

Bedenkenswert erscheint der Vorschlag des Bundesrates aus seiner Stellungnahme, den Straftatkatalog in einer Nr. 8 noch um die in §§ 177 Abs. 4 – 8 StGB genannten qualifizierten Sexualdelikte zu ergänzen (BT-Drucks. 19/18470, S. 19). Zwar übersieht die Begründung des Bundesrates („Schutz für Frauen“), dass § 126 StGB jedenfalls primär nicht dem Schutz derjenigen Individualrechtsgüter dient, die durch die im Katalog genannten Straftatbestände geschützt werden sollen, sondern den Schutz des öffentlichen Friedens bezweckt.⁴ Unstreitig kann aber die Androhung qualifizierter Sexualstraftaten, die einen erhöhten Schweregrad besitzen und durchaus ähnlich dem

² Zu den grundsätzlichen Bedenken gegen die Gleichstellung dieser Personengruppe mit den Vollstreckungsbeamten der §§ 113, 114 StGB s. aber *Bosch*, in *MüKo-StGB*, 3. Aufl. 2017, § 114 Rn. 1.

³ Zur Eignungsklausel siehe *Krauß*, in *LK-StGB*, 12. Aufl. 2009, § 126 Rn. 26 ff.

⁴ *Kuhli*, in *Matt/Renzikowski*, StGB, 2. Aufl. 2020, § 126 Rn. 1.

von § 126 Abs. 1 Nr. 3 StGB erfassten § 226 StGB nachhaltige Folgen haben können, geeignet sein, die Bevölkerung in besonderem Maße zu beunruhigen.

4. Kritisch zu sehen ist der Vorschlag, in § 140 Nr. 2 StGB künftig auch das Billigen noch nicht begangener oder in strafbarer Weise versuchter Straftaten unter Strafe zu stellen und damit die Strafbarkeit weit ins Vorfeld der entsprechenden Taten auszudehnen. Schon die Frage, inwieweit das bloße Gutheißen von Taten, die in ihren einzelnen Modalitäten noch gänzlich unbestimmt sind und womöglich in weiter Zukunft liegen oder – in den allermeisten Fällen – sogar niemals verwirklicht werden, tatsächlich das Vertrauen in die Geltungskraft der Rechtsordnung zu erschüttern vermag und wirklich das Entstehen eines Klimas begünstigt, in dem die entsprechenden Taten gedeihen können, lässt sich jenseits alltagspsychologischer Erwägungen nur schwer beantworten. Bereits dies führt dazu, dass die vorgeschlagene Regelung unter Legitimitäts Gesichtspunkten nicht unbedenklich erscheint. Jedenfalls drohen nicht unerhebliche Auslegungs- und Anwendungsprobleme. So stellt sich etwa die Frage, ob künftig jeder „Facebook-Like“ zu einem Posting, in dem eine der in § 140 StGB genannten Straftaten begrüßt wird, seinerseits als Billigen nach § 140 StGB zu bestrafen wäre. Bejahte man dies, kämen hier nicht nur die Strafverfolgungsorgane sehr schnell an ihre Grenzen; es stellte sich die Frage nach der Strafwürdig- und -bedürftigkeit des entsprechenden Verhaltens. Zwar ließe sich das Ausscheiden solcher Fälle aus dem Anwendungsbereich des § 140 StGB damit begründen, sie seien nicht geeignet, den öffentlichen Frieden zu stören. Angesichts der Vagheit dieses Tatbestandsmerkmals ist allerdings keineswegs gewährleistet, dass damit in der Praxis eine Beschränkung des Anwendungsbereichs rechtssicher gelingt. Auf der Grundlage des Gesetzesentwurfs lässt sich die Frage jedenfalls nicht mit der nötigen Sicherheit beantworten. Die Antwort würde damit der Justiz überlassen, so dass divergierende Entscheidungen drohten. Aber auch wenn man die Problematik der „Likes“ einmal zurückstellt, dürfte es Polizei, Staatsanwaltschaft und Gerichten schon unter Kapazitätsgesichtspunkten ganz erhebliche Probleme bereiten, auch nur ansatzweise sämtliche Postings zu verfolgen, die nach dem Entwurf künftig unter § 140 StGB fallen sollen.
5. Ein Schwerpunkt des Gesetzesentwurfs der Bundesregierung und der verschiedenen Reformüberlegungen liegt bei den Beleidigungsdelikten.
 - a) Hier ist im Gesetzesentwurf zunächst die Schaffung eines weiteren Qualifikationstatbestandes zu § 185 StGB in Form der öffentlich, in einer Versammlung oder durch Verbreiten von Schriften begangenen Beleidigung plausibel begründet. Die Annahme,

dass beleidigende Äußerungen, die über einen längeren Zeitraum von einem großen Personenkreis abrufbar sind, für den Betroffenen besonders schwer wiegen können, erscheint richtig. Stimmig ist auch die Ergänzung des § 186 StGB; hier wird eine Ungereimtheit im Verhältnis zu § 187 StGB beseitigt.⁵

- b) Ebenso überzeugt die Ergänzung des § 188 Abs. 1 StGB. Hiermit wird eine durch die restriktive Interpretation des Tatbestandsmerkmals des politischen Lebens entstandene Schutzlücke geschlossen. Das erscheint auf Basis der tatsächlichen Grundannahmen des Entwurfs geboten, da sich gerade Personen, die sich hauptamtlich oder auch ehrenamtlich auf regionaler oder kommunaler Ebene engagieren, in zunehmendem Maße ehrenrührigen Tatsachenbehauptungen ausgesetzt sehen. Ob man dabei die Formulierung des Regierungsentwurfs oder den Vorschlag des Bundesrates aus seiner Stellungnahme vorzieht, ist Geschmackssache. Für letzteren streitet die etwas höhere sprachliche Präzision, für erstere ihre Knappheit. Die Bedenken des Bundesrates hinsichtlich der hinreichenden Bestimmtheit der Formulierung des Regierungsentwurfs (BT-Drucks. 19/18470, S. 21) erscheinen jedenfalls nicht begründet. Bislang wurden auf regionaler oder kommunaler Ebene politisch tätige Personen aus dem von § 188 StGB geschützten Personenkreis ausgeschlossen, weil sie aufgrund der räumlichen Begrenztheit ihres Wirkens nicht im politischen Leben des *gesamten* Volkes stünden.⁶ Dieser Argumentation ist mit der Formulierung des Regierungsentwurfs die Grundlage entzogen. Befürchtungen, dass etwa auf Bezirksebene tätige Personen auch weiterhin nicht erfasst würden, sind vor diesem Hintergrund nicht gerechtfertigt. Denn stellt der Regierungsentwurf mit der Formulierung, dass das politische Leben des Volkes *bis* zur kommunalen Ebene reicht, klar, dass die räumliche Begrenztheit des Wirkens der Anwendung des § 188 StGB nicht entgegensteht, gilt das selbstverständlich auch für die Bezirksebene.

Weitergehend wäre zu überlegen, ob dem Diskussionsentwurf des Bayerischen Staatsministeriums der Justiz für ein „Gesetz zur nachdrücklichen strafrechtlichen Bekämpfung der Hassrede und anderer besonders verwerflicher Formen der Beleidigung“ (Diskussionsentwurf, S. 1 f.) und der Anregung des Bundesrates (BT-Drucks. 19/18470, S. 20) entsprechend der Anwendungsbereich des § 188 StGB auch auf Beleidigungen gem. § 185 StGB zu erstrecken ist. Denn eine Vergiftung des politischen Klimas durch Ehrabschneidungen und Diffamierung des politischen Gegners als

⁵ S. dazu *Lackner/Kühl*, StGB, 29. Aufl. 2018, § 187 Rn. 3.

⁶ *Valerius*, in BeckOK-StGB, Stand 01.02.2020, § 188 Rn. 5 m.w.N.

Kampfmittel, der § 188 StGB gerade entgegenwirken soll,⁷ kann nicht nur von ehrenrührige Tatsachenbehauptungen, sondern ebenso von ehrenrührigen Werturteilen drohen. Freilich darf man sich von einer solchen Ergänzung auch nicht zu viel versprechen, da das starke Gewicht, welches das BVerfG der Meinungsfreiheit im Verhältnis zum Ehrschutz gerade für den Bereich der politischen Auseinandersetzung zuerkennt und das hier häufig zu einer Verneinung des § 185 StGB oder zu einer Bejahung der rechtfertigenden Wahrnehmung berechtigter Interessen gem. § 193 StGB führt,⁸ selbstverständlich unangetastet bliebe.

Richtigerweise hält der Gesetzentwurf der Bundesregierung in § 188 StGB am Erfordernis einer Eignung der ehrverletzenden Äußerung, das öffentliche Wirken der politisch tätigen Person erheblich zu erschweren, fest. Der Vorschlag des Bayerischen Diskussionsentwurfs und der ihm folgenden Stellungnahme des Bundesrates, die Eignungsklausel zu streichen, verdient keine Zustimmung. Dass § 188 StGB Personen des politischen Lebens einen verstärkten Ehrschutz einräumt, liegt, wie eben erwähnt, in dem Schaden begründet, den Ehrabschneidungen der politischen Kultur zufügen können. Daher erscheint es sachgerecht, solche ehrverletzenden Äußerungen aus dem Anwendungsbereich der Vorschrift auszuschneiden, denen eine Eignung zu einer solchen Schadenszufügung fehlt. Eben das sicherzustellen, ist eine Funktion der Eignungsklausel.⁹ Bei Äußerungen, die nicht geeignet sind, das politische Wirken des Betroffenen zu erschweren, besteht Grund zu der Annahme, dass hier eine Beeinträchtigung der politischen Kultur nicht droht. Damit wird die betroffene Person im Übrigen nicht schutzlos gestellt; es verbleibt selbstverständlich immer noch der Schutz durch die §§ 185 – 187 StGB.

Umgekehrt führt die im Bayerischen Diskussionsentwurf und dem ihm folgenden Antrag von Bündnis 90/Die Grünen vorgeschlagene Einfügung des Erfordernisses, dass die Äußerung *in Beziehung* zur politischen Tätigkeit stehen müsse, zu einer problematischen *Verengung* des Tatbestandes. Zu Recht ist es bislang nicht notwendig, dass die behauptete ehrenrührige Tatsache sich auf das politische Wirken des Opfers bezieht.¹⁰ Das Vertrauen der Bevölkerung in die Integrität der politisch tätigen Person, dem für die Erfüllung ihrer politischen Aufgaben eine erhebliche Bedeutung zukommt, kann ohne Weiteres auch durch andere ehrenrührige Tatsachenbehauptun-

⁷ Hilgendorf, in LK-StGB, 12. Aufl. 2009, § 188 Rn. 1.

⁸ Näher dazu Eisele/Schittenhelm, in Schönke/Schröder, 30. Aufl. 2019, § 193 Rn. 15 ff.; Gaede, in Matt/Renzikowski, § 193 Rn. 16 f. jeweils m.w.N.

⁹ Regge/Pegel, in MüKo-StGB, 3. Aufl. 2017, § 188 Rn. 12.

¹⁰ Eisele/Schittenhelm, in Schönke/Schröder (Fn. 8), § 188 Rn. 4.

gen beruflicher oder privater Art – etwa dergestalt, dass sie an ihrem (nicht im politischen Bereich angesiedelten) Arbeitsplatz Gelder unterschlagen habe oder ihren Partner oder ihre Partnerin misshandele – erschüttert werden. Zudem würden bislang nach herrschender Meinung erfasste Personen wie Bundesverfassungsrichter, Gewerkschaftsführer oder Spitzenvertreter von Arbeitgeberverbänden, die zwar im politischen Leben des Volkes stehen, sich aber nicht im engeren Sinne politisch betätigen,¹¹ künftig aus dem Anwendungsbereich des § 188 StGB ausgeschlossen. Diese Konsequenzen werden im Diskussionsentwurf nicht angesprochen und sind wohl auch nicht bedacht.

- c) Überzeugend ist im Gesetzentwurf auch die Umgestaltung des § 188 StGB von einem reinen zu einem relativen Antragsdelikt (begrenzt durch ein Widerspruchsrecht der beleidigten Person) in § 194 StGB. Die hiergegen geäußerten Bedenken des Deutschen Richterbundes (Stellungnahme zum Referentenentwurf, S. 3) erscheinen wenig plausibel, musste doch die Staatsanwaltschaft schon bislang im Kontext des § 376 StPO (Anklageerhebung bei Privatklagedelikten) darüber entscheiden, ob sie im Falle des hinreichenden Verdachts einer Begehung des § 188 StGB das öffentliche Interesse bejaht, ohne dass dies als „politisches Statement“ missdeutet worden und sie deshalb unter Rechtfertigungsdruck geraten wäre.
- d) Eine weitergehende Umgestaltung der Beleidigungsdelikte, wie sie etwa im Bayerischen Diskussionsentwurf und in dem diesen übernehmenden Änderungsantrag von Bündnis 90/Die Grünen befürwortet wird, sollte nicht vorschnell vorgenommen werden. Zuvor bedarf der eingehenden Prüfung und Diskussion, ob die vorgeschlagenen Änderungen aus Gründen der Wertungskonsistenz weitere Anpassungen bei anderen Delikten wie etwa den Straftaten gegen die körperliche Unversehrtheit oder gegen die persönliche Freiheit notwendig machten und ob solche umfassenderen Änderungen rechtspolitisch wünschenswert wären. So wirft der Vorschlag, die Strafzumessungskriterien der menschenverachtenden Beweggründe bei den Beleidigungstatbeständen bereichsbeschränkt zu qualifizierenden Merkmalen auf Tatbestandsebene aufzuwerten (Diskussionsentwurf, S. 2, 21 ff.), nicht nur die Frage nach dem Verhältnis zu § 46 StGB auf, sondern auch die weitere Frage, wieso nicht entsprechende Qualifikationstatbestände etwa für die Körperverletzung, die Freiheitsberaubung, die Nötigung oder die Bedrohung geschaffen werden. Insgesamt drohen hier Faktoren, die bei der Bestimmung der konkreten Strafe *innerhalb* des gesetzlichen Strafrahmens ihren

¹¹ Valerius, in BeckOK-StGB (Fn. 6), § 188 Rn. 6.

Platz haben, übergewichtet zu werden, wenn sie nunmehr eine Erhöhung des *gesamten Strafrahmens* rechtfertigen sollen.

6. Kritisch zu sehen sind die im Gesetzentwurf vorgeschlagenen Änderungen bei § 241 StGB. Erfasst würden dem Wortlaut nach auch die Ankündigung einer Ohrfeige (Bedrohung mit einer Tat gegen die körperliche Unversehrtheit), das Androhen eines Einsperrens für wenige Minuten im Zimmer (Bedrohung mit einer Tat gegen die persönliche Freiheit) oder das Inaussichtstellen des Zerkratzens eines PKW (Bedrohung mit einer Tat gegen eine Sache von bedeutendem Wert.) Auch wenn man bei letzterem in Anknüpfung an die Rechtsprechung zum Tatbestandsmerkmal der fremdem Sache von bedeutendem Wert bei anderen Straftatbeständen wie §§ 263 Abs. 3 Nr. 5, 306f Abs. 2, 315 Abs. 1, 315a Abs.1, 315b Abs. 1, 315c Abs. 1, 315d Abs. 2 verlangt, dass nicht nur der Wert der Sache selbst, sondern auch der drohende Schaden „bedeutend“ sein muss,¹² so ist die dafür nach derzeitiger Rechtsprechung zu veranschlagende Untergrenze von ca. 750 – 1.300 €¹³ schnell überschritten.

Mit dem Gesetzentwurf wird der bisherige Schutzzweck des § 241 StGB – Schutz des individuellen Rechtsfriedens, also des Vertrauens des Einzelnen auf seine durch das Recht gewährleistete Sicherheit vor *besonders gravierenden* Bedrohungen¹⁴ – weit überdehnt. Für eine Einbeziehung von Taten gegen Sachen, die sich nicht als Verbrechen darstellen, besteht vor dem Hintergrund des Schutzzwecks der Vorschrift kein kriminalpolitisches Bedürfnis. Bei Taten gegen die körperliche Unversehrtheit und die sexuelle Selbstbestimmung wird man mit dem Vorschlag des Bundesrates (BT-Drucks. 19/18470, S. 22) und dem Änderungsantrag von Bündnis 90/Die Grünen zumindest fordern müssen, dass diese mit einer im Mindestmaß erhöhten Freiheitsstrafe bedroht sind. Selbiges gilt – entgegen dem insoweit auf der Linie des Regierungsentwurfs liegenden Vorschlag des Bundesrates und dem Änderungsantrag von Bündnis 90/Die Grünen – auch für Taten gegen die persönliche Freiheit. Insbesondere die Einbeziehung der einfachen Freiheitsberaubung erfasste, wie oben am Beispiel aufgezeigt, auch bagatellartige Fallkonstellationen, die weit jenseits des oben genannten Schutzzwecks des § 241 StGB liegen. Insgesamt gilt bei diesem Straftatbestand im Blick zu behalten, dass die Strafbarkeit an ein Verhalten im Vorfeld der eigentlichen Rechtsgutsverletzung anknüpft, die erst durch die tatsächliche Ausführung der

¹² Näher dazu Wessels/Hettinger/Engländer, Strafrecht BT I, 43. Aufl. 2019, Rn. 1030.

¹³ Dezidiert für eine Untergrenze von lediglich 750 € BGH NSTZ 2011, 215. Zur Gegenansicht (nicht mehr unter 1.300 €) s. Fischer, StGB, 66. Aufl. 2019, § 315 Rn. 16a.

¹⁴ Sinn, in MüKo-StGB (Fn. 9), § 241 Rn. 2.

angedrohten Straftat eintritt, was im Hinblick auf das verfassungsrechtliche Erfordernis der Verhältnismäßigkeit besonders in Rechnung zu stellen ist.

Generalstaatsanwaltschaft München
Der Beauftragte der bayerischen Justiz
zur strafrechtlichen Bekämpfung von
Hate-Speech



Generalstaatsanwaltschaft München • 80097 München

I. Per E-Mail an

Deutscher Bundestag

Ausschuss für Recht
und Verbraucherschutz
Konrad-Adenauer-Straße 1
10557 Berlin

Sachbearbeiter
Herr Oberstaatsanwalt Hartleb

Telefon
(089) 5597- 4524

Telefax
(089) 5597- 5358

E-Mail
ABTEILUNGE@gensta-m.bayern.de

Ihr Zeichen, Ihre Nachricht vom
PA 6- 5410-2.2

Bitte bei Antwort angeben
Unser Zeichen, Unsere Nachricht vom
GenStA M 4021-503-G-1245/2019

Datum
04.05.2020

Gesetzesentwurf der Fraktionen CDU/CSU und SPD, Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (BT-Drucksache 19/17741) sowie Gesetzesentwurf der Bundesregierung, Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (BT-Drucksache 19/18470)

Zu den vorbenannten, gleichlautenden Gesetzesentwürfen nehme ich wie folgt Stellung:

I. Änderungen des Strafgesetzbuches (Artikel 1):

1. Ergänzung des § 46 StGB

Die Ergänzung des § 46 Abs. 2 Satz 2 StGB um antisemitische Beweggründe ist zu begrüßen. Selbst wenn bereits nach der bisherigen Rechtslage solche Beweggründe unter „sonst menschenverachtende“ Beweggründe gemäß § 46 Abs.

Hausanschrift
Karlsstraße 66
80335 München

Haltestelle
Stiglmaierplatz
U-Bahn: U 1, U 7
Trambahn: 20, 21

Telefon
(089) 5597-08
(Vermittlung)

Telefax
5597-4125

E-Mail:
poststelle@gensta-m.bayern.de

2 Satz 2 StGB subsumierbar sind, erscheint die ausdrückliche Aufnahme antisemitischer Beweggründe als Klarstellung und Bekräftigung der bisherigen Rechtslage angezeigt.

2. Erweiterung des § 115 Abs. 3 StGB

Die Erweiterung des nach § 115 Abs. 3 StGB vor Widerstandshandlungen und tätlichen Angriffen geschützten Personenkreises um Hilfeleistende "eines ärztlichen Notdienstes oder einer Notaufnahme" ist zu begrüßen. Ärztliche Notdienste leisten einen unverzichtbaren Beitrag für die Gesellschaft und sind daher ebenso schützenswert wie die bereits erfassten Mitarbeiterinnen und Mitarbeiter von Feuerwehren, Katastrophenschutz oder Rettungsdiensten. Dies gilt umso mehr, als sich Übergriffe gegen ärztliche Notdienste in jüngster Zeit häuften.

3. Ergänzung des § 126 StGB

Der Erweiterung des Straftatenkatalogs des § 126 Abs. 1 StGB um das Vergehen der gefährlichen Körperverletzung begegnen keine Bedenken. Darüber hinaus ist die vom Bundesrat angeregte Aufnahme der Verbrechen gemäß § 177 Abs. 4 bis 8 StGB zu begrüßen. Anzumerken ist, dass mit der Änderung des § 126 Abs. 1 Nr. 3 StGB auch Weiterungen in anderen Straftatbeständen einhergehen, die auf den in § 126 Abs. 1 StGB enthaltenen Straftatenkatalog dynamisch verweisen (vgl. §§ 130a, 140, 145 d StGB).

4. Erweiterung des § 140 StGB

Die geplante Änderung wird begrüßt. Sie ist insbesondere geeignet, der zunehmenden Verrohung der Kommunikation in den sozialen Medien in Form von Aggression, Einschüchterung und Drohungen entgegen zu wirken. Ein nicht unerheblicher Anteil der Hasskommentare im Internet besteht in dem Gutheißen der in § 140 StGB-E aufgeführten Katalogtaten. Dies trägt zu einer nicht mehr hinnehmbaren Verrohung des gesellschaftlichen Klimas bei und bereitet den Nährboden für reale Gewalttaten. Derartige Äußerungen sind nicht notwendigerweise von anderen Straftatbeständen, insbesondere §§ 111, 126, 130, 131 StGB erfasst, sodass eine zu schließende Strafbarkeitslücke besteht.

5. Änderungen der §§ 185, 188, 194 StGB

Die in den §§ 185, 188, 194 StGB vorgesehenen Änderungen schöpfen den Regelungs- und Handlungsbedarf im Bereich der Beleidigungsdelikte nicht aus. Zwar ist zu begrüßen, dass die Gesetzesentwürfe einen Qualifikationstatbestand für öffentlich, in einer Versammlung oder durch Verbreitung von Schriften getätigte Beleidigungen vorsehen. Es besteht nach hiesiger Ansicht aber weitergehender Reformbedarf. Die Regelungen zur Beleidigung, üblen Nachrede und Verleumdung stammen noch aus der Zeit der Einführung des Reichsstrafgesetzbuches im Jahr 1871 und geben aus diesem Grund keine Antworten auf Phänomene jüngerer Zeit, insbesondere strafbarer Hassrede im Internet. Derartige Änderungen sind etwa in dem Diskussionsentwurf der Bayerischen Staatskanzlei für ein Gesetz zur nachdrücklichen strafrechtlichen Bekämpfung der Hassrede und anderer besonders verwerflicher Formen der Beleidigung näher dargestellt, welche zu begrüßen sind.

Die aus dem vorliegenden Gesetzesentwürfen resultierenden Schutzdefizite zeigen sich insbesondere bei der Beleidigung von Personen des politischen Lebens. So werden zwar auch kommunalpolitisch tätige Personen (eindeutig) in den Schutzbereich des § 188 StGB einbezogen und die Strafverfolgungsbefugnis durch Änderung des § 194 StGB erweitert. Die Vorschrift des § 188 StGB ist in der Praxis jedoch weitestgehend bedeutungslos. Das hat seinen Grund darin, dass Fälle der Beleidigung gem. § 185 StGB hiervon nicht erfasst werden und mit der in § 188 StGB enthaltenen Eignungsklausel erhebliche Bewertungsunsicherheiten einhergehen, die dem Erfordernis eines effektiven Schutzes ebenfalls zuwiderlaufen.

6. Erweiterung des § 241 StGB

Die Erweiterung wird begrüßt. Sie ist angesichts der in der staatsanwaltlichen Praxis oft als unbefriedigend empfundenen Situationen, in denen der Bedrohungsstatbestand auch bei massiven Drohungen gegen den Leib oder mit Vergewaltigung ins Leere lief, überfällig. Auch ist zu begrüßen, dass der Begriff der körperlichen Unversehrtheit im Rahmen der Drohung herangezogen wurde, da dieser Begriff der gesetzgeberischen Systematik entspricht und eine klare und eindeutige Abgrenzung ermöglicht. Die Gefahr einer ausufernden Strafverfolgung besteht nicht, da weiterhin die Möglichkeit einer Privatklageverweisung verbleibt. Diese ist lediglich dann ausgeschlossen, wenn die Tat öffentlich oder durch Verbreiten von Schriften erfolgt (§ 241 Abs. 4 StGB-E. i.V.m § 374 Abs. 1 Nr. 5

StPO-E). Dies jedoch aus gutem Grund: Bedrohungen, die beispielsweise über das Internet öffentlich begangen werden, erfahren eine erheblich größere Verbreitung. Zudem ist deren Entfernung wesentlich erschwert.

II. Änderungen in der Strafprozessordnung (StPO) (Artikel 2)

1. Die Änderungen in § 100g StPO und § 100j StPO

Gegen die vorgesehene Angleichung der Regelungen über die Verkehrs- und Bestandsdatenerhebung bei Telemediendiensten und Telekommunikationsunternehmen in §§ 100g, 100j StPO bestehen im Grundsatz keine durchgreifenden Bedenken, auch wenn nach hiesiger Auffassung in Übereinstimmung mit einem Teil der Kommentarliteratur (siehe etwa BeckOK-StPO/Bär, 36. Edition, § 100g Rn. 26) mit §§ 161, 163 StPO bereits ausreichende Befugnisnormen für die Datenerhebung bei den Anbietern von Telemediendiensten zur Verfügung stehen.

Allerdings greift die Angleichung zu kurz. Sie erfolgt nur teilweise und reicht zudem nicht aus, um die Urheber strafrechtlich relevanter Hasskommentare ermitteln und zur Verantwortung ziehen zu können. Den Ermittlungsbehörden müssen die für die Verfolgung von Hate-Speech erforderlichen strafprozessualen Instrumente an die Hand gegeben werden. Deshalb sollten insbesondere folgende Ergänzungen der rechtlichen Regelungen in Erwägung gezogen werden:

a) § 100g Abs. 1 StPO

Im Rahmen der Verkehrsdatenerhebung nach § 100g Abs. 1 StPO erscheint es zunächst – um jedweden Auslegungsschwierigkeiten oder Missverständnissen in der Rechtspraxis vorzubeugen – angezeigt, explizit klarzustellen, dass Nr. 2 auch mittels Telemediendiensten begangene Straftaten erfasst.

Die Nr. 2 gilt bislang nur für Straftaten, die „mittels Telekommunikation“ (etwa unter Nutzung des Internets als notwendiges Tatmittel) begangen wurden. Dies wird freilich praktisch stets auch gegeben sein, wenn strafrechtlich relevante Hate-Speech über einen Telemediendienst (wie etwa Facebook) verbreitet wird, da der Nutzung eines solchen Dienstes in aller Regel auch eine Telekommunikation zugrunde liegt. Gleichwohl sollte eine entsprechende Klarstellung im

Gesetzeswortlaut, jedenfalls aber in der Gesetzesbegründung, erfolgen, um etwaigen gegenläufigen Auslegungsversuchen, Missverständnissen oder Rechtsanwendungsproblemen von vornherein keinen Raum zu lassen.

Damit wird im Ergebnis zudem unmissverständlich klargestellt, dass die Straftat, die mittels eines Telemediums begangen wird, - anders als bei Nr. 1 - nicht von erheblicher Bedeutung sein muss. Dies trägt dem Umstand Rechnung, dass derjenige Beschuldigte seinen Anspruch auf Wahrung der Vertraulichkeit des Mediums mindert, der dieses missbräuchlich als Tatmittel einsetzt (vgl. BVerfG NJW 2006, 3197 [3198]).

b) § 100g Abs. 2 StPO

Darüber hinaus sollte neben der Erweiterung des § 100g Abs. 1 StPO konsequenterweise auch § 100g Abs. 2 StPO entsprechend erweitert werden. Dies erfordert insbesondere zweierlei:

- eine Erweiterung der Zugriffsbefugnis des § 100g Abs. 2 StPO auf Nutzungsdaten, die aufgrund einer im TMG nach dem Vorbild des § 113b TKG zu schaffenden Speicherverpflichtung (siehe dazu näher unten unter III.) von den Telemediendiensten verpflichtend zu speichern sind.

- eine Anpassung des § 100g Abs. 2 StPO auch auf der Ebene der Anlasstaten dahingehend, dass eine effektive Bekämpfung von Hate-Speech erfolgen kann. Dies könnte in der Weise geschehen, dass der Straftatenkatalog des § 100g Abs. 2 Satz 2 StPO auf bestimmte schwere Straftaten, die im Bereich Hate-Speech relevant sind, erweitert wird. Eine solche Ergänzung ist zur effektiven strafrechtlichen Verfolgung von Hate-Speech nicht nur erforderlich, sondern verfassungsrechtlich auch zulässig.

Erforderlich ist sie, weil gerade im Bereich der über das Internet verbreiteten Hate-Speech die bei den Diensteanbietern gespeicherten Verkehrs- und Nutzungsdaten, insbesondere die dynamischen IP-Adressen, oft der alleinige Ermittlungsansatz zur Identifizierung der Täter sind. Die Tatbegehung vollzieht sich praktisch ausschließlich über die digitale Welt, so dass es Spuren in der realen Welt meist nicht gibt. Die Ermittlungsbehörden sind daher zur Identifizierung der Urheber strafrechtlich relevanter Inhalte auf die Daten, insbesondere die IP-Adressen,

angewiesen.

Verfassungsrechtlich zulässig ist die Ergänzung, weil das Bundesverfassungsgericht für den Abruf und die unmittelbare Nutzung der Daten aus Verhältnismäßigkeitsgründen im Bereich der Strafverfolgung nur einen durch bestimmte Tatsachen begründeten Verdacht einer schweren (und nicht einer besonders schweren) Straftat verlangt (BVerfG NJW 2010, 833 [841]).

Als „schwer“ in diesem Sinne ist mit Blick auf den Strafraum beispielsweise der im Bereich der Hasskriminalität besonders relevante Straftatbestand der Volksverhetzung nach § 130 Abs. 1 und Abs. 3 StGB aber auch die Verleumdung gemäß § 187 StGB in Form des Qualifikationstatbestandes oder die Üble Nachrede und Verleumdung gegen Personen des öffentlichen Lebens gemäß § 188 StGB zu qualifizieren. Für diese Tatbestände sieht das Gesetz eine Freiheitsstrafe bis zu fünf Jahren vor. Auch die öffentliche Aufforderung zu Straftaten (§ 111 StGB) kommt in Betracht, sofern zu einer Straftat aufgerufen wird, deren Höchststrafe mindestens 5 Jahre Freiheitsstrafe beträgt.

Zwar qualifiziert nach der Rechtsprechung des Bundesverfassungsgerichts allein eine Höchststrafe von fünf Jahren Freiheitsstrafe ein Delikt noch nicht als schwere Straftat, bei dem ein Eingriff in Art 10 Abs. 1 Grundgesetz erst verhältnismäßig ist. Vielmehr ist eine Gesamtschau vorzunehmen, die insbesondere die jeweils geschützten Rechtsgüter in den Blick nimmt und so die Qualifizierung einer Straftat als "schwer" rechtfertigt. Von Belang ist insoweit, ob eine besondere Bedeutung des geschützten Rechtsguts oder ein besonderes öffentliches Interesse an der Strafverfolgung vorliegt. (vgl. BVerfG NJW 2012, 833 [836]). Eben dieses besondere öffentliche Interesse und die besondere Bedeutung des geschützten Rechtsguts ist grundsätzlich – nicht zuletzt mit Blick auf die historisch gewachsene Verantwortung der Bundesrepublik Deutschland für die Verbrechen der nationalsozialistischen Gewalt- und Willkürherrschaft – aber auch bei der Bekämpfung des Rechtsextremismus und der Hasskriminalität zu bejahen.

2. Änderungen in § 100j Abs. 1 StPO

Begrüßt wird jedenfalls die vom Bundesrat angeregte Angleichung des § 100j Abs. 1 Satz 2 StPO-E. Damit wird dem Doppeltürmodell des Bundesverfassungsgerichts genüge getan und ein Gleichlauf der in den Gesetzesentwürfen beabsichtigten

Voraussetzungen in § 15b Abs. 2 TMG-E und § 100j Abs. 1 Satz 2 Satz 2 StPO-E hergestellt.

Die Praxisrelevanz der Regelung des § 15b TMG-E dürfte allerdings gering sein. Gesetzeskonform müssen die Passwörter bei den Anbietern als Hash vorliegen. Gemäß § 15 Abs. 3 Satz 2 TMG-E soll die Verschlüsselung unberührt bleiben. Nach hiesigem Kenntnisstand gibt es derzeit keine erfolgversprechende Methode zur Entschlüsselung gehashter Passwörter.

III. Änderung des Telemediengesetzes (TMG) (Artikel 5)

Gegen die vorgesehene Neuregelung des Auskunftsverfahrens für die Telemedienanbieter in einem neuen § 15a TMG bestehen – aus strafprozessualer Sicht – keine durchgreifenden Bedenken, auch wenn nach hiesiger Auffassung bereits mit den derzeitigen Regelungen in §§ 14 Abs. 2, 15 Abs. 5 S. 4 TMG eine ausreichende Rechtsgrundlage für die Übermittlung der Daten durch die Telemedienanbieter zur Verfügung steht. Diese Rechtsgrundlage wird nun in § 15a TMG überführt, der dem § 113 TKG nachgebildet ist und künftig die Telemedienanbieter nicht nur berechtigt, sondern ausdrücklich auch dazu verpflichtet, die zu beauskunftenden Daten unverzüglich und vollständig zu übermitteln, was aus Klarstellungsgründen zu begrüßen ist. Zu begrüßen ist ferner, dass die Telemedienanbieter zum Stillschweigen gegenüber dem Betroffenen bzw. Dritten verpflichtet werden.

Inkonsequent ist es allerdings, zwar eine dem § 113 TKG entsprechende Regelung in das TMG einzuführen, aber auf eine dem § 113b TKG entsprechende Regelung zur Datenspeicherung zu verzichten. Eine solche Speicherung insbesondere von (dynamischen) IP-Adressen ist – wie oben unter II.1.b) gezeigt – für eine effektive Bekämpfung von Rechtsextremismus und Hasskriminalität im Internet unerlässlich. Die gespeicherten IP-Adressen gewinnen dabei nicht nur Bedeutung im Rahmen des Abrufs und der unmittelbaren Nutzung nach § 100g StPO, sondern auch im Rahmen der mittelbaren Nutzung nach § 100j Abs. 2 StPO, wonach eine Bestandsdatenauskunft – unabhängig von einem begrenzenden Straftatenkatalog – auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse verlangt werden darf. Eben diese Befugnisnorm des § 100j Abs. 2 StPO soll durch die Gesetzesentwürfe auch auf Telemediendienste erweitert werden. Praktische Wirksamkeit kann diese Erweiterung aber nur erlangen, wenn sichergestellt ist,

dass die IP-Adressen im Zeitpunkt der Bestandsdatenabfrage noch bei den Diensteanbietern gespeichert sind.

IV. Änderung des Netzwerkdurchsetzungsgesetzes (NetzDG) (Artikel 6)

Die geplanten Änderungen des Netzwerkdurchsetzungsgesetzes (NetzDG) werden begrüßt.

Insbesondere die vorgesehene Einführung der Meldepflicht gemäß § 3a NetzDG stellt ein entscheidendes Instrument dar, die Bekämpfung von Hate-Speech zu intensivieren, stellt sie doch erstmals eine Verpflichtung der Anbieter sozialer Netzwerke dar, entsprechende Hate-Speech Straftaten den Strafverfolgungsbehörden anzuzeigen, anstatt entsprechende Posts lediglich zu löschen.

Durch die Definition des Beschwerde-Begriffs in § 1 NetzDG wird klargestellt, dass von § 3a Abs. 2 Nr. 1 NetzDG-E auch Beschwerden erfasst werden, die nicht explizit nach dem NetzDG erfolgt sind. Allerdings ist darauf hinzuweisen, dass diejenigen Posts nicht von der Anzeigepflicht umfasst sind, die die sozialen Netzwerke ohne das Vorliegen einer Beschwerde eigenständig finden und löschen. Diese Löschungen machen aber einen großen Teil der Löschungen aus. Insofern wäre zu überlegen, die Meldeverpflichtung gemäß § 3a NetzDG zu geeigneter Zeit nachzuschärfen.

In diesem Zusammenhang ist anzumerken, dass im weiteren Verlauf auch eine Ausweitung der Adressaten der Verpflichtungen auf soziale Netzwerke mit weniger als 2 Millionen Nutzern bundesweit bzw. auch auf Gaming-Plattformen im Blick behalten werden sollte.

Die in § 3a Abs. 4 NetzDG-E genannten, dem Bundeskriminalamt zu übermittelnden Informationen, sind allerdings nicht ausreichend. Um Beweismittelverlust durch Zeitablauf zu verhindern, sollten die sozialen Netzwerke dem Bundeskriminalamt sämtliche Informationen liefern müssen, die dort sowohl eine rechtliche Prüfung als auch eine Identifizierung des Täters ermöglichen:

Dazu gehört neben dem inkriminierten Inhalt auch der Kontext, in dem der Inhalt steht, d.h., in aller Regel muss ein Screenshot der fraglichen Seite gesichert und

übermittelt werden, aus dem sich auch ein etwaiger Ausgangsbeitrag und vorangegangene Kommentare ergeben. Dies ist sowohl für die oftmals vorzunehmende Abwägung mit der Meinungsfreiheit als auch für die Frage der fehlenden Rechtfertigung relevant. Es müssen zudem sowohl die URL als auch die ID des Posts sowie ein sekundengenauer Zeitstempel (inklusive der verwendeten Zeitzone) übermittelt werden. Zudem sieht § 3a Abs. 4 NetzDG-E keine Übermittlung der hinterlegten Bestandsdaten vor. Deshalb müsste in dem Fall, in dem eine Identifizierung des Täters nicht über den Inhalt oder die mitgeteilte IP-Adresse erfolgen kann, eine Erhebung der Daten bei den meist ausländischen sozialen Netzwerken im Wege der Rechtshilfe erfolgen. Zwar haben die großen sozialen Netzwerke Möglichkeiten für Strafverfolgungsbehörden geschaffen, online Auskunftersuchen über Bestandsdaten zu stellen. Oft werden diese Ersuchen aber nicht inhaltlich beantwortet, sondern es wird auf den Rechtshilfeweg verwiesen. In der Praxis zeigt sich dann, dass entsprechende Rechtshilfeersuchen mit erheblichem Zeitverzug verbunden sind und oft nicht zu einem Ermittlungserfolg führen. Insbesondere ist die im Bereich Hate-Speech besonders relevante Rechtshilfe in die USA nur unter engen Voraussetzungen (tatsächliche Bedrohung oder Anstiftung zu bevorstehender Gewalt) möglich.



Stellungnahme zum Entwurf der Fraktionen der CDU/CSU und SPD eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (BT-Drucksache 19/17741) und zu dem Entwurf der Bundesregierung eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (BT-Drucksache 19/18470)

1. Einleitung

Die Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW) ist seit Anfang des Jahres 2016 mit der Verfolgung herausgehobener Fälle politisch motivierter Hasskriminalität im Internet befasst. Seit Februar 2017 ist sie als Mitinitiatorin des Projektes „Verfolgen statt nur Löschen“ landesweit in die Bekämpfung der digitalen Hasskriminalität eingebunden. Zudem nimmt die ZAC NRW seit August 2018 zentral die Strafanzeigen des Bundesamtes für Justiz entgegen, die im Zusammenhang mit den dortigen Ordnungswidrigkeitenverfahren nach dem Network Enforcement Act (NetzDG) gestellt werden. Seit Juli 2019 obliegt der ZAC NRW auch die Verfahrensführung bei herausgehobenen Taten politisch motivierter Hasskriminalität im Internet unter Einsatz von Medien mit besonderer Reichweite, insbesondere in Fällen, in denen sich die Tat gegen gesellschaftlich und/oder politisch exponierte Personen richtet.

Im Rahmen ihrer vorbenannten Zuständigkeiten hat die ZAC NRW umfangreiche Praxiserfahrungen sowohl im Hinblick auf die gegenwärtige Situation der Bekämpfung der digitalen Hasskriminalität gewonnen als auch wesentliche Hemmnisse der Strafverfolgung identifiziert. Diese Stellungnahme zu den Gesetzentwürfen der Fraktionen der CDU/CSU und der SPD sowie der Bundesregierung soll sich daher vor allem auf besonders praxisrelevante Aspekte der gesetzlichen Neuregelung fokussieren.

Die dem Gesetzentwurf zugrundeliegende Zielrichtung der Gewährleistung eines freien Meinungsaustausches im Internet wird ausdrücklich begrüßt. Die insofern vorgestellten Maßnahmen zur Stärkung der materiell-rechtlichen und strafprozessualen Grundlagen für die Strafverfolgung digitaler Hasskriminalität können dazu einen wesentlichen Beitrag leisten.

Nicht Gegenstand dieser Stellungnahme sind alternative Ansätze zur Verbesserung der Bekämpfung digitaler Hasskriminalität. So hätte man als Mindermaßnahme zu einer umfassenden Meldepflicht erwägen können, durch eine funktionale Verbesserung der Strafverfolgung – etwa



durch die Bildung operativer Sondereinheiten von Polizei und Justiz unter Zuweisung auskömmlicher Ressourcen – die Effizienz der Strafverfolgung zu steigern. Ebenso wäre denkbar, durch eine einfachere Zugänglichkeit von Polizei und Justiz in den sozialen Medien und generell im digitalen Raum, Bereitschaft und Möglichkeit der Zivilgesellschaft, relevante Sachverhalte anzuzeigen, zu verbessern. Gegebenenfalls hätte sich eine Meldepflicht in Umsetzung dieser Maßnahmen zur Erreichung des Ziels einer verbesserten Strafverfolgung als entbehrlich erwiesen.

Der fortgeschrittene Gesetzgebungsprozess hat als wesentliches Defizit der bisherigen Rechtspraxis nicht die mangelnde Effektivität der Strafverfolgung, sondern den Umstand, dass *„die Strafverfolgungsbehörden [...] keine Kenntnis von den auf eine NetzDG-Beschwerde hingelöschten strafbaren Inhalten“* erlangen,¹ identifiziert. Daher sind vor allem die beabsichtigte Einführung einer Meldepflicht für Betreiber sozialer Medien im Internet und die begrüßenswerte stärkere Rolle des Bundeskriminalamtes (BKA) bei der Bekämpfung der Hasskriminalität im Internet in den Blick zu nehmen.

2. Organisatorische Aspekte

Hinsichtlich des durch die gesetzlichen Neuregelungen zu erwartenden Arbeitsaufkommens sind die durch den Bundesrat in seiner 988. Sitzung am 27. März 2020 aufgeworfenen Fragen zu den Kosten des Gesetzesvorhabens für die Landesjustizbehörden nach den Erfahrungen der Zentralstelle höchst praxisrelevant.

Insoweit ist zunächst festzustellen, dass das zusätzliche Arbeitsaufkommen nur zu einem Teil durch die bei dem BKA nach den Planungen vorgesehene Zentralstelle für Hasskriminalität aufgefangen werden kann. Die Tätigkeit des BKA soll sich demnach auf die Maßnahmen beschränken, die erforderlich sind, um die zuständige Strafverfolgungsbehörde auf Landesebene festzustellen.² Dementsprechend obliegt mit der weiteren Verfahrensführung bis hin zur Anklageerhebung, Durchführung der Hauptverhandlung und der gegebenenfalls anschließenden Vollstreckung der Großteil der anfallenden Mehrarbeit den Justizbehörden der Länder. Dem trägt der nunmehr vorliegende Gesetzentwurf mit dem vorgesehenen deutlichen Stellenaufwuchs bei den Strafverfol-

¹ Zu vgl. BT-Drs. 19/17741, S. 1 f.

² Zu vgl. BT-Drs. 19/17741, S. 15.



gungsbehörden der Länder Rechnung. Entgegen der Annahme des ursprünglichen Referentenentwurfs des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV), welcher lediglich von geringen Mehrkosten im justiziellen Kernbereich bei den Ländern ausging, sieht der in den Bundestag eingebrachte Gesetzentwurf jährliche Mehrkosten in Höhe von 23.950.000 Euro vor. Diese resultieren aus der Schaffung von 180 neuen Stellen für Staatsanwälte sowie weiteren 75 Richterstellen. Hinzu kommen zehn neue R2-Stellen für Abteilungsleiter in den Staatsanwaltschaften, weitere aufsichtführende Richter bei den Amtsgerichten und Stellen für Vorsitzende Richter bei den Landgerichten. Insgesamt sieht der Gesetzentwurf somit die Schaffung von 265 neuen Stellen innerhalb der Strafjustiz vor.³

Der Stellenansatz unterliegt schon hinsichtlich des Verhältnisses von R1- zu R2-Stellen Bedenken insoweit, als bei den Staatsanwaltschaften regelmäßig je vier Dezernentenstellen eine Abteilungsleiterstelle einzurichten ist. Unberücksichtigt bleiben ferner die erforderlichen Stellen im Rechtspfleger- und Unterstützungsbereich.

Die vorgenommene Bedarfsberechnung basiert auf der Annahme, dass durch die Betreiber der sozialen Plattformen an die neu einzurichtende Zentralstelle des BKA jährlich 250.000 Inhalten gemeldet werden, welche letztlich zu 150.000 zusätzlichen Ermittlungsverfahren bei den Staatsanwaltschaften führen.

Die bei der Berechnung zugrunde gelegten Fallenzahlen könnten nach hiesiger Auffassung jedoch deutlich höher ausfallen. So geht der Gesetzentwurf hinsichtlich des Anbieters Facebook von jährlich 70.000 relevanten Meldungen aus. Zutreffend wird dabei im Gesetzentwurf zunächst festgestellt, dass die von Facebook im Transparenzbericht für das erste Halbjahr 2019 ausgewiesenen Fallzahlen aufgrund der im Vergleich zu anderen Anbietern drastischen Abweichungen nach unten nicht zugrunde gelegt werden können. Der Gesetzentwurf orientiert sich daher hinsichtlich der Zahlen für Facebook an den von dem Anbieter YouTube ausgewiesenen 70.000 Fällen, welche einer künftigen Meldepflicht unterfallen würden. Facebook teilte hingegen öffentlich mit, im ersten Quartal 2019 seien in Deutschland mehr als 160.000 als Hassrede eingestufte Inhalte entfernt worden.⁴ Bei linearer Hochrechnung

³ Zu vgl. BT-Drs. 19/17741, S. 30.

⁴ Zu vgl. Dritter Facebook-Transparenzbericht zum NetzDG, abrufbar unter: <https://about.fb.com/de/news/2019/07/dritter-netzdg-transparenzbericht/>, abgerufen am 26.04.2020.



ergibt sich dementsprechend für das Jahr 2019 ein Fallaufkommen von 640.000 Löschungen. Unter der auch im Gesetzentwurf unterstellten praxisnahen Annahme, dass nur in der Hälfte der Löschvorgänge auch ein möglicherweise strafrechtlich relevanter und eine Meldepflicht auslösender Sachverhalt zugrunde liegt, wäre dementsprechend allein mit Blick auf Facebook von etwa 320.000 potenziell der Meldepflicht unterliegenden Vorgängen auszugehen.

Der Gesetzentwurf nimmt weiterhin an, dass von den prognostizierten 250.000 zu erwartenden Fällen, in denen ein Ermittlungsverfahren eingeleitet werden dürfte, lediglich 150.000 Fälle Arbeitsaufwand und somit Mehrkosten bei den Ländern hervorrufen werden. Dem begegnen aufgrund der hier gewonnen praktischen Erfahrungen Bedenken. In Übereinstimmung mit dem Gesetzentwurf ist zunächst auch aus Sicht der hiesigen Zentralstelle davon auszugehen, dass nicht alle gemeldeten Fälle zu neuen Ermittlungsverfahren bei den Strafverfolgungsbehörden der Länder führen werden. So wird die Prüfung der gemeldeten Fälle regelmäßig ergeben, dass entweder ein Anfangsverdacht nicht festgestellt werden kann oder aber erfolgversprechende Ermittlungsansätze zur Identifizierung des Verfassers des gemeldeten Postings nicht ersichtlich sind. Daraus kann jedoch nicht abgeleitet werden, dass diese Fälle bei der Berechnung der bei den Strafverfolgungsbehörden der Länder anfallenden Mehrarbeit vollständig ohne Beachtung bleiben können. Der Gesetzentwurf lässt insoweit außer Acht, dass ein Vorgang auch in den Fällen, in denen ein Anfangsverdacht nicht besteht oder erfolgversprechende Ermittlungsansätze nicht gegeben sind, durch die Staatsanwaltschaft gegebenenfalls angelegt und der Sachverhalt abschließend juristisch bewertet und entschieden werden muss, § 152 Abs. 2, § 160 Abs. 1, § 170 Abs. 2 StPO.⁵ Letztlich werden mithin alle gemeldeten Fälle, wenn sicherlich auch in Teilen nur in reduziertem Umfang, zu Mehrarbeit auf Seiten der Strafverfolgungsbehörden der Länder führen. Eine vollständige Vernachlässigung der Vorgänge ohne Anfangsverdacht oder erfolgversprechende Ermittlungsansätze bildet die tatsächlichen Arbeitsabläufe bei den Staatsanwaltschaften in der Praxis nur unzureichend ab.

Abzuwarten bleibt weiterhin, welche Konsequenzen für die Praxis sich aus den im Gesetzentwurf vorgesehenen Änderungen im materiellen Recht ergeben werden. Unabhängig von der Meldepflicht liegt es nicht

⁵ Je nach Ausgestaltung der Filterfunktion des Bundeskriminalamtes, dazu unten Abschnitt 3. a).



fern, dass durch die Erweiterung des materiellen Rechts in einer Vielzahl von Fällen Ermittlungsverfahren auf Anzeigen bezüglich bislang nicht strafbarer Sachverhalte einzuleiten sein werden. So soll etwa § 241 StGB auf Tatbestandsebene dahingehend erweitert werden, dass künftig auch die Bedrohung mit einer rechtswidrigen Tat gegen die sexuelle Selbstbestimmung, die körperliche Unversehrtheit, die persönliche Freiheit oder gegen eine Sache von bedeutendem Wert vom Tatbestand erfasst ist.⁶ Demnach werden deutlich mehr Fallkonstellationen dem Bedrohungstatbestand unterfallen. Ergänzend wurde die Bedrohung – insoweit einschränkend – mit einem Verbrechen, das sich gegen ein persönliches Rechtsgut wie das Leben, die sexuelle Selbstbestimmung, die körperliche Unversehrtheit oder die persönliche Freiheit richtet, ausweislich § 3a Absatz 2 Nr. 3 lit. c NetzDG-E in den Katalog der meldepflichtigen Tatbestände aufgenommen. Wesentliche Ausführungen dazu, ob und in welchem Umfang die erhebliche Ausweitung des Anwendungsbereichs des Bedrohungstatbestands Eingang in die Berechnung des zu erwartenden zusätzlichen Arbeitsaufkommens für die Justizbehörden der Länder gefunden hat, finden sich im Gesetzentwurf bislang nicht.

In der praktischen Fallbearbeitung durch die ZAC NRW im Rahmen ihrer Zuständigkeit für die Verfolgung herausgehobener politisch motivierter Hasskriminalität im Internet sind eine Vielzahl von Fallkonstellationen bekannt geworden, in denen die Aufnahme eines Ermittlungsverfahrens wegen Bedrohung gemäß § 241 StGB bislang abzulehnen war, in denen künftig jedoch regelmäßig ein Anfangsverdacht und somit die Voraussetzung für die Einleitung eines Ermittlungsverfahrens gegeben sein könnte. Entsprechend ist auch unter diesem Gesichtspunkt von einem bislang nicht abschließend quantifizierbaren Zuwachs an Ermittlungsverfahren auszugehen.

Die vorgenommene Bedarfsberechnung bei den Strafverfolgungsbehörden der Länder unterliegt auch mit Blick auf die im Gesetzentwurf angesetzten jährlichen Erledigungszahlen im Bereich der Staatsanwaltschaft weiteren Unwägbarkeiten. Der Gesetzentwurf geht davon aus, dass von den aus der Meldepflicht resultierenden Ermittlungsverfahren im Jahr durchschnittlich 800 bis 850 Fälle durch eine Staatsanwältin oder einen Staatsanwalt erledigt werden können. Nach den hiesigen Erfahrungen ist in einer politischen Abteilung bislang von 550 bis 600 jährlich erledigten Verfahren pro Staatsanwalt oder Staatsanwältin auszu-

⁶ Zu vgl. BT-Drs. 19/17741, S. 7.



gehen. Zwar mag materiellrechtlich regelmäßig ein Sachverhalt unterdurchschnittlicher Komplexität vorliegen. Unberücksichtigt bleibt bei dem Fallansatz des Gesetzentwurfs jedoch die hinzutretende technische und rechtliche Komplexität der Ermittlungen im Internet und regelmäßig im Konnex der internationalen Rechtshilfe. Nach den Erfahrungen der Zentralstelle lässt sich der jeweils erforderliche Ermittlungsaufwand nicht allein nach Fallgruppen sachgerecht bemessen.⁷ Denn bei der Bekämpfung der digitalen Hasskriminalität sind regelmäßig computerforensische Spuren auszuwerten und als Beweismittel heranzuziehen. Für den Nachweis der Täterschaft ist indes die jeweilige Deliktskategorie unerheblich. Eine effektivere Strafverfolgung in allen Fällen digitaler Hasskriminalität kann daher nur gelingen, wenn die besonderen Gegebenheiten der computerforensischen Beweisführung umfassend durch Staatsanwaltschaften und Gerichte beachtet werden.

Insoweit lässt der vorliegende Entwurf auch die erheblichen zusätzlichen Aus- und Fortbildungsaufwände unberücksichtigt. Mit der Steigerung des Fallaufkommens digitaler Sachverhalte werden die Landesjustizverwaltungen deutliche Anstrengungen unternehmen müssen, Staatsanwältinnen und Staatsanwälte, Richterinnen und Richter in stärkerem Maße für die Bewertung digitaler Sachverhalte und Beweismittel zu ertüchtigen.

Unabhängig davon, wie der konkrete Mehrbedarf in den Strukturen der Landesjustiz zu beziffern ist, steht jedenfalls fest, dass die künftigen Aufgaben mit dem vorhandenen Personalbestand nicht darstellbar sind und einen umfangreichen Stellenaufwuchs erfordern. Gleichzeitig dürfte auch jenseits der Frage der Verfügbarkeit geeigneter Staatsanwältinnen und Staatsanwälte respektive der Möglichkeit der Einstellung geeigneter Bewerberinnen und Bewerber der Aufbau von Strukturen der Landesjustiz, die eine effektive und verlässliche Strafverfolgung von Hasskriminalität im Internet in diesem Ausmaß sicherstellen, jedenfalls nicht kurzfristig gewährleistet werden können. Bei kurzfristiger Einführung der im Gesetzentwurf vorgesehenen Meldepflicht droht daher ein sprunghafter Anstieg der Verfahrenszahlen, ohne dass bei Polizei und Justiz die personellen Ressourcen zur Bearbeitung dieser Verfahren zur Verfügung stehen.

Daher könnte sich jedenfalls für den Zeitraum, welcher benötigt wird, um den erforderlichen Personalaufwuchs darzustellen, eine konsequente Einführung der Meldepflicht, ausgehend von einer anfänglichen

⁷ Zu vgl. BT-Drucksache 19/17741, S. 30.



Konzentration auf demokratiegefährdende Kerndelikte, empfehlen. Nach den Praxiserfahrungen der Zentralstelle dürften die Kerntatbestände, die den öffentlichen Frieden respektive die öffentliche Sicherheit schützen – vor allem die Tatbestände der Verwendung von Kennzeichen verfassungswidriger Organisationen und der Volksverhetzung – besonders relevant für den Schutz der demokratischen und pluralistischen Gesellschaft sein. Schutzzweck dieser Normen ist im Wesentlichen ein friedliches Zusammenleben im Staat im Sinne eines Zustands der Sicherheit. Die Normen stützen das Bewusstsein der Bevölkerung, in Ruhe und Frieden zu leben und gewährleisten damit eine existenzielle Grundlage der freiheitlichen und demokratischen Gesellschaft. Ist hingegen durch Hassrede im Internet eine Strafnorm verletzt, die den individuellen Rechtsfrieden des Einzelnen schützt, wie etwa die Bedrohung gemäß § 241 StGB, könnte es der durch die Tat geschädigten Person vorbehalten bleiben, selbst darüber zu befinden, ob Strafverfolgung begehrt wird oder nicht. So ist insbesondere auf die Fallkonstellationen hinzuweisen, in denen eine Bedrohung zwar objektiv ernstlich war, aber vom adressierten Individuum subjektiv nicht ernst genommen wurde. In solchen Fällen erscheint eine Meldepflicht nicht erforderlich.

Soweit der Bundesrat in seiner Stellungnahme vom 27.03.2020 eine zehnmonatige Frist für das Inkrafttreten der gesetzlichen Neuregelung einer Meldepflicht vorsieht, dürfte es sich aus Sicht der staatsanwaltlichen Praxis um eine Minimalfrist handeln. In Ansehung der vorausgeführten personellen Mehraufwände, der Vorläufe für die Einstellung und die Ausbildung neuer Assessorinnen und Assessoren dürften binnen zehn Monaten funktionsfähige Strukturen zur Bearbeitung der erheblichen Fallzahlen aus der Meldepflicht nur mit höchsten Anstrengungen zu etablieren sein.

Schließlich weist der Bundesrat zurecht auf das Erfordernis einer Berücksichtigung der Personal- und Sachbedarfe im Polizeibereich hin. Selbst wenn durch die stärkere Rolle des Bundeskriminalamtes die Vorbewertung des Sachverhaltes und die Identifizierung Tatverdächtiger zentralisiert vorgenommen werden, verbleibt der weit überwiegende Teil der Ermittlungsarbeit bei den örtlich zuständigen Polizeibehörden. Auch hier sind die besondere Komplexität digitaler Sachverhalte und die erheblichen Aufwände für die – nach den Erfahrungen der ZAC NRW regelmäßig erforderliche – Auswertung computerforensischer Beweismittel wie Mobiltelefone oder Laptops zu berücksichtigen.



3. Rechtliche Aspekte

a) Aufgaben des Bundeskriminalamts

Die vorliegende Fassung des Gesetzentwurfes bedarf nach hiesiger Einschätzung einer Präzisierung im Hinblick auf die rechtliche Verankerung der Rolle des BKA. Während der Gesetzentwurf einerseits ausführt, „*die Entgegennahme der Meldungen, Zuständigkeitsermittlung und Weiterleitung an die zuständigen Strafverfolgungsbehörden der Länder*“ erfolge „*in Wahrnehmung der Zentralstellenaufgabe des BKA*“⁸ und damit an § 2 BKAG anzuknüpfen scheint, ordnet § 3a Abs. 2 NetzDG-E das Tätigwerden als „*Zentralstelle zum Zwecke der Ermöglichung der Verfolgung von Straftaten*“ in die Reichweite von § 152 Abs. 2, § 160 Abs. 1 StPO ein. Ausweislich der Ausführungen im Gesetzentwurf zu Zielsetzung und Notwendigkeit der Regelungen beschränkt sich die Tätigkeit des BKA im Rahmen der Zentralstellenfunktion zur Unterstützung bei der Verfolgung von Straftaten auf die Maßnahmen, die erforderlich sind, um die zuständige Strafverfolgungsbehörde auf Landesebene festzustellen. Das BKA soll demnach ausdrücklich selber keine Strafverfolgung übernehmen.⁹ In den Ausführungen zu den weiteren Kosten sieht der Gesetzentwurf hingegen unter anderem vor, dass die gemeldeten Inhalte durch das BKA im Rahmen der Zentralstellentätigkeit auf ihre strafrechtliche Relevanz hin überprüft werden sollen.¹⁰ Der Gesetzentwurf stellt somit zwar einerseits ausdrücklich fest, dass das BKA selbst keine Aufgaben der Strafverfolgung übernimmt, beschreibt aber andererseits bei der weiteren Ausdifferenzierung des Aufgabenfeldes polizeiliche Tätigkeiten, welchen regelmäßig ein repressiver Charakter zuzuschreiben ist.

So soll dem BKA die Überprüfung von gemeldeten Fällen auf strafrechtliche Relevanz und die anschließende Identifizierung des Verfassers des verfahrensgegenständlichen Postings durch Abfrage von Bestandsdaten bei Telekommunikations- und Telemediendiensteanbietern obliegen. Eine so ausgestaltete polizeiliche Tätigkeit könnte, auch vor dem Hintergrund der auf eine intensivere und effektivere Strafverfolgung zur Bekämpfung des Rechtsextremismus und der Hasskriminalität ausgerichteten Gesamtzielrichtung des Gesetzentwurfs,¹¹ als klassische Maßnahme aus dem Bereich der Strafverfolgung zu qualifizieren sein.

⁸ Zu vgl. BT-Drs. 19/17741, S. 41.

⁹ Zu vgl. BT-Drs. 19/17741, S. 15.

¹⁰ Zu vgl. BT-Drs. 19/17741, S. 29.

¹¹ Zu vgl. BT-Drs. 19/17741, S. 3.



Zutreffend weist der Bundesrat auf den auch hier gesehenen Präzisierungsbedarf hin.¹² Soweit der Bundesrat anregt, zu prüfen, „*ob im Zuge der Präzisierung klargestellt werden kann, dass die zur Entgegennahme der auf Grundlage der Meldepflicht nach § 3a NetzDG-E übermittelten Meldungen zuständige Zentralstelle die Aufgabe hat, lediglich die ihr gemeldeten und nach dortiger Einschätzung strafrechtlich relevanten Inhalte an die zuständigen Strafverfolgungsbehörden zur Ermöglichung der Strafverfolgung weiterzuleiten.*“, bedarf es auch nach hier vertretener Auffassung einer eindeutigen gesetzlichen Regelung.

Denn ihrem materiellen Gehalt nach könnte die Tätigkeit des BKA jedenfalls auch als Maßnahme im Bereich der Strafverfolgung zu qualifizieren sein. Daraus folgt die Notwendigkeit, die dem BKA gemeldeten Fälle zunächst einer materiell-rechtlichen Prüfung auf strafrechtliche Relevanz hin zu unterziehen.¹³ Polizeiliche Maßnahmen im Bereich der Strafverfolgung setzen als notwendige Bedingung einen Anfangsverdacht voraus, § 152 Abs. 2, 160 Abs. 1 StPO. Wenn die Zentralstellen- respektive Filterfunktion des Bundeskriminalamtes demgegenüber weiter verstanden werden soll, bedarf es schon im Hinblick auf eine Abgrenzung zum Anwendungsbereich des Legalitätsprinzips einer ausdrücklichen gesetzlichen Normierung.

Unabhängig von der konkreten Ausgestaltung der Zentralstellen- und Filterfunktion des BKA dürfte sich nach den Erfahrungen der ZAC NRW jedenfalls dessen enge organisatorische Verzahnung mit der Justiz respektive justitiellen Zentralstellen empfehlen. Denn ein erheblicher Teil der zu beurteilenden Sachverhalte erfordert eine umfassende juristische Bewertung. Besonders der Tatbestand der Volksverhetzung zeichnet sich durch komplexe juristische Fragestellungen aus und verlangt mit Blick der besonderen Bedeutung des Grundrechts auf Meinungsfreiheit für das demokratische Gemeinwesen regelmäßig eine präzise Einzelfallprüfung unter Berücksichtigung des Gesamtkontextes. Bereits die Einleitung eines Ermittlungsverfahrens tangiert den demokratischen Diskurs und kann für die betroffene Person eine erhebliche

¹² Zu vgl. BT-Drs. 19/18470, S. 26 f.

¹³ Zu vgl. S. 9 der Stellungnahme des Bundesdatenschutzbeauftragten zum Referentenentwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität vom 16.01.2020, abrufbar unter: https://www.bfdi.bund.de/DE/Infothek/Transparenz/Stellungnahmen/2020/Gesetz_Bekämpfung_Hasskriminalität_BReg.html, abgerufen am 26.04.2020.



Belastung darstellen. Sie setzt deshalb eine sorgfältige juristische Prüfung voraus, die nicht pauschal allein der Polizei zugewiesen werden sollte.

b) Organisatorische Abläufe

Die Überprüfung des für die Einleitung eines Ermittlungsverfahrens konstitutiven Anfangsverdachts fällt in den originären Aufgabenbereich der Strafverfolgungsbehörden und sollte mit Blick auf die grundrechtliche Schutzfunktion strafprozessualer Verfahrensvoraussetzungen keinesfalls auf Private - etwa Beschäftigte in den Löschzentren der sozialen Plattformen - ausgelagert werden. Dementsprechend verbietet sich aus hiesiger Sicht eine beim BKA durch Eingang der Meldung seitens der Anbieter der sozialen Plattformen automatisiert ausgelöste Abfrage von Daten bei Telekommunikations- und/oder Telemediendiensteanbietern. Die rechtliche Einordnung der gemeldeten Postings durch die Meldenden kann die Überprüfung des Vorliegens eines Anfangsverdachts durch die Strafverfolgungsbehörden nicht ersetzen. Nur wenn die materiell-rechtliche Prüfung durch die Strafverfolgungsbehörden das Vorliegen eines Anfangsverdachts ergibt, können weitere Ermittlungsmaßnahmen zur Identifizierung des Verfassers des gemeldeten Postings im Wege der Abfrage von personenbezogenen Daten einen verhältnismäßigen Eingriff insbesondere in das Grundrecht auf informationelle Selbstbestimmung des jeweiligen Nutzers darstellen. In Ansehung der grundrechtlichen Sensibilität wird auch die öffentliche Akzeptanz der gesetzlichen Neuregelung dabei umso stärker ausfallen, je deutlicher sie Transparenz und Verhältnismäßigkeit vermittelt.

c) Digitalisierung

Besonders hervorzuheben ist die vollständige Digitalisierung der Verfahrensweisen und Abläufe als zwingende Voraussetzung für eine zeitgerechte und wirksame Strafverfolgung. Nach den Erfahrungen der hiesigen Zentralstelle lassen sich über die Digitalisierung erhebliche Ressourcenoptimierungen erzielen, so dass es sich anbietet, die im Gesetzentwurf gemäß § 3a Absatz 5 NetzDG-E vorgesehenen Schnittstellen im Sinne einer umfassenden Cloudinfrastruktur auszugestalten. Mit einer Stärkung des BKA als Betreiber der Meldeinfrastruktur ist überdies die technische Grundlage gesichert und gleichzeitig die Möglichkeit eröffnet, eine möglichst frühzeitige Einbindung der Justiz zu gewährleisten.



d) Quick Freeze

Das rechtliche Erfordernis einer Überprüfung jedes gemeldeten Einzelfalls auf strafrechtliche Relevanz steht im Spannungsverhältnis zu der praktischen Herausforderung, die Einhaltung der rechtlichen Vorgaben bei einer Vielzahl von zu erwartenden Meldungen zu gewährleisten. Erschwerend kommt diesbezüglich hinzu, dass mangels Mindestspeicherfristen eine Abfrage der Daten zu den durch die sozialen Plattformen übermittelten IP-Adressen bei den Telekommunikationsanbietern nur innerhalb eines Zeitraums von wenigen Tagen Aussicht auf Erfolg verspricht. Als Lösungsansatz könnte sich ein bislang im Gesetzentwurf nicht vorgesehenes, im Dialog mit Vertretern der Zivilgesellschaft durch die hiesige Zentralstelle jedoch bereits diskutiertes sogenanntes Quick-Freeze-Verfahren¹⁴ erweisen. Denkbar wäre etwa, dass das BKA unmittelbar nach Eingang der Meldung seitens eines sozialen Netzwerks zu der zugehörigen IP-Adresse eine automatisierte Aufforderung an den entsprechenden Telekommunikationsanbieter übermittelt, woraufhin dieser die relevanten Daten zu der übermittelten IP-Adresse „einzufrieren“ hat. Sodann wird der gemeldete Inhalt auf seine strafrechtliche Relevanz hin überprüft und nur für den Fall, dass eine solche auch tatsächlich festgestellt werden kann, werden die zuvor gesicherten Daten durch das BKA bei dem Telekommunikationsanbieter tatsächlich angefordert.

Aufgrund der hohen Anzahl der zu erwartenden Meldungen wird dies zur Folge haben, dass künftig Daten von Nutzern bei den Telekommunikationsanbietern länger als bisher vorgehalten werden müssen. Im Vergleich zu einer umfassenden sogenannten Vorratsdatenspeicherung geschieht dies jedoch in einem deutlich reduzierteren Umfang und nicht anlasslos. Eine längere Speicherzeit erfolgt nur für solche Daten, welche den IP-Adressen der durch die sozialen Plattformen gemeldeten Inhalte zuzuordnen sind. Die grundrechtliche Eingriffsintensität ist demnach deutlich unterhalb der Schwelle einer umfassenden Vorratsdatenspeicherung anzusiedeln. Da auf diese Weise gewährleistet werden könnte, dass Daten bei den Telekommunikationsanbietern nur zu Vorgängen mit strafrechtlicher Relevanz abgefragt werden, bestehen seitens der Zentralstelle im Hinblick auf die grundrechtsrelevante Eingriffsintensität verfassungsrechtliche Bedenken nicht.

¹⁴ Zu vgl. S. 20 f. der gemeinsamen Stellungnahme der zivilgesellschaftlichen Organisationen ichbinhier e.V. und HateAid gGmbH zum Referentenentwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes des BMJV, abrufbar unter: https://www.ichbinhier.eu/wp-content/uploads/2020/02/200217_Stellungnahme-ichbinhier-HateAid-NetzDG.pdf, abgerufen am 26.04.2020.



4. Über den Gesetzentwurf hinausgehende Aspekte

Der Gesetzentwurf nimmt mit der Einführung einer Meldepflicht *ein* Instrumentarium für die effektivere Bekämpfung der Hasskriminalität im Internet in den Blick. Er lässt indes andere, nicht minderbedeutende Ansatzpunkte für eine effektivere Strafverfolgung außer Acht.

Nach den Erfahrungen der ZAC NRW erweist sich vor allem das Auskunftsverhalten der Diensteanbieter als wesentliches Ermittlungshemmnis. Vor dem Hintergrund der unbestrittenen Komplexität der Rechtslage im internationalen Kontext der regelmäßig nicht in der Bundesrepublik ansässigen Diensteanbieter scheitert die Mehrzahl von Ermittlungsverfahren nicht am Fehlen einer Meldung respektive Strafanzeige, sondern an für die Identifizierung und Verfolgung von Tätern relevanten, indes nicht erteilten Auskünften der Anbieter. Die Strafverfolgungsbehörden sehen sich regelmäßig auf die internationale strafrechtliche Rechtshilfe verwiesen, die jedoch mit Blick auf die kurzen inländischen Speicherfristen ohne Vorratsdatenspeicherung und die durchschnittlich mehrmonatige Laufzeit solcher Ersuchen wenig erfolgversprechend ist.

Im Rahmen einer – nicht repräsentativen – statistischen Auswertung von mehr als 400 Vorgängen der ZAC NRW, die nicht zur Ermittlung tatverdächtiger Personen geführt haben, hat fast die Hälfte der bei der ZAC NRW eingegangenen Strafanzeigen für die Einleitung eines Ermittlungsverfahrens mangels Anfangsverdachts keine Veranlassung gegeben. Umgekehrt bedurfte es in den wegen Anfangsverdachts eingeleiteten Ermittlungsverfahren in fast jedem Fall der Mitwirkung der Anbieter sozialer Netzwerke.

Die durch die Anbieter sozialer Netzwerke nach § 5 Abs. 2 Satz 1 NetzDG zu bestellende empfangsberechtigte Person im Inland spielt in der Praxis der Auskunftersuchen keine nennenswerte Rolle. Denn die Zentralstelle ist jedenfalls bei den US-amerikanischen Plattformen in die jeweiligen elektronischen Auskunftsportale eingebunden. Die Auskunftssachverhalte werden daher schon aus Beschleunigungsgründen regelmäßig im unmittelbaren Geschäftsverkehr bearbeitet.

Soweit Ersuchen an US-amerikanische Plattformbetreiber erforderlich und sachgerecht waren, richteten sie sich im Wesentlichen an Twitter (69 % der Fälle), außerdem an Facebook (14 %), Google (14 %) und VKontakte (3 %).



Inhaltlich beantwortet wurden die Ersuchen vollumfänglich von Google, nur gelegentlich von Facebook. Im Übrigen sind die Ersuchen ergebnislos geblieben. Insgesamt wurde nur jedes zwanzigste Ersuchen mit Daten beauskunftet.

Das Problem des unter Hinweis auf die Rechtshilfesituation defizitären Auskunftsverhaltens der Anbieter sozialer Netzwerke und von Onlineplattformen ist bislang ungelöst. § 5 Absatz 2 Satz 2 NetzDG sieht beispielsweise eine lediglich formale Auskunftsverpflichtung der empfangsberechtigten Person sozialer Netzwerke binnen 48 Stunden vor. Eine inhaltliche Auskunft ist nicht vorgeschrieben und wird von der Mehrzahl der Netzwerke – wie ausgeführt – regelmäßig nicht erteilt. Ohne eine Pflicht zur umfassenden inhaltlichen Beauskunftung von Ersuchen der Strafverfolgungsbehörden unter Zugrundelegung des Marktortprinzips steht zu besorgen, dass die auch bei Einführung der Meldepflicht in zahlreichen Fällen weiterhin erforderlichen Auskünfte der sozialen Netzwerke sich als fortdauerndes und wesentliches Hemmnis der Strafverfolgung erweisen werden.

Mit Blick auf den Gesetzentwurf der Bundesregierung eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes (NetzDGÄndG-E)¹⁵ und die dort vorgenommenen Anpassungen des Gesetzes an unionsrechtliche Vorgaben (zu vgl. etwa § 3e NetzDGÄndG-E) zum Herkunftslandprinzip im Sinne des Art. 3 ECRL dürfte sich jedenfalls empfehlen, die Kapazitäten der internationalen strafrechtlichen Rechtshilfe nachhaltig zu erhöhen und nachdrücklich auf eine europäische Vereinheitlichung und Vereinfachung der Rechtsgrundlagen hinzuwirken.

Mit Besorgnis sieht die Zentralstelle erste Verdrängungseffekte einer stärkeren Ausübung des „digitalen Hausrechts“ durch die Plattformbetreiber und einer verstärkten Strafverfolgung. Manche strafrechtlich relevante Kommunikation verlagert sich bereits jetzt in soziale Medien, deren Bereitschaft zur Kooperation mit den Strafverfolgungsbehörden noch erheblich geringer ausgeprägt ist als bei US-amerikanischen Unternehmen und deren Herkunftsländer für Rechtshilfemaßnahmen deutscher Strafverfolgungsbehörden nur sehr eingeschränkt erreichbar sind.

¹⁵ Abrufbar unter https://www.bmjjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_Aenderung_NetzDG.pdf, abgerufen am 27.04.2020.



Hier ein wirkungsvolles Strafverfolgungsinstrumentarium zu etablieren, dürfte auch unter Geltung der Meldepflicht für strafbare Inhalte in sozialen Medien eine fortdauernde Herausforderung für die Ermittlungsbehörden bleiben.

Köln, 04.05.2020

gez. Hartmann
Oberstaatsanwalt als Hauptabteilungsleiter
Leiter der ZAC NRW



Stellungnahme zur Anhörung des Ausschusses Recht und Verbraucherschutz zum „Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität“ am 06. Mai 2020

Berlin, 05. Mai 2020

Mit dem Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (BT-Drucksache 19/17741) der Fraktionen von CDU/CSU und SPD liegen dem Bundestag nun Pläne vor, die weit über die zuvor diskutierte Stärkung des Netzwerkdurchsetzungsgesetzes (NetzDG) hinausgehen. Neben einer Ausweitung des NetzDG in Form einer Meldepflicht für die Betreiber sozialer Netzwerke enthält der Gesetzentwurf u.a. Neuregelungen in der Strafprozessordnung (StPO) und dem Telemediengesetz (TMG) zur Herausgabe von Bestands- und Nutzungsdaten sowie Passwörtern an zuständige Behörden. Auf Basis der vorgeschlagenen Änderungen drohen zum Teil tiefgreifende Einschnitte in das informationelle Selbstbestimmungsrecht gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz (GG), in das Recht auf Gewährleistung der Vertraulichkeit und Integrität von Kommunikationssystemen nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sowie in das Fernmeldegeheimnis nach Art. 10 GG aller Bürger.

eco – Verband der Internetwirtschaft e.V. bekennt sich zum Kampf gegen Rechtsextremismus und unterstützt das Vorgehen gegen rechtswidrige Inhalte im Internet. Dazu betreibt eco u.a. eine Beschwerdestelle zur Bekämpfung rechtswidriger Inhalte im Internet. Nach Einschätzung der Internetwirtschaft bestehen hinsichtlich des Gesetzentwurfes erhebliche verfassungsrechtliche, datenschutzrechtliche und europarechtliche Bedenken, die eco bereits im Januar 2020 in einer Stellungnahme¹ an das Bundesministerium für Justiz und Verbraucherschutz adressiert worden sind. Diese Bedenken hat eco im Zuge einer Kommentierung des Notifizierungsverfahrens ([2020/65/D](#)) ebenfalls an die Europäische Kommission gerichtet.

▪ Einführung neuer Auskunftspflichten für Telemediendiensteanbieter

Um eine vermeintlich effektivere Strafverfolgung und Rechtsdurchsetzung für rechtswidrige Inhalte im Internet zu erreichen, soll eine umfangreiche Auskunftspflicht über Nutzungs- und Bestandsdaten potentiell tatverdächtiger Nutzer für die Strafverfolgungs- und Sicherheitsbehörden gegenüber Telemediendiensteanbietern geschaffen werden. Auf Grundlage der Auskunftspflicht werden personenbezogene Daten z.B. Informationen zum Nutzungsverhalten von Nutzern in erheblichen Umfang an die berechtigten Behörden herausgegeben.

Unter Maßgabe von §§ 100g, 100j StPO i.V.m. § 15a TMG wird eine weitreichende Rechtsgrundlage zur Identifizierung von Nutzern im Internet für Ermittlungs- und Strafverfolgungsbehörden geschaffen, die für alle Telemediendiensteanbieter gilt und

¹Stellungnahme des eco zum Referentenentwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität vom 17. Januar 2020
https://www.eco.de/wp-content/uploads/2020/01/20200117_eco-stn-zum-gesetz-zur-bekaempfung-von-rechtsextremismus-und-hasskriminalitaet-1.pdf



damit erheblich über die diskutierten Maßnahmen zur Stärkung des NetzDG hinausgehen. Im Ergebnis wird die vorgeschlagene Ausweitung der bestehenden Auskunftspflichten auf Telemediendiensteanbieter zu einer breiten Betroffenheit bei den Telemediendiensteanbietern führen.

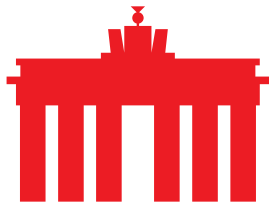
In Bezug auf die Beauskunftung von Bestandsdaten durch die Telemediendiensteanbieter gem. § 100j Abs. 1 S. 1 StPO sind weitere Differenzierungen aus Sicht des eco unerlässlich. Es ist nicht sachgerecht, eine Norm für Telemediendiensteanbieter zu schaffen, die schlicht dem Telekommunikationsgesetz (TKG) nachgebildet ist. Entsprechende Regelungen sind aufgrund des hohen Grads an Standardisierung sowie der hohen Normierungsdichte im Telekommunikationssektor nicht ohne weiteres auf den Telemedienbereich übertragbar. Entgegen der Charakteristika im TKG ist zu beachten, dass bei Telemediendiensten eine hohe Anzahl von Unternehmen betroffen sind. Eine Ersteinschätzung des eco zeigt, dass in Deutschland rund 2,3 Millionen Unternehmen als geschäftsmäßige Anbieter von Telemedien gelten, die von der Regelung betroffen sind. Zudem gilt es bei Telemediendiensten zu beachten, dass deren Anwendung, im Gegensatz zu Telekommunikationsanbietern, auf einer heterogenen technischen Landschaft basieren und deshalb auch unterschiedliche Formen von Informationen verarbeiten. Vor dieser Ausgangslage scheint es zweifelhaft, ob die Einführung von Auskunftspflichten für alle Betreiber von Telemediendiensten ohne sachgerechte Anpassungen für unterschiedliche Arten von Telemediendiensten, Geschäftsmodellen und betrieblichen Abläufen sowie unter Berücksichtigung ihres technischen Aufbaus, nicht zu weit greifen.

Zwar schafft der Gesetzgeber mit dem vorgelegten Gesetzesentwurf einige notwendige Differenzierungen in Bezug auf die rechtlichen Anforderungen zur Herausgabe von Bestands- und Nutzungsdaten sowie von Passwörtern, dies täuscht jedoch nicht darüber hinweg, dass die Herausgabe von Bestands- und Nutzungsdaten im Sinne von Art. 16 i.V.m. Art 52 EU-Grundrecht-Charta unverhältnismäßig ist. Der vorgesehene und weit gefasste Adressatenkreis der Auskunftspflicht steht nur in geringem Ausmaß im Zusammenhang mit den angesprochenen Delikten und ist somit nicht auf das absolut Notwendige zu deren Bekämpfung begrenzt.

▪ **Herausgabe von Passwörtern durch Telemediendiensteanbieter**

Neben der Herausgabeverpflichtung von Bestands- und Nutzungsdaten durch die Telemediendiensteanbieter sollen auf Grundlage von § 15b TMG auch Daten von Telemediendiensteanbietern herausgegeben werden, mit deren Hilfe auf Endgeräte oder Speicher zugegriffen werden kann, also insbesondere Passwörter. Zur Bereitstellung der Informationen sollen Telemediendiensteanbieter sämtliche unternehmensinternen Daten heranziehen.

eco kritisiert den Vorschlag eines § 15b TMG scharf. Mit dem Vorschlag greift der Gesetzgeber tief in die Nutzerrechte und die Privatsphäre von Nutzern ein, zudem werden Telemediendiensteanbieter mit weiteren Belastungen konfrontiert, die möglicherweise die Sicherheit der IT-Systeme gefährden. Mit dem Gesetzesentwurf der Regierungsparteien ist klargestellt worden, dass die Herausgabe von Passwörtern nur bei besonders schweren Straftaten, zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung und zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person unter Vorliegen einer richterlichen Anordnung

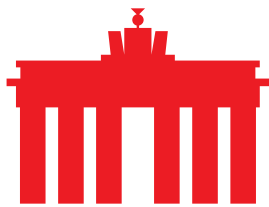


zulässig ist. Dabei soll eine etwaig bestehende Verschlüsselung entsprechender Angaben unberührt bleiben. Trotz der vorgenommenen Klarstellung und Eingrenzungen bestehen noch immer ungeklärte Fragen und die Regelung bleibt hoch problematisch.

Die Herausgabe von Passwörtern ermöglicht Ermittlungs- und Strafverfolgungsbehörden den Zugriff auf Online-Konten und damit auf die digitale Identität der Nutzer. Mit diesen Daten werden umfangreiche Onlinedurchsuchungen ermöglicht, einschließlich des Zugriffs auf Kommunikationsinhalte z.B. E-Mails, in der Cloud hinterlegte Fotos, Dokumente Chat- und Messengernachrichten. Im Ergebnis wird auf Grundlage der Rechtsanpassung ein Eingriff und somit auch eine Einschränkung des Kernbereiches der privaten Lebensgestaltung der Nutzer möglich. Dieser Eingriff betrifft nicht nur den angefragten Nutzer, sondern bei mehrseitigen Kommunikationen auch Dritte, die in der Regel keinen Anlass für die Datenherausgabe gegeben haben. Der Gesetzgeber hat den Gesetzesentwurf zwar dahingehend angepasst, dass die Herausgabe nur unter Maßgabe eines Verdachts besonders schwerer Straftaten erfolgen darf, jedoch bleibt die Verhältnismäßigkeit der Norm aufgrund des breiten Adressatenkreises und der umfassenden Eingriffstiefe zweifelhaft. § 15b TMG führt eine Reihe an Behörden und Stellen an, die befugt sind, entsprechende Anfragen an die Telemediendiensteanbieter zu stellen.

Zudem ist es bedenklich, dass die Herausgabe von Informationen mit deren Hilfe auf Speicher des Telemediendienstes sowie auf Speicher und Endgeräte der Nutzer zugegriffen werden kann, auch ein sicherheitskritisches Problem für die Anbieter von Telemediendiensten darstellt. Die Passwörter der Nutzer dürfen aus Sicherheitsgründen u.a. wegen des Datenschutzes nur verschlüsselt gespeichert werden, so dass diese nicht unmittelbar für den Anbieter einsehbar sind. Der Gesetzesentwurf stellt klar, dass die Passwörter nicht unverschlüsselt gespeichert und herausgegeben werden müssen, jedoch bleibt unklar, inwieweit eine Verpflichtung für die Telemediendiensteanbieter z.B. E-Mailprovider, Social-Media-Plattformen und Internetforen, aus der Heranziehung aller im Unternehmen verfügbarer Daten abgeleitet werden kann, die anfragenden Behörden bei der Entschlüsselung der Passwörter durch die Bereitstellung der Verschlüsselungsverfahren zu unterstützen. Aus Gründen der IT-Sicherheit, des Datenschutzes sowie des Grundrechts auf Vertraulichkeit der Kommunikation wäre eine solche Verpflichtung der Telemediendiensteanbieter fatal. In diesem Zusammenhang bedarf es darüber hinaus der weiteren Diskussion, ob die Anbieter von Telemediendiensten grundsätzlich imstande wären, entsprechende Auflagen zur Offenlegung der Verfahren und Passwörter zu erfüllen, und unter welchen Bedingungen solche Anforderungen überhaupt grundrechtskonform wären. Eine Mitwirkungspflicht für Anbieter von Telemediendiensten bei der Entschlüsselung von Passwörtern bzw. bei der Bereitstellung von Informationen zum Entschlüsseln oder Zurücksetzen von Passwörtern ist in jedem Fall abzulehnen.

Mit der Schaffung von § 15b TMG geht ein erheblicher administrativer Aufwand für die Telemediendiensteanbieter einher. Gemäß Abs. 4 der Vorschriften ist die Prüfung zur Rechtmäßigkeit der Passwortabfrage durch entsprechendes Fachpersonal durchzuführen. Gerade für kleine und mittelständisch geprägte Anbieter von Telemediendiensten stellt der damit verbundene technische, organisatorische und personelle Erfüllungsaufwand eine enorme finanzielle Belastung dar. Weiterhin lässt der Gesetzesentwurf offen, ob den Diensteanbietern mögliche Mitwirkungspflichten bspw. bei der Identifizierung oder Zusammenführung von Daten obliegt.



Grundsätzlich sollte der Erfüllungsaufwand jener Verpflichtungen nicht zulasten der Unternehmen gehen.

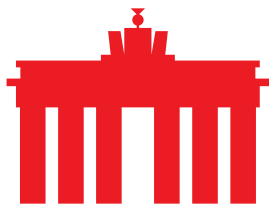
▪ **Einführung einer Meldepflicht für die Betreiber sozialer Netzwerke**

Das NetzDG soll mit dem vorliegenden Gesetzesentwurf um eine Meldepflicht für die Betreiber sozialer Netzwerke zur effektiven Bekämpfung von Rechtsextremismus und Hasskriminalität ausgeweitet werden. Die Einführung einer Meldepflicht in § 3a NetzDG bei den Betreibern sozialer Netzwerke für die Inhalte aus dem Beschwerdeverfahren ist in mehrfacher Hinsicht kritisch zu bewerten.

Gemäß dem Anwendungsbereich von § 3a NetzDG sollen auch kinderpornographische bzw. Kindesmissbrauchsinhalte der Meldepflicht unterliegen. Aus dem Betrieb der Beschwerdestelle beim eco ist anzumerken, dass zur Eindämmung von Kindesmissbrauchsinhalten bereits eine zentrale Stelle beim Bundeskriminalamt (BKA) existiert. Um eine effektive Eindämmung kinderpornografischer bzw. Kindesmissbrauchsinhalten mit der Einführung der Meldepflicht sicherzustellen, müssen die Zuständigkeiten beim BKA im Voraus geklärt und den Betreiber sozialer Netzwerke mitgeteilt werden. Darüber hinaus sollte eine Meldepflicht für jene Inhalte den generell bestehenden Bemühungen Rechnung tragen. So erhält z.B. das BKA schon heute zumindest von den amerikanischen Plattformanbietern / sozialen Netzwerken über eine Kooperation mit dem amerikanischen Center for missing and exploited children (NCMEC) Meldungen zu Kindesmissbrauchsinhalten, sofern es deutsche Tatverdächtige gibt. Darauf aufbauend ist bei der Ausgestaltung der Meldepflicht darauf zu achten, dass mögliche Doppelmeldungen aus den unterschiedlichen Meldesträngen vermieden werden, auch um eine effektive Strafverfolgung sicherzustellen.

Mit der Einführung einer Meldepflicht im NetzDG werden die Betreiber sozialer Netzwerke dazu verpflichtet Inhalte und Angaben zur Nutzeridentifizierung z.B. IP-Adresse und Portnummer proaktiv an das BKA auszuleiten. eco wertet es kritisch, dass bereits mit der Meldung an das BKA die vorstehenden Informationen zugänglich gemacht werden, obwohl kein konkreter Anfangsverdacht durch die jeweils zuständige (Ermittlungs-)Behörde geprüft worden ist. Die ordnungsgemäße Umsetzung der Meldepflicht führt bei den Betreibern sozialer Netzwerke insbesondere bei denen mit Sitz im Ausland zu zahlreichen rechtlichen Schwierigkeiten im Hinblick auf geltendes EU-Recht z.B. Datenschutzgrundverordnung und E-Commerce Richtlinie, Gesetze im Land der europäischen Niederlassung, Rechtsvorschriften des Heimatstaates und internationale Verträge.

Nach Einschätzung des eco verstößt die Meldepflicht gem. § 3a NetzDG in der bisher diskutierten Ausgestaltung gegen geltendes EU-Recht, u.a. gegen die E-Commerce Richtlinie (2000/31/EG). Die Betreiber sozialer Netzwerke sollen, ungeachtet ihres europäischen Niederlassungsstaates, zur Ein- und Vorhaltung von Prüfungs- und Meldepflichten nach deutschem Recht verpflichtet werden. Derartige Entwicklungen stehen nicht im Einklang mit dem Herkunftslandprinzip nach Art. 3 der Richtlinie. Des Weiteren gestattet Art. 15 Abs. 2 2. Halbsatz der Richtlinie den Mitgliedstaaten mögliche Vorschriften zu erlassen, in deren Folge zuständige Behörden auf Verlangen Informationen zur Nutzeridentifikation erhalten können. § 3a Abs. 4 Nr. 2 NetzDG konstituiert dem widersprechend eine Meldepflicht, ohne dass



es ein konkretes Verlangen zur Ermittlung des Nutzers im Einzelfall der zuständigen Behörde, gibt.

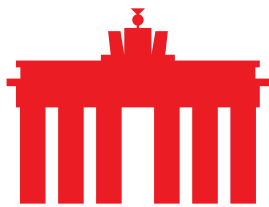
Zudem sind mit der Einführung der Meldepflicht im NetzDG zahlreiche Verstöße gegen die Datenschutzgrundverordnung (EU) 2016/679 und gegen die Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung zu erwarten. Mit der Meldepflicht werden die Betreiber sozialer Netzwerke auf Grundlage deutscher Rechtsvorschriften zur Herausgabe personenbezogener Daten verpflichtet, wovon auch Nutzern aus dem europäischen Ausland betroffen sein können. Demzufolge besteht die Möglichkeit, dass auch Inhalte, IP-Adressen und Portnummern von Personen außerhalb der Bundesrepublik Deutschland übermittelt werden. Im Ergebnis werden zahlreiche personenbezogene Daten von Personen aus dem (EU-)Ausland an deutsche Strafverfolgungsbehörden übermittelt, deren Herausgabe nicht von einer europäischen Rechtsgrundlage abgedeckt ist. Die Betreiber sozialer Netzwerke erwarten infolge der Meldepflicht zahlreiche Konflikte mit den europäischen Datenschutzbehörden, in deren Folge die deutschen Strafverfolgungsbehörden zur Löschung der Nutzerdaten aufgefordert werden.

Bereits zur Implementierung des Beschwerdeverfahrens haben die Betreiber sozialer Netzwerke große Anstrengungen und Investitionen unternommen, um die notwendigen rechtlichen, technischen und organisatorischen Vorkehrungen zu treffen. Dabei haben die Unternehmen auch Verfahren und Organisationsprozesse zur Bearbeitung von Anfragen der Strafverfolgungsbehörden etabliert. Dies gilt sowohl für im Inland ansässige Anbieter, als auch für Anbieter mit Sitz in einem anderen Staat. Zur Beauskunftung stellen die Betreiber sozialer Netzwerke sog. Law-enforcements Portale für die Auskunftserteilung und –abwicklung zur Verfügung, durch deren Einsatz die anfragenden Behörden schnell, effektiv und verschlüsselt Daten abfragen können. Die Nutzung dieser Portale hat sich bewährt und sollte künftig fortbestehen. Die betroffenen Anbieter von sozialen Netzwerken und Plattformen beauskunfteten auf freiwilliger Basis die durch die Strafverfolgungsbehörden angefragten Daten ohne dass die Behörden auf internationale Rechtshilfeersuchen (MLAT-Verfahren) verwiesen werden. Dabei sind Mindeststandards zu berücksichtigen, die für die Anfrage erfüllt sein müssen, um nicht im Heimatland der Betreiber für eine widerrechtliche Datenherausgabe in die Haftung genommen zu werden.

In Anlehnung an die Gesetzesbegründung geht der Gesetzgeber davon aus, dass ein dreimonatiges Zeitfenster für die Umsetzung der Meldepflicht gem. NetzDG auf Seiten der beteiligten Behörden und der betroffenen Unternehmen als erforderlich und ausreichend zu werten ist. Diese Einschätzung teilt eco nicht und spricht sich dafür aus, dass die Betreiber sozialer Netzwerke eine angemessene Umsetzungsfrist erhalten, um die technischen Anforderungen und personellen Vorkehrungen hinsichtlich der Meldepflicht im NetzDG treffen zu können.

▪ **Datenspeicherung beim Bundeskriminalamt**

Mit der Einführung einer Meldepflicht für die Betreiber sozialer Netzwerke an das BKA wird binnen kurzer Zeit eine umfangreiche Datenbank zu gemeldeten Inhalten und potentiell tatverdächtigen Nutzer beim BKA entstehen. Nach Auffassung des eco gilt es als bedenklich, dass der Gesetzesentwurf keine eindeutigen Vorgaben



zur Verarbeitung, Speicherung und Vernichtung der aus der Meldepflicht erlangten Daten beim enthält. Lediglich die Gesetzesbegründung stellt klar, dass die aus der Meldepflicht erhobenen Daten nach der Erfüllung des Normzwecks zu löschen sind. Aufgrund der fehlenden Rechtsetzung erwachsen Risiken zum Umgang mit den massenhaft auflaufenden Datensätzen und über die Befugnisse der Ermittlungsbehörden. So ist nicht abschließend klargestellt, ob und wie die aus der Meldepflicht erlangten Datensätze für weitere Ermittlungen verwendet bzw. zur Klärung anderer Delikte herangezogen werden dürfen. Deshalb ist es zwingend erforderlich, dass die Anforderungen an den Datenumgang und vor allem an das Löschen der Datensätze durch das BKA vor der Einführung der Meldepflicht im NetzDG umfassend und rechtssicher gesetzlich festgeschrieben werden.

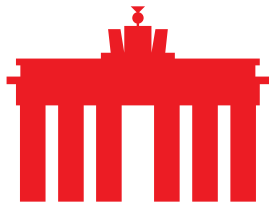
▪ **Mangelnde rechtstaatliche Kontrollmechanismen**

Die Herausgabepflicht für Passwörter, Bestands- und Nutzungsdaten, IP-Adressen und Portnummern würde im Falle der Verabschiedung des Gesetzesentwurfs weitgehend ohne hinreichende rechtstaatliche Sicherungs- und Kontrollmechanismen, wie etwa einen Richtervorbehalt oder strenge Gefahr in Verzug Regeln, erfolgen. Die mit dem Entwurf einforderbare Herausgabe von sensiblen Nutzerdaten ist vor dem damit einhergehenden Eingriff in das allgemeine Persönlichkeitsrecht und das Fernmeldegeheimnis der einzelnen Nutzerinnen und Nutzer mehr als fragwürdig.

▪ **Europäischer Gemeinschaftsstandard zur Bekämpfung rechtswidriger Inhalte im Internet**

Bei einem Vergleich der rechtlichen Situation in Europa wird deutlich, dass die Bundesrepublik Deutschland frühzeitig mit der Einführung des NetzDG einen regulatorischen Alleingang in Europa gewagt hat. Mit der Stellungnahme C(2019)8585 final) vom 22.11.2019 hat die Europäische Kommission bei den Ausführungen zur Notifizierung des französischen Gesetzgebungsverfahrens zur Bekämpfung von Hassinhalten im Internet angekündigt, dass ein europäischer Rechtsakt zu dieser Rechtsfrage im Rahmen des Digital Services Act angestrebt ist. Letztlich bittet die EU-Kommission die Französische Republik darum, dass nationale Gesetzgebungsverfahren auszusetzen. Unter Maßgabe dieser Ausgangssituation bleibt unklar, warum die Bundesrepublik Deutschland gleich zwei Gesetzgebungsverfahren zur Ausweitung bzw. Überarbeitung des NetzDG vorgelegt hat, anstatt sich auf Grundlage der bisherigen Erfahrung mit dem NetzDG in den europäischen Rechtsetzungsprozess einzubringen. Um das Auseinanderfallen der in diesem Kontext geltenden europäischen Rechtsvorschriften zu verhindern, sollte die Bundesrepublik Deutschland äußerst bedacht handeln.

Über eco: Mit über 1.100 Mitgliedsunternehmen ist eco der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, formt Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Leitthemen sind Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen



VERBAND DER INTERNETWIRTSCHAFT E.V.



sowie Ethik und Selbstregulierung. Deshalb setzt sich eco für ein freies, technikneutrales und leistungsstarkes Internet ein.

Uwe Lübking
Beigeordneter

Herrn Prof. Dr. Heribert Hirte; MdB
Vorsitzender des
Ausschusses für Recht und Verbraucherschutz
Paul-Löbe-Haus Konrad-Adenauer-Str. 1
10557 Berlin

Marienstraße 6
12207 Berlin

Telefon: 030-77307-245
Telefax: 030-77307-255

Internet: www.dstgb.de
E-Mail: dstgb@dstgb.de

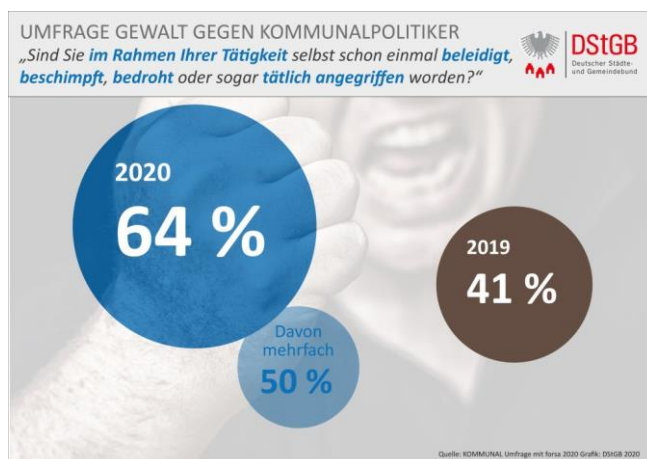
Datum
04.05.2020

Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität - BT-Drucksache 19/17741 und Änderungsantrag 1 (Strafrecht) der Fraktion BÜNDNIS 90/DIE GRÜNEN im 6. Ausschuss zu dem Gesetzentwurf der Fraktionen der CDU/CSU und SPD - Drucksache 19/17741 -

Sehr geehrter Herr Vorsitzender,
sehr geehrte Abgeordnete,

für die Möglichkeit zur Stellungnahme zum o.g. Gesetzesentwurf „Bekämpfung des Rechtsextremismus und der Hasskriminalität“ bedanken wir uns.

Kommunalpolitikerinnen und Kommunalpolitiker wurden und werden in den letzten



Jahren vermehrt beleidigt und bedroht oder sogar körperlich angegriffen. Dies führt nicht zuletzt dazu, dass in der haupt- und ehrenamtlichen Kommunalpolitik darüber nachgedacht wird, ob ein Amt oder Mandat weiter ausgeübt wird oder ob ein Amt überhaupt angestrebt wird. Die Meinungsfreiheit im demokratischen Diskurs ist ein hohes Gut, aber Grenzen müssen da gesetzt werden, wo ehrverletzende Beleidigungen

oder aber demokratiegefährdende Bedrohungen Realität werden. Eine Umfrage der Zeitschrift Kommunal und Forsa im Auftrag von Report München aus diesem Jahr zeigt nochmal, dass die Angriffe, Bedrohungen und Beleidigungen in deutschen Rathäusern leider weiter zunehmen.

Der DStGB begrüßt deshalb ausdrücklich die Intention der Änderungen des Strafgesetzbuches zum besseren Schutz kommunaler Amts- und Mandatsträger, der jedoch aus unserer Sicht nicht ausreichend ist. Es braucht vielmehr einen wirksamen Schutz jenseits der Beleidigungsdelikte. Daher schlagen wir die Einführung eines § 238 a StGB vor, der bestehende Strafbarkeitslücken schließen könnte. Darüber hinaus plädieren wir für eine Änderung des § 36 GVG (Vorschlagslist zur Schöffenvwahl).

Neben den Änderungen der strafrechtlichen Vorschriften müssen diese aber auch konsequent umgesetzt werden. Aus unserer Sicht ist es zwingend notwendig, dass Schwerpunktstaatsanwaltschaften in den Ländern eingerichtet und der Informationsaustausch verbessert wird. Die ZAC NRW (Zentral- und Ansprechstelle Cybercrime) und ZIT Hessen (Zentralstelle zur Bekämpfung der Internetkriminalität) leisten hervorragende Arbeit. Nach diesem Vorbild sollten weitere Schwerpunktstaatsanwaltschaften auch in den anderen Bundesländern eingerichtet werden. Die Staatsanwaltschaften sollten für die besondere Spezifika der Thematik und die organisierte Dimension von Hass im Netz sensibilisiert und geschult werden.

Das Bundesministerium der Justiz und für Verbraucherschutz sollte hier, wie schon im Ergebnispapier zur Task Force „Umgang mit rechtswidrigen Hassbotschaften im Internet“ angekündigt, mit den Ländern den Austausch suchen. Der Beschluss des Bundesrates – BR-Drs. 418/19 vom 29.11.2019 – bildet eine gute Grundlage für weitere Gespräche. Vor diesem Hintergrund begrüßen wir die Änderungen im BKA-Gesetz und im Telemediengesetz, die eine schnellere und effektivere Ermittlung von Urhebern von Beleidigungen und Bedrohungen im Internet ermöglichen sollen.

Neben dem Strafrecht muss auch mehr für die Prävention und den Opferschutz getan werden. In jedem Bundesland sollten, wie es teilweise bereits geschieht, zentrale Anlaufstellen für Betroffene von Hate Speech geschaffen werden, die auf das Themenfeld spezialisiert und damit als Schnittstelle für alle betroffenen Institutionen dienen können. Zentrale Hilfestellen für Betroffene sollten in den sozialen Netzwerken prominent eingebunden werden.

Wir plädieren weiterhin dafür, dass in den Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBv) im Bereich der Beleidigungsdelikte klargestellt wird, dass bei Delikten gegen Beschäftigte im öffentlichen Dienst und Amtsträger in ihrer jeweiligen Funktion grundsätzlich von einem öffentlichen Interesse an der Strafverfolgung auszugehen ist.

Der Vorschlag zu einer grundsätzlichen Reform der Beleidigungsdelikte, wie ihn die Fraktion Bündnis90/Die Grünen basierend auf dem Diskussionsentwurf des Bayerischen Staatsministeriums für Justiz vorschlägt, wird aus Sicht des Deutschen Städte- und Gemeindebundes im Grunde nach begrüßt. Dies würde das bisherige Strafrecht im Bereich der Beleidigungsdelikte übersichtlicher machen

und an die Herausforderungen des Strafrechts im 21. Jahrhundert besser anpassen als punktuelle Änderungen.

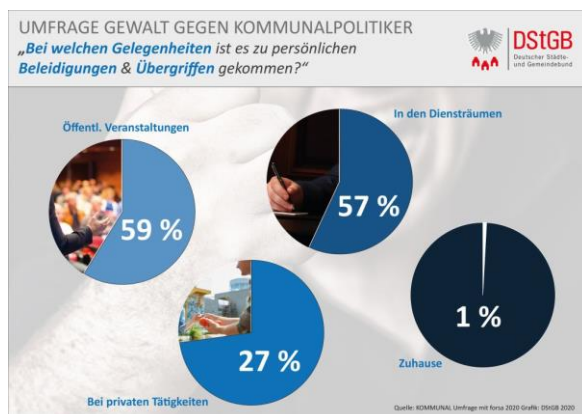
Zu den Vorschlägen des Entwurfes von CDU/CSU und SPD im Einzelnen:

Zu § 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 die analoge Welt. Darum halten wir es für sachgerecht und notwendig, Mitarbeiter und Mitarbeiterinnen § 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.

Zu §185 StGB

Die Schaffung des weiteren Qualifikationstatbestandes der öffentlich oder durch Schriften – also auch im Internet – verbreiteten Beleidigung in § 185 StGB ist überfällig. Ehrverletzungen finden im Netz einen großen Resonanzraum und verbreiten sich außerordentlich schnell. Die Beleidigungen im Netz können auch zu



weiteren Straftaten führen, auch zu körperlicher Gewalt. Sie wiegen damit für die Betroffenen ungleich schwerer als solche Beleidigungen, die 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 Officialdelikte fokussieren. Die Anpassung des §185 StGB an die Besonderheiten des Internets ist ausdrücklich zu begrüßen. Eine Umfrage der Fachzeitschrift Kommunal aus dem Sommer 2019 zufolge, wird ein Großteil der Beleidigungen in den sozialen Medien geäußert. Dieser neuen Entwicklung durch eine Modifizierung des §185 StGB Rechnung zu tragen, indem das Strafmaß auf maximal 2 Jahre Freiheitsstrafe angehoben wird, kann aus kommunaler Sicht ausdrücklich begrüßt werden.

Zu § 188 Absatz 1 Satz 2 neu StGB

Die Erweiterung des § 188 StGB auf Kommunalpolitiker ist angesichts der Beleidigungs- und Bedrohungslagen der letzten Jahre überfällig. Gerade die Amts- und Mandatsträger auf der kommunalen Ebene arbeiten täglich vor Ort haupt- und ehrenamtlich für den Bestand der Demokratie. Die Klarstellung zur Einbeziehung von Kommunalpolitikerinnen und Kommunalpolitikern wird daher aus Sicht des DStGB begrüßt. Die vorgesehene Ergänzung in § 188 Absatz 1 Satz 2 StGB-E, wonach

das politische Leben des Volkes bis zur kommunalen Ebene reicht, begegnet im Hinblick auf das strafrechtliche Bestimmtheitsgebot allerdings Bedenken, weil daraus nicht hervorgeht, welcher Personenkreis genau erfasst ist. Der DStGB schließt sich insofern den Bedenken des Bundesrates an. Die im Gesetzentwurf des Bundesrates „Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Verbesserung des strafrechtlichen Schutzes von im politischen Leben des Volkes stehenden Personen“ vom 29. November 2019, BR-Drucksache 418/19 (Beschluss), verwendete Definition ist demgegenüber vorzugswürdig. Sie begrenzt den geschützten Personenkreis, trägt den in einzelnen Ländern bestehenden Besonderheiten beim Verwaltungsaufbau Rechnung und schafft Rechtsklarheit.

Zu § 241 StGB

Die Erweiterung des § 241 StGB greift eine Forderung des DStGB auf, nachdem bisher nur Bedrohungen mit Verbrechen strafbar sind, aber die häufigen und nicht zuletzt sehr einschneidenden Bedrohungen mit Vergehen, wie Körperverletzungen zu Lasten des Bedrohten oder seiner Familie, nicht tatbestandsmäßig waren. Gerade aufgrund des Ziels des § 241 StGB den individuellen Rechtsfrieden zu wahren, ist eine Ausweitung um bestimmte – besonders einschneidende – Vergehen folgerichtig und angesichts der Bedrohungslage, der sich Kommunalpolitikerinnen und Kommunalpolitiker genauso wie Beschäftigte in den Verwaltungen jeden Tag ausgesetzt sehen, dringend notwendig. 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. Allerdings reicht diese Änderung nach unserem Dafürhalten nicht aus. Gerade sogenannte „diffuse“ Drohungen, wie „fühl dich nicht zu sicher“, „wir können jederzeit zuschlagen“ oder „Wir wissen, auf welche Schule deine Tochter geht“ dürften auch zukünftig den Tatbestand des § 241 StGB nicht erfüllen.

Weitergehende Einschränkungen, wie im Änderungsantrag von Bündnis90/Die Grünen gefordert, aus Sicht des Deutschen Städte- und Gemeindebundes abgelehnt. Hier geht es aus gerade um einen umfassenden Schutz, der auch Bedrohungen mit der Zerstörung von Sachen von bedeutendem Wert außerhalb von Brandstiftungsdelikten umfasst.

Vorschlag für einen § 238a StGB

Der Deutsche Städte- und Gemeindebund fordert daher die Einführung eines § 238a StGB mit folgendem Wortlaut:

„§ 238a Nachstellung gegenüber Amts- und Mandatsträgern

Absatz 1: *Wer einem Amts- oder Mandatsträger oder einem für den öffentlichen Dienst besonders Verpflichteten unbefugt nachstellt, indem er*

1. *seine räumliche Nähe privat aufsucht,*
2. *unter Verwendung von Telekommunikationsmitteln oder sonstigen Mitteln der Kommunikation oder über Dritte privat Kontakt zu ihm herzustellen versucht,*
3. *unter missbräuchlicher Verwendung von dessen personenbezogenen Daten*
4. *Bestellungen von Waren oder Dienstleistungen für ihn aufgibt oder Dritte*
5. *veranlasst, mit diesem Kontakt aufzunehmen,*
6. *ihn mit der Verletzung von Leben, körperlicher Unversehrtheit, Gesundheit oder Freiheit seiner selbst oder einer ihm nahestehenden Person bedroht oder*
7. *eine andere vergleichbare Handlung vornimmt und die Handlung für sich oder zusammen mit anderen Handlungen geeignet ist, seine*
8. *Lebensführung zu beeinträchtigen*

wird, sofern die Tat in Zusammenhang mit seiner Amts- oder Mandatsführung steht, mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

Absatz 2: *Die Tat wird nur auf Antrag verfolgt.“*

Im Gegensatz zu Nachstellungen nach § 238 StGB wäre es aufgrund der Begrenzung des Personenkreises und dem Zusammenhang mit der Ausübung eines öffentlichen Amtes nicht erforderlich, dass die Tat beharrlich erfolgen und es zu einer schwerwiegenden Beeinträchtigung der Lebensführung im Sinne des § 238 geführt haben muss.

Beharrlichkeit ist aufgrund der gegenüber § 238 StGB anderen Bedrohungslage nicht erforderlich. Die Taten zu Lasten der Amts- oder Mandatsträger werden nicht nur durch den einen Täter, sondern durch eine Vielzahl an unterschiedlichen, nicht verbundenen Tätern ausgeführt, daher ist es hier geboten auf das Merkmal beharrlich zu verzichten.

Eine schwerwiegende Beeinträchtigung der Lebensführung, wie es der § 238 StGB verlangt, wäre bei einem neu zu schaffenden § 238a StGB entbehrlich. Die hohen Hürden, die das Erfolgsdelikt des § 238 StGB setzt, würden aufgrund der Zielrichtung des § 238a StGB dazu führen, dass der Bereich der Strafbarkeit zu stark eingeschränkt werden würde. Ziel sollte es sein, dass die Amts- und Mandatsträger weiterhin ihre Aufgaben gegenüber dem Allgemeinwohl erfüllen können. Daher sollte auf die schwerwiegende Beeinträchtigung verzichtet werden.

Zur weiteren Begründung der Notwendigkeit der Einführung des § 238a StGB verweisen wir auf das anliegende Gutachten von Prof. Dr. Cristian Friedrich Majer aus dem Jahr 2016.

Vorschlag zur Änderung § 38 GVG

Zur Vorbereitung einer Schöffenwahl ist eine Vorschlagsliste gem. § 36 GVG „aufzulegen“ – also öffentlich zu machen. Dabei sind u.a. Geburtsdatum und Geburtsort aber auch die Wohnanschrift „aufzulegen“. Das ist aus unserer Sicht problema-

tisch: Zum einen erschließt sich bereits nicht der Sinn einer so detaillierten Angabe von persönlichen Daten. Verwechslungsgründe wird man in der Regel bereits über das Alter ausscheiden können. Aber selbst dann stellt sich die Frage der Erforderlichkeit und insbesondere der Angemessenheit der gesetzlichen Regelung. Denn neben dem Datenschutz geht es auch um berechnete Sicherheitsbelange der Schöffen. Sie sind einem Berufsrichter gleichgestellt und urteilen mit erheblichen Auswirkungen für die Angeklagten. Uns ist bekannt, dass sehr viele Berufsrichter aus der Strafgerichtsbarkeit ihre Wohnanschrift selbst in Telefonbüchern unterbinden. Es gibt sogar Auskunftssperren – u.a. gegenüber der Straßenverkehrsbehörden und Einwohnermeldeämter. Stets muss man über das Gericht die Anschrift des Richters erfahren. Auch das ist ein Sicherheitsstandard zugunsten der Berufsrichtern. Anders sieht dies aktuell für Schöffen aus. Auch wenn die Liste nur eine Woche ausgelegt wird (und damit nicht im Internet dauerhaft abrufbar sein dürfte), kann durch entsprechende Recherche die Wohnanschrift eines Schöffen später rückverfolgt werden. Von daher regen wir an, die Vorschrift entsprechend anzupassen. Schließlich stellt sich noch das Problem, dass eine Person mit einer Meldesperre gar nie Schöffe werden könnte. Dabei ist der Staat aber auf das Ehrenamt angewiesen.

Mit freundlichen Grüßen

Anlage

**Bedrohungen und Beschimpfungen
von
(Ober-)BürgermeisterInnen
sowie sonstigen Amts- und
MandatsträgerInnen
Strafbarkeitslücken und Handlungsoptionen**

Rechtsgutachten

von

Prof. Dr. Cristian Friedrich Majer

© Copyright:

Freiherr vom Stein-Akademie für Europäische Kommunalwissenschaften e.V., Stuttgart

2016

Prof. Dr. Cristian Friedrich Majer

Bedrohungen und Beschimpfungen von (Ober-)BürgermeisterInnen sowie sonstigen Amts- und MandatsträgerInnen – Strafbarkeitslücken und Handlungsoptionen

Rechtsgutachten im Auftrag der Freiherr vom Stein Akademie für Europäische
Kommunalwissenschaften, Stuttgart

Gliederung

I. Problemstellung

II. Geltende Rechtslage zur Strafbarkeit

- 1. Beleidigung, § 185 StGB**
- 2. Volksverhetzung, § 130 StGB**
- 3. Nachstellung, § 238 StGB**
- 4. (Versuchte) Nötigung, § 240 StGB**
- 5. Bedrohung mit einem Verbrechen, § 241 StGB**

III. Strafbarkeitslücken

- 1. Vorschlag für die Einführung eines § 238a StGB**
- 2. Wortlaut des § 238a StGB**
- 3. Erläuterungen**

IV. Ergebnis

Gutachten zur Bedrohung und Beschimpfung von Bürgermeisterern und sonstigen Amts- und Mandatsträgern

I. Problemstellung

Seit einiger Zeit sind kommunale Amts- und Mandatsträger wie Politiker allgemein verstärkten verbalen Angriffen aus der Bevölkerung mittels Telefon, E-Mail oder sozialen Medien ausgesetzt. Die Anonymität der Fernkommunikation begünstigt diese Tendenz noch, wobei einige der Absender auf ihren Klarnamen nicht verzichten. Die Anonymität senkt auch die Hemmschwelle für Straftaten massiv ab, die Absender fühlen sich häufig sicher vor Strafverfolgung. Massiv zugenommen – sowohl im Hinblick auf die Anzahl, wie auch auf die Heftigkeit – haben die Angriffe durch die Probleme im Hinblick auf die Flüchtlingsunterbringung und den Umgang mit Zuwanderung allgemein. Viele der Angriffe haben einen rechtsextremen Hintergrund, wobei auch andere Gruppen mit anderem Hintergrund, wie etwa radikale Tierschützer gelegentlich eine Rolle spielen, was Informationen aus der Praxis zeigen.

Diese Angriffe, welche teilweise bis hin zu konkreten Morddrohungen gehen, führen in manchen Fällen zu einer enormen psychischen Belastung. Einige Mandatsträger haben infolgedessen bereits den Rücktritt von ihren Ämtern erklärt.

Zu untersuchen ist, inwieweit diese „Hass-Mails“ und ähnliche Verhaltensweisen Straftatbestände erfüllen und wie eine effektive Strafverfolgung bewerkstelligt werden kann. Zu untersuchen ist auch, ob und inwieweit Strafbarkeitslücken bestehen und bejahendenfalls, wie diesen begegnet werden kann.

II. Geltende Rechtslage zur Strafbarkeit

1. Beleidigung, § 185 StGB

In Betracht kommt für viele der bekannt gewordenen Fälle eine Strafbarkeit wegen Beleidigung nach § 185 StGB.

Unter einer Beleidigung im Sinne des § 185 StGB wird herkömmlich die Kundgabe von Missachtung in der Weise, dass dem Betroffenen der sittliche, personale oder soziale Geltungswert durch das Zuschreiben negativer Qualitäten ganz oder teilweise abgesprochen wird, verstanden.¹

Viele der bekannt gewordenen Verhaltensweisen wie etwa die Bezeichnung als „Schwein“² oder „Arschloch“³ oder „Krüppel“⁴ erfüllen diesen Tatbestand unproblematisch.

Allerdings ist bei Beleidigungen im Sinne des § 185 StGB – sofern es sich um Werturteile und nicht um Tatsachenbehauptungen handelt – stets zu prüfen, ob eine Rechtfertigung nach § 193 StGB (Wahrnehmung berechtigter Interessen) vorliegt. Hier relevant ist vor allem eine Rechtfertigung aufgrund der Meinungs- oder Kunstfreiheit nach Art. 5 I bzw. III GG.⁵ Dabei gilt, dass auch polemisierende Überspitzungen und Vereinfachungen, mögen sie auch als geschmacklos, unpassend oder falsch anzusehen sein, hinzunehmen sind, wenn es dem Kritiker darum geht, seiner Ansicht

¹ Siehe etwa Eisele, in: Schönke/Schröder, § 185 StGB Rn. 2; BayObLG NJW 2005, 1291.

² http://www.mdr.de/sachsen/beleidigung-buergermeister-pirna100_zc-f1f179a7_zs-9f2fcd56.html, Abruf am 17.12.2015.

³ DER SPIEGEL vom 24.10.2015, S. 24.

⁴ DER SPIEGEL vom 24.10.2015, S. 24.

⁵ Lenckner/Eisele, in: Schönke/Schröder, § 193 Rn. 8.

Nachdruck zu verleihen.⁶ Eine Grenze findet dies jedoch, soweit nicht mehr die Kritik, sondern die Diffamierung und Herabsetzung der Person im Vordergrund steht („Schmähkritik“).⁷

Nach diesen Maßstäben kommt eine Rechtfertigung nur in manchen der hier in Rede stehenden Fälle in Betracht, das gilt etwa für die Bezeichnung „Asylantenoberbürgermeister“⁸ oder der Bezeichnung der Bundeskanzlerin als „Königin der Schlepper“⁹. Diese Bezeichnungen sind geschmack- und niveaulos, enthalten jedoch einen inhaltlichen Vorwurf, weshalb eine Rechtfertigung durch die Meinungsfreiheit möglich erscheint. In der Rechtsprechung mit dieser Begründung als zulässig angesehen wurde etwa die Bezeichnung als „Volksverräter“,¹⁰ was freilich nicht zwingend erscheint. Als strafbare Beleidigung angesehen wurde hingegen die Bezeichnung als „Oberfaschist“,¹¹ für zulässig hingegen die Bezeichnung der Polizeiarbeit als „SS-Methoden“.¹² Für die oben genannten Beispiele („Schwein“, „Arschloch“, „Krüppel“) oder auch „blöde Schlampe“¹³ und „stinkende Ratte“¹⁴ scheidet eine Rechtfertigung aus, da sie keine nennenswerte Kritik mehr transportieren, sondern die Diffamierung in den Vordergrund stellen.

Hinsichtlich der strafrechtlichen Ahndung ist zu beachten, dass es sich bei einer Beleidigung nach § 185 StGB um ein Privatklagedelikt gemäß § 374 I Nr. 2 StPO handelt. Die darin aufgeführte Ausnahme betrifft nur die Beleidigung politischer Körperschaften nach § 194 IV StGB, nicht die Beleidigung von Amtsträgern nach § 194 III StGB.

In diesen Fällen findet eine Strafverfolgung nur dann statt, wenn die Staatsanwaltschaft ein öffentliches Interesse daran bejaht (§ 376 StPO). Dabei handelt es sich um einen Ermessensbegriff, dessen Ausübung durch die RiStBV näher bestimmt wird.¹⁵ Nr. 229 sieht dabei vor, dass bei Beleidigungen von Amtsträgern diesen Gelegenheit gegeben wird, einen Strafantrag zu stellen; dennoch wird auch in diesen Fällen gemäß Absatz 2 das öffentliche Interesse geprüft. Allerdings bestimmt § 86 Abs. 2, dass ein öffentliches Interesse in der Regel vorliegt, wenn der „Rechtsfrieden über den Lebenskreis des Verletzten hinaus gestört und die Strafverfolgung ein gegenwärtiges Anliegen der Allgemeinheit ist“, was bei der Stellung des Verletzten im öffentlichen Leben der Fall sein kann. Verneint die Staatsanwaltschaft allerdings das öffentliche Interesse, gibt es für den Betroffenen keine Möglichkeit, rechtlich hiergegen vorzugehen;¹⁶ ein Klageerzwingungsverfahren ist wegen § 172 II 3 StPO ausgeschlossen.

Es bleibt die Möglichkeit der Privatklage, welche aber von den Betroffenen im Hinblick auf den erheblichen Aufwand und die Vielzahl der Fälle kaum genutzt wird.

Wichtig wäre, die Staatsanwaltschaften dazu anzuhalten, bei Beleidigungen von Mandatsträgern stets konsequent öffentliche Klage zu erheben, sofern ein Strafantrag vorliegt. Im Hinblick auf die derzeitige erhebliche Überlastung bleibt aber zu befürchten, dass das Vollzugsdefizit damit nicht wirksam beseitigt werden kann.

⁶ BVerfG NJW 1992, 2815, 2816; BGH NJW 1994, 124, 126.

⁷ BVerfG NJW 2003, 961, 962; BVerfG NJW 1991, 95 ff.

⁸ DER SPIEGEL vom 24.10.2015, S. 25.

⁹ DER SPIEGEL vom 24.10.2015, S. 25.

¹⁰ Sächs. VerfGH BeckRS 2011, 25479.

¹¹ OLG Karlsruhe NJW 1986, 1262, 1264.

¹² OLG Frankfurt, NStZ-RR 2012, 244.

¹³ <http://www.n-tv.de/politik/Polizei-ermittelt-wegen-Hass-gegen-Merkel-article15815531.html>

¹⁴ <http://www.faz.net/aktuell/politik/inland/drohungen-gegen-politiker-du-stinkende-ratte-13874653.html> (Abruf am 30.12.2015).

¹⁵ Senge, in Karlsruher Kommentar zur StPO, § 376 Rn. 2.

¹⁶ Senge, in Karlsruher Kommentar zur StPO, § 376 Rn. 2.

2. Volksverhetzung, § 130 StGB

Viele der hier zu untersuchenden Verhaltensweisen haben einen rechtsextremen Hintergrund, sodass auch an eine Strafbarkeit wegen Volksverhetzung nach § 130 StGB zu denken ist. In der hier relevanten Variante des § 130 I Nr. 2 StGB ist es u.a. strafbar, wenn jemand eine Bevölkerungsgruppe, Teile einer solchen oder einen einzelnen wegen seiner Zugehörigkeit zu einer solchen „beschimpft, böswillig verächtlich macht oder verleumdet“, sofern er dadurch ihre Menschenwürde angreift; allerdings nur dann, wenn dies in einer Weise erfolgt, die geeignet ist, den öffentlichen Frieden zu stören.

Beschimpfen meint dabei eine besonders herabsetzende Missachtenskundgebung.¹⁷ Der Angriff auf die Menschenwürde setzt voraus, dass es sich um eine besonders massive Herabsetzung handelt, wenn den Betroffenen ihr Lebensrecht und ihr Eigenwert abgesprochen wird,¹⁸ wie etwa der Bezeichnung von Asylbewerbern als Parasiten.¹⁹

Strafbar ist außerdem die Aufstachelung zum Hass oder zu Gewalt- und Willkürmaßnahmen durch die genannten Verhaltensweisen (§ 130 I Nr. 1 StGB) sowie – hier weniger relevant – die Leugnung, Billigung oder Verharmlosung von NS-Verbrechen (§ 130 III, IV StGB).

Volksverhetzung kann als Begleittat vorliegen, die hier untersuchten Verhaltensweisen stellen jedoch in der Regel selbst keine Volksverhetzung dar, da sie sich gezielt und zum Teil gegen Mandatsträger richten (womit die Eignung zur Gefährdung des öffentlichen Friedens fraglich wird) und diese außerdem nicht wegen einer Zugehörigkeit zu einer bestimmten Bevölkerungsgruppe, sondern wegen ihrer Position und ihrem Handeln angegriffen werden.

3. Nachstellung, § 238 StGB

In Betracht kommt außerdem eine Strafbarkeit gemäß § 238 StGB.

Die im Jahre 2007 neu in das Strafgesetz aufgenommene Vorschrift soll Verhaltensweisen erfassen, welche unterhalb der Schwelle der Straftatbestände der §§ 123, 240, 177, 223 StGB liegen, aber durch nachhaltige und wiederholtes Stalking schwerwiegende Folgen für das Opfer mit sich bringen.²⁰

Letztlich erfasst werden sollen Verhaltensweisen, welche umgangssprachlich als Psychoterror bezeichnet werden.²¹

Das Gesetz führt mehrere Varianten auf, welche als Tathandlung geeignet sind. Nr. 1 erfasst das Aufsuchen räumlicher Nähe, Nr. 2 den Versuch der Herstellung der Kontaktaufnahme unter Verwendung von Telekommunikationsmitteln oder sonstigen Mitteln der Kommunikation, Nr. 3 die Bestellung von Waren unter dem Namen des Opfers und ähnliche Verhaltensweisen, Nr. 4 die Drohung mit der Verletzung bestimmter Rechtsgüter, Nr. 5 schließlich vergleichbare Handlungen.

Sämtliche Handlungen müssen unbefugt und beharrlich erfolgen und das Opfer in seiner Lebensgestaltung schwerwiegend beeinträchtigen.

a) Die Variante des Nr. 1 ist für die hier zu untersuchenden Fälle weniger relevant; erforderlich hierfür ist das gezielte Aufsuchen der räumlichen Nähe.²² Diese Variante ist erkennbar auf die häufigen Fälle des Stalkings durch ehemalige Lebensgefährten oder Verehrer zugeschnitten.

¹⁷ Sternberg-Lieben, in: Schönke-Schröder, StGB, § 130 Rn. 5d.

¹⁸ OLG Frankfurt NJW 1995, 143; a.A. (zu eng): Sternberg-Lieben a.a.O.

¹⁹ KG JR 1998, 213; Sternberg-Lieben a.a.O.

²⁰ Eisele, in: Schönke-Schröder, StGB, § 238 Rn. 1.

²¹ Mitsch, NJW 2007, 1237 (1238).

²² Eisele, in: Schönke-Schröder, StGB, § 238 Rn. 9.

Denkbar ist die Verwirklichung der Variante allerdings bei Protestkundgebungen unmittelbar vor dem Haus des Opfers. Die erforderliche Nähe liegt hier zweifellos vor, ausreichend ist nämlich der Aufenthalt in Sichtweite.²³

In Frage steht hier aber die Verwirklichung des Merkmals „unbefugt“. Umstritten ist dabei, ob es sich auf den Tatbestand oder die Rechtswidrigkeit bezieht. Überwiegend wird differenziert, ob es sich um eine grundsätzlich unzulässige Verhaltensweise (wie in den Nrn. 3 und 4) oder um eine grundsätzlich zulässige Verhaltensweise (Nr. 1 und 2) handelt.²⁴ Nur im letztgenannten Fall bezieht sich das Merkmal auf den Tatbestand. Geschützt werden sollten insbesondere recherchierende Journalisten im Hinblick auf die Pressefreiheit nach Art. 5 I GG, wobei auch hier eine generelle Verneinung des Tatbestandes nicht in Betracht kommt („Paparazzi“); es kommt vielmehr stets auf die Umstände des Einzelfalls an.²⁵

Ob es sich bei wiederholten Protestkundgebungen vor dem Haus eines Mandatsträgers um eine zulässige Versammlung handelt, welche den Schutz des Art. 8 GG genießt und daher im Rahmen des § 238 StGB als nicht „unbefugt“ anzusehen ist, ist unter dem Aspekt der kollidierenden Grundrechte des Art. 8 GG einerseits und des allgemeinen Persönlichkeitsrechts des Betroffenen nach Art. 1 I i.V.m. 2 I GG zu bewerten. Danach ergibt sich regelmäßig der Vorrang der Persönlichkeitsrechte der Betroffenen. So hat das OVG Berlin eine Protestkundgebung zum Privathaus des ehemaligen regierenden Bürgermeisters als unzulässig angesehen.²⁶ Ausdrücklich anerkannt wurde das Bedürfnis nach Schutz der Privatsphäre auch von Personen des öffentlichen Lebens vor derartigen Kundgebungen, da sie psychischen Druck ausüben.²⁷ In demselben Sinne hatte bereits der VGH München betreffs einer Kundgebung vor dem Privathaus des ehem. bayerischen Innenministers entschieden.²⁸

Unter Zugrundelegung dieser Kriterien scheidet eine Rechtfertigung der Protestkundgebungen vor den privaten Häusern und Wohnungen der Betroffenen regelmäßig aus. Sie sind regelmäßig als unbefugt im Sinne des § 238 StGB anzusehen.

b) Weitaus häufiger einschlägig ist hingegen die Variante des Versuchs der Herstellung der Kontaktaufnahme unter Verwendung von Kommunikationsmitteln, sonstigen Mitteln der Kommunikation oder über Dritte (Nr. 2). Typische Verhaltensweisen sind etwa Telefonanrufe, das Versenden von E-Mails oder das Versenden von Nachrichten in sozialen Netzwerken wie etwa Facebook.²⁹ Die hier in Rede stehenden Verhaltensweisen verwirklichen damit typischerweise die Tathandlung des § 238 I Nr. 2 StGB. Auch das Kontaktieren Dritter, etwa Familienangehöriger, ist tatbestandsmäßig. Schwierigkeiten bestehen hier im Hinblick auf den Nachweis der Urheberschaft, sofern die Nachricht oder der Anruf anonym erfolgt.³⁰

Auch hier ist allerdings das Merkmal „unbefugt“ problematisch; denkbar ist eine Rechtfertigung aufgrund der Meinungsfreiheit nach Art. 5 I GG. Eine Kontaktaufnahme zu einem Amts- oder Mandatsträger ist nicht per se unzulässig. Auch bei dieser müssen aber die oben genannten Maßstäbe bezüglich Nr. 1 und der Versammlungsfreiheit nach Art. 8 I GG Berücksichtigung finden. Eine private Kontaktaufnahme zu einem Mandatsträger ist regelmäßig nicht von der Meinungsfreiheit gerechtfertigt, insoweit muss auch hier der Schutz der Privatsphäre regelmäßig Vorrang haben. Anderes gilt aber etwa für Facebook-Accounts, in denen sich Mandatsträger gezielt an die Öffentlichkeit wenden und politische Themen diskutieren.³¹ Eine Kontaktaufnahme durch Beiträge in diesem Forum verletzt

²³ Eisele, in: Schönke-Schröder, StGB, § 238 Rn.8; Sonnen, in: Kindhäuser/Neumann/Paefgen, StGB, § 238 Rn. 29; Kinzig/Zander JA 2007, 481, 483.

²⁴ Sonnen, in: Kindhäuser/Neumann/Paefgen, StGB, § 238 Rn.50 m.w.N.

²⁵ Sonnen a.a.O.

²⁶ BeckRS 2012, 49589.

²⁷ OVG Berlin a.a.O.

²⁸ BeckRS 1995, 08392.

²⁹ Eisele, in: Schönke-Schröder, StGB, § 238 Rn. 9; Peters, NSTz 2009, 238 (240).

³⁰ Peters, NSTz 2009, 238 (240).

³¹ Siehe etwa den Facebook-Account des Tübinger Oberbürgermeisters Palmer.

die Privatsphäre nicht, da die Öffentlichkeit gerade zur Diskussion eingeladen wird; anderes gilt jedoch für private Nachrichten.

Die private Kontaktaufnahme zu einem Mandatsträger ist daher auch regelmäßig unbefugt im Sinne des § 238 StGB.

c) Die Bestellung von Waren bzw. das Schalten von Kontaktanzeigen und ähnliches Verhalten unter der Verwendung von personenbezogenen Daten (Nr. 3) spielt hier nur eine geringe Rolle. Weitaus häufiger relevant ist die Variante der Bedrohung mit einer Verletzung von Leben, körperlicher Unversehrtheit, Gesundheit oder Freiheit, wobei auch Rechtsgüter einer nahestehenden Person erfasst sind, § 238 I Nr. 4 StGB. Gesundheit umfasst dabei nach überwiegender Meinung auch die seelische Gesundheit, sodass psychische Verletzungen mitumfasst sind.³² Unter Freiheit ist nicht die allgemeine Handlungsfreiheit des Art. 2 I GG, sondern ebenso wie in § 35 StGB lediglich die körperliche Fortbewegungsfreiheit zu verstehen.³³

Viele E-Mails und Anrufe verwirklichen diese Tatbestandsvariante, wenn etwa mit der Verbringung in ein KZ gedroht wird. Zu beachten ist allerdings, dass viele Drohungen zu unbestimmt sind, um einem bestimmten Rechtsgut zugeordnet zu werden; das gilt etwa für die Aussagen „Halt die Fresse, oder ich bin morgen bei dir“³⁴ oder „Heiko, bald ist deine Zeit abgelaufen“³⁵, beide gegenüber dem Bundesjustizminister.

§ 238 I Nr. 5 StGB enthält schließlich eine Generalklausel über nicht in Nrn. 1-4 enthaltene Verhaltensweisen. Diese müssen den genannten Verhaltensweisen vergleichbar sein und soll insbesondere künftigen technischen Entwicklungen Raum tragen.³⁶ Nennenswerte Bedeutung kommt der Norm im Hinblick auf die untersuchten Verhaltensweisen nicht zu.

d) Sämtliche Tatbestandsvarianten müssen „beharrlich“ begangen worden sein. Erforderlich ist ein wiederholtes und andauerndes Verhalten, welches zusätzlich eine besondere Hartnäckigkeit und gesteigerte Gleichgültigkeit aufweisen soll.³⁷ Welche Verhaltensweisen dazu genügend sind, ist in der Rechtsprechung umstritten. Nach dem LG Lübeck soll schon eine einmalige Wiederholung ausreichend sein.³⁸ Der BGH hat es ausdrücklich abgelehnt, eine Mindestzahl an Wiederholungen zu fordern, maßgeblich ist vielmehr eine Gesamtwürdigung, wobei eine mindestens einmalige Wiederholung immer Voraussetzung ist.³⁹

Dieses Merkmal ist in den hier untersuchten Fällen besonders schwierig nachzuweisen. Die Tathandlungen werden hier nicht von einer bestimmten Person begangen, wie es dem Leitbild des Stalkers als abgewiesenem Verehrer bzw. ehem. Lebensgefährten entspricht, sondern von einer Vielzahl von Personen, welche zudem oft anonym bleiben, sodass eine Zuordnung eines bestimmten Verhaltens zu einer bestimmten Person kaum möglich erscheint.

Möglich ist aber die Begehung (mit Ausnahme der Nr. 1) in Mittäterschaft.⁴⁰ Insbesondere bei organisierten Attacken, wie sie bei rechtsextremem Hintergrund durchaus möglich sind, kommt eine Mittäterschaft in Betracht. Diese hat zur Folge, dass die einzelnen Handlungen gemäß § 25 II StGB wechselseitig zugerechnet werden. Voraussetzung ist ein gemeinsamer Tatentschluss, aufgrund dessen die Handlungen vorgenommen werden.⁴¹ Dieser muss nachgewiesen werden, was hier allerdings erhebliche Schwierigkeiten aufwirft. Aus einer Massivität und hohen Anzahl von Anrufen und Mails aus

³² Sonnen, in: Kindhäuser/Neumann/Paefgen, StGB, § 238 Rn. 39.

³³ Sonnen, in: Kindhäuser/Neumann/Paefgen, StGB, § 238 Rn. 39.

³⁴ DER SPIEGEL vom 24.10.2015, S. 29. Hier kommt versuchte Nötigung in Betracht, siehe unten.

³⁵ DER SPIEGEL vom 24.10.2015, S. 29.

³⁶ BT-Drucks 16/3641.

³⁷ BGH NJW 2010, 1680 (1682); Sonnen, in: Kindhäuser/Neumann/Paefgen, StGB, § 238 Rn. 42.

³⁸ BeckRS 2008, 05249.

³⁹ NJW 2010, 1680 (1682).

⁴⁰ Eisele, in: Schönke-Schröder, StGB, § 238 Rn. 35.

⁴¹ Heine/Weißer, in: Schönke-Schröder, StGB, § 25 Rn. 71.

einem bestimmten Milieu kann nicht ohne weiteres auf eine besondere Organisation geschlossen werden. Es ist denkbar, dass ein Verhalten in bestimmten Kreisen eine besondere Reaktion auslöst, ohne dass diese organisiert werden muss.

e) Weiter erforderlich ist, dass die Handlungen zu einer „schwerwiegenden Beeinträchtigung der Lebensführung“ des Opfers geführt haben. Der Bundesgerichtshof fordert hierbei, dass das durch die Handlungen bewirkte Verhalten zu „gravierenden, ernst zu nehmenden Folgen führt, die über durchschnittliche, regelmäßig hinzunehmende Beeinträchtigungen der Lebensgestaltung erheblich und objektivierbar hinausgehen“.⁴² Maßnahmen der Eigensicherung wie etwa ein Anrufbeantworter oder eine Fangschaltung sollen nicht ausreichen, genügen sollen dagegen der Wechsel von Wohnung und Arbeitsplatz, das Verlassen der Wohnung nur noch in Begleitung von Dritten und ähnliche Maßnahmen.⁴³

Nach diesem Maßstab wird man das Merkmal bejahen können, wenn ein Mandatsträger aufgrund der Angriffe gegen ihn zurücktritt, wie etwa im Fall des ehrenamtlichen Bürgermeisters von Tröglitz in Sachsen⁴⁴ oder des Bezirksbürgermeisters des Reutlinger Stadtteils Oferdingen.⁴⁵

In den sonstigen Fällen ist das Tatbestandsmerkmal zu verneinen. Ein Mandatsträger, der den permanenten Anfeindungen trotzt und weiterhin wie gewohnt seiner Arbeit nachgeht, ist insoweit nicht geschützt, auch wenn diese eine erhebliche psychische Belastung darstellen.

f) Als Zwischenergebnis ist festzuhalten, dass der Tatbestand des Nachstellens nach § 238 StGB in den hier vorliegenden Konstellationen nur sehr selten erfüllt sein wird.

Zwar liegen die Tatbestandsvarianten des Nachstellens häufig vor, regelmäßig sind diese auch unbefugt im Sinne der Vorschrift; allerdings fehlt es meist an der – auf einen bestimmten Täter bezogenen – Beharrlichkeit und auch meist an der schwerwiegenden Beeinträchtigung der Lebensführung.

4. (Versuchte) Nötigung, § 240 StGB

Nach § 240 StGB macht sich strafbar, wer einen anderen Menschen mit Gewalt oder einem empfindlichen Übel bedroht bzw. Gewalt anwendet, diesen damit zu einem bestimmten Verhalten veranlassen will und dieses Verhalten auch gezeigt wird. Die Tat ist zudem nur rechtswidrig, wenn die Anwendung der Gewalt oder die Androhung des Übels zu dem bestimmten Zweck auch als verwerflich anzusehen ist (§ 240 II StGB)

a) Nötigungshandlung

Erfasst ist zunächst die Anwendung von Gewalt. Unter Gewalt im Sinne des § 240 StGB versteht man sowohl vis absoluta (willensbrechende Gewalt, etwa Schläge) als auch vis compulsiva (willensbeugende Gewalt, etwa beim Zufahren mit dem PKW auf einen Fußgänger).⁴⁶ Das Merkmal der Anwendung von Gewalt hat in den hier zu untersuchenden Fallkonstellationen (glücklicherweise) nur eine geringe Bedeutung.

Weitaus häufiger ist die Tatbestandsvariante der Drohung mit einem empfindlichen Übel. Unter Drohung ist zunächst einmal das Inaussichtstellen eines Übels erfasst, dessen Verwirklichung davon abhängen soll, dass der Bedrohte nicht nach dem Willen des Täters reagiert.⁴⁷

⁴² NJW 2010, 1680 (1683).

⁴³ BGH NJW 2010, 1680 (1683) unter Hinweis auf BT-Dr 16/575, S. 8; ebenso OLG Hamm BeckRS 2009, 06849.

⁴⁴ <https://www.tagesschau.de/inland/troeglitz-103.html> (Abruf am 29.12.2015).

⁴⁵ <http://www.tagblatt.de/Nachrichten/Reaktionen-auf-Bezirksbuergermeister-Ruecktritt-251617.html> (Abruf am 29.12.2015).

⁴⁶ BGH DAR/S 1987, 195; Eser/Eisele, in: Schönke/Schröder, StGB, § 240 Rn. 4.

⁴⁷ Eser/Eisele, in: Schönke/Schröder, StGB, Vor § 234 ff. Rn.30.

Ein empfindliches Übel ist immer dann gegeben, wenn es sich um einen Nachteil handelt, der geeignet ist, einen besonnenen Menschen zu dem angestrebten Verhalten zu veranlassen (im konkreten Fall verneint für die Drohung gegenüber einem Bürgermeister mit der Offenbarung von strafbaren Handlungen in der Verwaltung).⁴⁸ Als Beispiele genannt werden die Drohung mit dem Entzug eines Arbeitsverhältnisses, mit Lärmterror oder der Offenbarung intimer Verhältnisse.⁴⁹

Erfasst ist selbstverständlich auch die Drohung mit Gewalt. Die Drohung muss nicht ausdrücklich erfolgen, auch eine konkludente Drohung ist möglich.⁵⁰ Ausreichend ist zudem, dass das Übel für einen Dritten angedroht wird, sofern dies auch für den Genötigten ein Übel darstellt.⁵¹

Nach diesen Maßstäben dürfte es eine Nötigungshandlung sein, wenn Kinder eines Mandatsträgers zur Schule begleitet werden und dies ihm gezielt zur Kenntnis gebracht wird. In diesem äußerlich neutralen Verhalten liegt die versteckte Drohung, man könne jederzeit rechtswidrige Taten gegenüber den Kindern begehen und daher die Drohung mit einem empfindlichen Übel.

Auch eine Drohung liegt in der Aussage „Halt die Fresse, oder ich bin morgen bei dir!“.⁵² Hier wird zwar keine konkrete Handlung in Aussicht gestellt, die Auslegung ergibt jedoch, dass es sich bei dieser Handlung um eine rechtswidrige Tat zu Lasten des Genötigten handeln sollte (Körperverletzung, Hausfriedensbruch, Beleidigung).

Abzugrenzen ist die Drohung allerdings von der Warnung. Eine solche liegt nach – allerdings umstrittener⁵³ – Rechtsprechung immer dann vor, wenn der Äußernde nicht vorgibt, auf den Eintritt des Übels Einfluss zu haben.⁵⁴ Im zitierten Urteil des BGH wurde eine bloße Warnung angenommen, wenn in Aussicht gestellt wird, eine Person würde von einem erneuten (vom Täter erhofften) NS-Regime zur Verantwortung gezogen werden. Auf dieses Übel gab der Täter keinen Einfluss zu haben vor. Mehrdeutig ist auch das öffentliche Zeigen eines Galgens mit bestimmten Personen.⁵⁵ Zwar wird hier der Wunsch nach ihrer Ermordung deutlich, es ist aber zweifelhaft, ob der Eintritt vom Willen des Äußernden abhängen soll, hier kommt es auf die Umstände an.

Bereits aus diesem Grund dürften viele der hier diskutierten Fälle keine strafbare Nötigung darstellen. Anderes gilt nur dann, wenn der Täter angibt, sich an derartigen Entscheidungen beteiligen zu wollen (beispielsweise bei „Wir werden dich ins KZ stecken“).

b) Nötigungserfolg

Erforderlich ist ein durch die Nötigungshandlung hervorgerufenen Verhalten. Dieses kann jedes Tun, Dulden oder Unterlassen sein. Es muss allerdings ein von der Nötigungshandlung getrenntes Verhalten sein, die bloße Einschüchterung und das Verbreiten von Angst sind nicht tatbestandsmäßig.⁵⁶

Nötigungserfolg in den hier untersuchten Fällen kann jede politische Entscheidung sein, etwa die Nichteröffnung einer Flüchtlingsunterkunft oder die Verweigerung der Unterstützung für Tierversuche. Allerdings ist erforderlich, dass der Nötigungserfolg die spezifische und unmittelbare Folge der Handlung ist.⁵⁷

Daran dürfte es in den meisten der hier untersuchten Fälle fehlen. Zudem wird man aus politischen Gründen kaum jemals eine Entscheidung mit Nötigungshandlungen der Bürger begründen können.

⁴⁸ BGH NStZ 1992, 278.

⁴⁹ Eser/Eisele, in: Schönke/Schröder, StGB, § 240 Rn. 9.

⁵⁰ KG BeckRS 2013, 00923; Sinn, in: Münchener Kommentar zum StGB, § 240 Rn. 69.

⁵¹ BGH NJW 1992, 702 (203); Sinn, in: Münchener Kommentar zum StGB, § 240 Rn. 84.

⁵² DER SPIEGEL vom 24.10.2015, S. 29.

⁵³ Kritisch etwa Sinn, in: Münchener Kommentar zum StGB, § 240 Rn. 75.

⁵⁴ BGH NStZ 2009, 692.

⁵⁵ <http://www.faz.net/aktuell/politik/inland/drohungen-gegen-politiker-du-stinkende-ratte-13874653.html> (Abruf am 30.12.2015).

⁵⁶ Eser/Eisele, in: Schönke/Schröder, StGB, § 240 Rn. 12.

⁵⁷ BGH NSTZ-RR 2006, 77; Eser/Eisele, in: Schönke/Schröder, StGB, § 240 Rn. 14.

Liegt ein Nötigungserfolg nicht vor bzw. beruht er nicht beweisbar auf einer Nötigungshandlung, kommt jedoch eine Versuchsstrafbarkeit in Betracht.

c) Finalität

Nicht ausreichend ist hier Vorsatz, es muss dem Täter gerade darauf ankommen, den Nötigungserfolg zu erreichen (Absicht, *dolus directus* 1. Grades).⁵⁸ Daran fehlt es, wenn die Handlungen nur der Empörung Luft machen sollen bzw. aus Unzufriedenheit heraus erfolgen oder aber lediglich Angst verbreiten sollen, was in den meisten Fällen hier vorliegen dürfte wie etwa bei „Heiko, deine Zeit ist bald abgelaufen“⁵⁹ oder „Du Hexe wirst brennen“⁶⁰. Anderes dürfte für die erwähnte Nötigungshandlung gegenüber dem Bundesjustizminister („Halt die Fresse, oder ich bin morgen bei dir“)⁶¹ gelten. Hintergrund war wohl dessen Äußerung über PEGIDA als „Schande für Deutschland“. Angestrebtes Ziel der Äußerung ist das Unterlassen weiterer negativer Aussagen über Pegida.

d) Verwerflichkeit

Nicht jede Nötigung ist rechtswidrig, sie ist es nach § 240 II StGB nur dann, wenn die Anwendung der Gewalt oder die Androhung des Übels zu dem angestrebten Zweck als verwerflich anzusehen ist.

Das ist bereits dann der Fall, wenn das Nötigungsmittel eine strafbare Handlung darstellt.⁶² Die Androhung einer Körperverletzung etwa ist also per se verwerflich. Die Verwerflichkeit kann sich aber auch aus der Unerlaubtheit des vom Täter verfolgten Zwecks ergeben. Dabei ist es nicht erforderlich, dass der Nötigungserfolg als solcher unzulässig ist; es genügt, dass der Täter keinen Anspruch darauf hat.⁶³ Das dürfte für die meisten der hier im Raum stehenden politischen Entscheidungen gelten. Allerdings stehen diese auch immer in Bezug auf die Stimmabgabe durch den Bürger. Droht also ein Bürger einem Bürgermeister, ihn das nächste Mal nicht mehr zu wählen, falls er eine bestimmte politische Entscheidung nicht treffe bzw. nicht rückgängig mache, ist das nicht als verwerflich anzusehen.

Schließlich kann sich die Verwerflichkeit auch bei erlaubttem Mittel und erlaubttem Zweck aus der fehlenden Beziehung zwischen Mittel und Zweck ergeben (Inkonnexität), was aber für die hier untersuchten Fälle kaum Bedeutung haben wird.

e) Eine (versuchte) Nötigung ist in den hier untersuchten Fällen zwar vereinzelt gegeben, meist jedoch zu verneinen. Manchmal liegt bereits keine Drohung, sondern eine Warnung vor. Häufig kommt es dem Täter aber nicht auf ein bestimmtes Verhalten, sondern allgemein auf die Einschüchterung an, weshalb die erforderliche Absicht fehlt.

5. Bedrohung mit einem Verbrechen, § 241 StGB

In Betracht kommt außerdem die Bedrohung mit einem Verbrechen gemäß § 241 StGB.

Voraussetzung hierfür ist, dass der Täter das Opfer oder eine ihm nahestehende Person mit der Begehung eines Verbrechens bedroht. Verbrechen sind nur Straftaten, in denen das Gesetz als Mindestmaß eine Freiheitsstrafe von 1 Jahr festsetzt (§ 12 I StGB). Die Drohung mit der Begehung eines Vergehens (das sind alle übrigen Straftaten) ist nicht tatbestandsmäßig.

Verbrechen sind etwa Mord (§ 211 StGB) und Totschlag (§ 212 StGB); bei den Körperverletzungsdelikten sind es die schwere Körperverletzung nach § 226 StGB (etwa bei Behinderung als Folge) und Körperverletzung mit Todesfolge (§ 227 StGB). Die einfache (§ 223 StGB) und gefährliche (§ 224 StGB), wie etwa die gemeinschaftliche Körperverletzung, sind lediglich Vergehen. Wer also Drohungen der Art

⁵⁸ Sinn, in: Münchener Kommentar zum StGB, § 240 Rn. 105.

⁵⁹ DER SPIEGEL vom 24.10.2015, S. 29.

⁶⁰ DER SPIEGEL vom 24.10.2015, S. 25.

⁶¹ DER SPIEGEL vom 24.10.2015, S. 29.

⁶² Eser/Eisele, in: Schönke/Schröder, StGB, § 240 Rn. 19.

⁶³ Eser/Eisele, in: Schönke/Schröder, StGB, § 240 Rn. 20.

„Wir kommen vorbei und schlagen dich krankenhaushausreif“ ausstößt, macht sich nicht nach § 241 StGB strafbar.

Aber auch bei Drohungen mit einem Tötungsdelikt kommt es darauf an, ob diese ernst gemeint oder lediglich als Beschimpfung bzw. Verwünschung anzusehen sind.⁶⁴ Zumal müssen diese hinreichend konkret sein, allgemeine Drohungen genügen nur, wenn sie in Verbindung mit anderen Umständen auf ein hinreichend konkretes Verbrechen schließen lassen.⁶⁵

Nach diesen Kriterien wäre ein Foto, in welchem ein Landrat mit einem Blitz durch den Kopf dargestellt wird, verbunden mit dem Text „Kanaken-Landrat, verpiss dich!“, „Der Blitz soll dich treffen“, „du wirst sehen, was passiert“, „fühl dich nur nicht zu sicher“⁶⁶ wohl nicht konkret genug. Zwar lässt sich hieraus der Wunsch entnehmen, der Landrat möge zu Tode kommen, es wird aber nicht konkret auf die Begehung durch einen Täter hingewiesen. Die sonstigen Drohungen weisen nicht eindeutig auf ein Verbrechen hin.

Drohungen wie etwa „du Hexe wirst brennen“⁶⁷ können allerdings durchaus ernst gemeint sein, wie Attentate etwa auf die Kölner OB oder diverse Brandanschläge auf Unterkünfte zeigen,⁶⁸ und damit den Tatbestand des § 241 StGB erfüllen.

Dasselbe dürfte für das Versenden einer fingierten Todesanzeige des Adressaten gelten;⁶⁹ zwar wird auch hier eine bestimmte Tat nicht angekündigt (nur der Erfolg des Todes), der Kontext kann aber ergeben, dass der Tod durch Handlungen der Absender eintreten soll.

Der Tatbestand der Bedrohung mit einem Verbrechen nach § 241 StGB ist daher in einigen der hier untersuchten Fällen durchaus gegeben, in anderen allerdings mangels Konkretisierung eines Verbrechens im Sinne des § 12 I StGB nicht.

⁶⁴ Eser/Eisele, in: Schönke/Schröder, StGB, § 241 Rn. 4.

⁶⁵ BGH NStZ-RR 2003, 45; Toepel, in: Kindhäuser/Neumann/Paefgen, StGB, § 241 Rn. 14.

⁶⁶ <http://www.faz.net/aktuell/politik/inland/drohungen-gegen-politiker-du-stinkende-ratte-13874653.html> (Abruf am 30.12.2015).

⁶⁷ DER SPIEGEL vom 24.10.2015, S. 25.

⁶⁸ <http://www.spiegel.de/panorama/justiz/henriette-reker-koeln-attentaeter-frank-s-war-vorbestraft-a-1058854.html>, Abruf am 30.10.2015.

⁶⁹ <http://www.faz.net/aktuell/politik/inland/drohungen-gegen-politiker-du-stinkende-ratte-13874653.html> (Abruf am 30.12.2015).

III. Strafbarkeitslücken

Zusammengefasst lässt sich sagen, dass für die hier untersuchten Fälle erhebliche Strafbarkeitslücken bestehen. Zwar sind Beleidigungen vom strafrechtlichen Schutz umfasst, die viel häufigeren Drohungen jedoch überwiegend nicht. Solche Drohungen beeinträchtigen das persönliche Empfinden oft ungleich mehr als Beleidigungen. Eine isolierte Drohung, die lediglich die Einschüchterung bezweckt, ist für sich genommen nur dann strafbar, wenn das angedrohte Verhalten ein Verbrechen darstellt (§ 241 StGB). Drohungen mit der Begehung eines Vergehens („wir schlagen dich krankenhausreif“) oder diffuse Drohungen („fühl dich nicht zu sicher“, „wir können jederzeit zuschlagen“) sind nach geltendem Recht nicht strafbar.

1. Vorschlag für die Einführung eines § 238a StGB

Die Massivität und der lange Zeitraum, in welchem Drohungen und Beleidigungen ausgesprochen oder sonst kommuniziert werden, stehen häufig den Beeinträchtigungen, wie sie Stalking-Opfer oft ausgesetzt sind, kaum nach. Dennoch ist eine Strafbarkeit nach § 238 StGB nur in wenigen Fällen gegeben.⁷⁰ Dies liegt vor allem darin begründet, dass die Taten nur selten zu einer „schwerwiegenden Beeinträchtigung der Lebensgestaltung“ führen und zudem die Taten nicht – im Hinblick auf eine einzelne Person – beharrlich erfolgen. Dennoch führen sie zu massiven psychischen Belastungen und Beeinträchtigungen, die Opfer leben manchmal in permanenter Angst um sich und ihre Familien. Nicht zuletzt ist aber auch die Funktionsfähigkeit des Staates selbst bedroht, wenn es aufgrund derartiger Umstände unattraktiv wird, sich um eine Führungsposition in Politik und Verwaltung zu bewerben. Aus diesem Grund ist es geboten, dass Strafgesetzbuch um eine weitere Bestimmung zu ergänzen, die sich darauf beschränkt, Amts- und Mandatsträger zu schützen und andererseits auf die Merkmale der Beharrlichkeit und der schwerwiegenden Beeinträchtigung der Lebensführung zu verzichten.

2. Wortlaut des § 238a StGB

§ 238a Nachstellung gegenüber Amts- und Mandatsträgern

„ Absatz 1: Wer einem Amts- oder Mandatsträger oder einem für den öffentlichen Dienst besonders Verpflichteten unbefugt nachstellt, indem er

1. seine räumliche Nähe privat aufsucht,
2. unter Verwendung von Telekommunikationsmitteln oder sonstigen Mitteln der Kommunikation oder über Dritte privat Kontakt zu ihm herzustellen versucht,
3. unter missbräuchlicher Verwendung von dessen personenbezogenen Daten Bestellungen von Waren oder Dienstleistungen für ihn aufgibt oder Dritte veranlasst, mit diesem Kontakt aufzunehmen,
4. ihn mit der Verletzung von Leben, körperlicher Unversehrtheit, Gesundheit oder Freiheit seiner selbst oder einer ihm nahe stehenden Person bedroht oder
5. eine andere vergleichbare Handlung vornimmt

und die Handlung für sich oder zusammen mit anderen Handlungen geeignet ist, seine Lebensführung zu beeinträchtigen

wird, sofern die Tat in Zusammenhang mit seiner Amts- oder Mandatsführung steht, mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

Absatz 2: Die Tat wird nur auf Antrag verfolgt.“

⁷⁰ Siehe oben unter 3.

3. Erläuterungen

a) Taugliche Tatopfer sind nur Amts- und Mandatsträger. Zum Amtsträgerbegriff kann auf § 11 I Nr. 2 StGB zurückgegriffen werden, zum Begriff des für den öffentlichen Dienst besonders Verpflichteten auf § 11 I Nr. 4 StGB. Mandatsträger sind der in § 108e StGB genannte Personenkreis; kommunale Mandatsträger, welche nach der Rechtsprechung des BGH nicht als Amtsträger anzusehen sind,⁷¹ werden von § 108e III n.F. erfasst.⁷²

b) Ebenso wie bei § 238 StGB ist erforderlich, dass die Tat unbefugt erfolgt. Hierdurch werden insbesondere Tätigkeiten, die in Wahrnehmung von Meinungs-, Presse oder Kunstfreiheit ausgeübt werden, von der Strafbarkeit ausgenommen; allerdings ist auch hier wie bei § 238 StGB eine Abwägung erforderlich, auch hier kann die Privatsphäre Vorrang haben.⁷³

c) Zusätzlich erforderlich ist hier ein Zusammenhang mit der Ausübung des öffentlichen Amtes. Ausgeschieden werden sollen somit Verhaltensweisen, die ihre Ursache in rein privaten Beziehungen haben, etwa vom früheren Ehegatten eines Amts- oder Mandatsträgers begangen werden und ihren Grund in dieser Beziehung haben.

Ist ein solcher privater Zusammenhang nicht ersichtlich, ist das Merkmal regelmäßig erfüllt, Anlass für das Verhalten gegenüber den Betroffenen ist meist deren Ausübung des Amtes oder Mandats oder in diesem Zusammenhang erfolgte Äußerungen. Das sollte auch für den in § 11 I Nr. 4 StGB genannten Personenkreis gelten.

d) Nicht erforderlich hingegen ist, dass die Tat beharrlich im Sinne des § 238 StGB erfolgen muss. Das Leitbild des § 238 StGB ist gekennzeichnet durch einen Täter, dessen wiederholte Taten gegenüber einem Opfer dieses in seiner persönlichen Situation erheblich beeinträchtigt. In den hier untersuchten Fällen mögen manche der Täter wiederholt und nachhaltig auftreten, die Beeinträchtigung ergibt sich aber regelmäßig nicht durch die Verhaltensweisen eines einzelnen oder einer Gruppe, bei welcher die Voraussetzungen der Mittäterschaft nach § 25 II StGB vorliegen, sondern aus einem Summierungseffekt durch Verhaltensweisen vieler untereinander nicht verbundener Täter. Dies rechtfertigt es, auf das Merkmal „beharrlich“ hier zu verzichten. Soweit durch das Merkmal erlaubte Verhaltensweisen ausgeschieden werden sollten,⁷⁴ kann insoweit auf das Merkmal unbefugt verwiesen werden.

e) Nicht erforderlich ist außerdem, dass die Tat zu einer schwerwiegenden Beeinträchtigung der Lebensführung geführt haben muss. Erforderlich ist bei § 238 StGB nach dem Willen des Gesetzgebers, dass es sich um „ins Gewicht fallende, gravierende und ernst zu nehmende Beeinträchtigungen, die über durchschnittliche, regelmäßig hinzunehmende und zumutbare Beeinträchtigungen erheblich und objektivierbar hinausgehen“⁷⁵, handelt. Bei § 238 StGB handelt es sich demnach um ein Erfolgsdelikt.

Diese Voraussetzung schränkt als objektiv messbare Auswirkung im Fall der Amts- und Mandatsträger die Strafbarkeit zu sehr ein. Häufig ändern die Betroffenen ihr Lebensumfeld dadurch nicht, leiden aber (ebenso wie ihre Familien) massiv unter den Taten, auch wenn sie ihr Leben nicht objektiv messbar verändern. Zudem würde eine objektive Änderung des

⁷¹ BGH NStZ 2006, 329.

⁷² Kritisch zur Neufassung Hoven, NStZ 2015, 553, 555; Jäckle, ZRP 2014, 121.

⁷³ Zu § 238 StGB Sonnen, in: Kindhäuser/Neumann/Paefgen, StGB, § 238 Rn. 50.

⁷⁴ Sonnen, in: Kindhäuser/Neumann/Paefgen, StGB, § 238 Rn. 52.

⁷⁵ BT-Drucks. 16/3641, 14.

Umfelds, wie etwa ein Wohnsitz- oder Arbeitsplatzwechsel, wie sie im Fall des „privaten Stalkings“ sinnvoll sein mag, hier nicht viel bewirken.

f) Die genannten Verhaltensweisen sind der Vorschrift des § 238 StGB entlehnt. Zu ihrer Auslegung kann auf die Rechtsprechung und Literatur zu § 238 StGB zurückgegriffen werden.

Einer Ergänzung bedürfen allerdings die Nr. 1 und 2, welche äußerlich sozialadäquates Verhalten darstellen. Hier ist eine Eingrenzung des Tatbestandes erforderlich. Daher ist die Einschränkung aufzunehmen, dass die Kontaktaufnahme bzw. das Aufsuchen der räumlichen Nähe privat erfolgen muss. Eine dienstliche Kontaktaufnahme mit einem Amts- oder Mandatsträger ist erlaubt, hier kann sich die Strafbarkeit nur aus anderen Tatbeständen (z.B. §§ 185, 241 StGB) ergeben.

In Abweichung von § 238 ist hier nicht zu fordern, dass eine Beeinträchtigung der Lebensführung tatsächlich eintritt. Es genügt wenn die Handlungen für sich genommen oder zusammen mit Handlungen anderer dazu oder zur Beeinträchtigung der Lebensführung oder Amts- oder Mandatsführung geeignet sind. Es handelt sich bei § 238a StGB daher um ein Eignungsdelikt, wie es der ursprünglichen Konzeption der Strafbarkeit der Nachstellung auch entspricht. Die Verhaltensweisen müssen also eine gewisse Schwere aufweisen und in einem Summierungseffekt eine Beeinträchtigung mit sich bringen können, was bei Drohungen (Nr. 4) regelmäßig der Fall sein dürfte. Ausgeschieden werden somit nur Handlungen, welche auch im Zusammenwirken mit anderen Handlungen als Bagatelle und als bloß lästig und nicht beeinträchtigend angesehen werden, was insbesondere bei Nr. 1 und 2 denkbar ist. Andererseits ist es nicht gerechtfertigt, eine Eignung zur „schwerwiegenden“ Beeinträchtigung zur Lebensführung zu fordern. Ein zumutbares Maß an Beeinträchtigung ist im Hinblick auf die Unerlaubtheit der Verhaltensweisen nicht anzunehmen, bloße Lästigkeiten werden durch das Erfordernis der Eignung bereits ausgeschlossen.

g) Eine Aufnahme in den Katalog der Privatklagedelikte (§ 374 StPO) sollte unterbleiben. Durch das Antragserfordernis ist bereits klargestellt, dass die Verfolgung vom Willen des Opfers abhängt. Ein öffentliches Interesse ist in diesem Fall stets gegeben.

IV. Ergebnis

Die hier untersuchten Verhaltensweisen der Beschimpfung und Bedrohung von Amts- und Mandatsträgern werden durch das geltende Strafrecht nur teilweise erfasst, es bestehen erhebliche Strafbarkeitslücken. Diese sollten durch Schaffung einer neuen Strafvorschrift einer „Nachstellung gegenüber Amts- und Mandatsträgern“ (§ 238a StGB) ausgeräumt werden. Soweit die Verhaltensweisen vom geltenden Strafrecht umfasst sind, wie das etwa im Bereich der Beleidigungsdelikte nach §§ 185 ff. StGB der Fall ist, besteht ein starkes Vollzugsdefizit in der Praxis, welchem ebenfalls dringend abgeholfen werden muss, etwa durch eine Entlastung der Staatsanwaltschaften und Gerichte in anderen Bereichen und der massive Aufbau von Stellen in der Justiz.

Schriftliche Stellungnahme im Rahmen der öffentlichen Anhörung zu

a) Gesetzentwurf der Fraktionen der CDU/CSU und SPD

Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (BT-Drucksache 19/17741)

b) Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (BT-Drucksache 19/18470)

Vorbemerkungen

Das NetzDG aus dem Jahr 2017 war zweifellos ein richtiger Ansatz zur Bekämpfung der Hasskriminalität im Internet. Gleichwohl hat sich gezeigt, dass die Löschung rechtswidriger Inhalte allein nicht ausreichend ist, um der zunehmenden Verrohung durch Hass und Hetze wirksam zu begegnen. Kernpunkt der nunmehr vorliegenden, umfassenden Gesetzentwürfe ist daher, die Voraussetzungen für eine effektive Strafverfolgung zu schaffen.

Die gesetzgeberische Zielsetzung der Ermöglichung einer effektiven Strafverfolgung wird die beteiligten (Ermittlungs-) Behörden vor eine beispiellose Mammutaufgabe im Bereich der Bekämpfung der Massenkriminalität stellen. Denn es ist nicht nur die immense Anzahl der zu erwartenden Meldungen, sondern insbesondere die Flüchtigkeit der zur Verfügung stehenden Daten, die – im Gegensatz zur „Offline-Massenkriminalität“ – die Ermittlung der Verantwortlichen erheblich erschweren wird.

Massenkriminalität erfolgreich zu bekämpfen setzt aus unserer langjährigen Erfahrung bei der Bekämpfung der Verbreitung der Kinderpornographie zunächst insbesondere voraus, dass der Rechtsrahmen, in dem die Beteiligten tätig werden, klar definiert ist.

Ferner müssen die einzelnen Abläufe organisiert, strukturiert und – jedenfalls soweit möglich – automatisiert sein.

Dies mag banal bzw. selbstverständlich klingen. Gleichwohl hat das bisherige Gesetzgebungsverfahren gezeigt, dass auch grundsätzliche Fragestellungen jedenfalls noch nicht abschließend geklärt sind, die für das Ziel der Ermöglichung einer effektiven Strafverfolgung von wesentlicher Bedeutung sein dürften.

Als Vertreter einer Strafverfolgungsbehörde möchte ich in diesem fortgeschrittenen Stadium des Gesetzgebungsverfahrens und aufgrund der Vielzahl bereits vorliegender Stellungnahmen das Augenmerk ganz bewusst nur auf wenige, für die Effizienz der Strafverfolgung jedoch immens wichtige Punkte lenken, auf die der bisherige Diskurs noch nicht oder jedenfalls nicht primär gerichtet war.

I. Klarstellung der Aufgaben des Bundeskriminalamts

Auf eine wesentliche, sich im Kern nicht einmal aus dem Text des Gesetzentwurfs selbst, sondern vielmehr aus der Gesetzesbegründung ergebende Problemstellung hat der Bundesrat in seiner Stellungnahme vom 27.03.2020 (Drs. 87/20, S. 13 f.) hingewiesen. § 3a Absatz 2 NetzDG-E sieht vor, dass das Bundeskriminalamt (BKA) die Meldungen als Zentralstelle zum Zwecke der „Ermöglichung der Verfolgung von Straftaten“ entgegennimmt. Eine eindeutige Bestimmung, welche Aufgaben das BKA als Zentralstelle wahrnimmt, ergibt sich – wie der Bundesrat zu Recht feststellt – hieraus nicht.

Die sich aus der Gesetzesbegründung ergebende Aufgabenbeschreibung dagegen erscheint bislang zumindest missverständlich, wenn sie einerseits feststellt, dass sich die Tätigkeit des BKA im Rahmen der Zentralstellenfunktion auf die Maßnahmen beschränkt, die erforderlich sind, um die zuständige Strafverfolgungsbehörde auf Landesebene festzustellen andererseits aber davon ausgeht, dass das BKA „...nach Einschätzung, ob es sich um einen strafbaren Inhalt handelt, die beim sozialen Netzwerk gespeicherten Daten, soweit sie zur Identifizierung des Verfassers erforderlich sind, anfordern und diese Daten der zuständigen Strafverfolgungsbehörde in den Ländern übermitteln...“ wird.

Im Kern geht es darum, ob das BKA zunächst eine Bewertung der Meldung auf strafrechtliche Relevanz vornehmen darf oder muss, bevor es die übermittelte IP-Adresse

beim Access-Provider abfragt. Nach hiesiger Einschätzung ist das BKA hierzu sogar gesetzlich verpflichtet.

Der Bundesrat weist in diesem Zusammenhang zu Recht darauf hin, dass auch in der analogen Welt die Polizei nicht sämtliche ihr zugetragenen Erkenntnisse ungefiltert der Staatsanwaltschaft übermittelt werden. Die Vorlagepflicht der Polizeibehörden des § 163 Abs. 2 StPO besteht nämlich gerade nicht, wenn bereits der Anfangsverdacht einer Straftat, die Voraussetzung für den sog. „ersten Zugriff“ – also die beweissichernden Erstmaßnahmen – nicht vorliegt.

Hinzu kommt, dass die qualifizierte Bestandsdatenabfrage des § 10 Abs. 2 BKAG zumindest „einen hinreichenden Anfangsverdacht gemäß den §§ 161, 163 StPO oder eine konkrete Gefahr im Sinne der polizeilichen Generalklausel“ voraussetzt (*Schenke/Graulich/Ruthig*, Sicherheitsrecht des Bundes, § 10 BKAG, Rn. 19) voraussetzt. Eine Abfrage gem. § 10 Abs. 2 BKAG ohne jegliche Prüfung, ob die Meldung überhaupt einen strafrechtlich relevanten Inhalt aufweist, wäre daher nicht rechtmäßig und würde, wie der Bundesrat feststellt, eine Vertiefung des Eingriffs in das Grundrecht auf informationelle Selbstbestimmung der Nutzer zur Folge haben, die mangels Erforderlichkeit auch datenschutzrechtlich bedenklich wäre.

Das mögliche (Gegen-) Argument, es habe bereits eine Prüfung auf strafrechtliche Relevanz durch die sozialen Netzwerke stattgefunden, verkennt, dass es sich bei den Tatbeständen des § 3 Abs. 2 Nr. 3. NetzDG-E überwiegend um komplexe Vorschriften handelt, deren Bewertung vertiefte juristische Kenntnisse voraussetzt. Die Erfahrungen, die meine Zentralstelle in Zusammenarbeit mit Nichtregierungsorganisationen im Zuge des Aktionsprogramms der hessischen Landesregierung unter dem Schlagwort #HessengegenHetze gemacht hat, zeigen, dass von den übermittelten Meldungen – obgleich die Kooperationspartner teils juristisch geschult waren – über 60 Prozent als strafrechtlich nicht relevant eingestuft werden mussten. Es wäre also zu befürchten, dass – ohne jegliche Prüfung durch das BKA – in vielen tausend Fällen zu Unrecht Bestandsdatenabfragen erfolgen und strafrechtlich irrelevante Sachverhalte an die Strafverfolgungsbehörden übermittelt würden.

Eine weitere Problemstellung, die sich unmittelbar an die Frage der Aufgaben des BKA als Zentralstelle anschließt und die bislang noch nicht explizit behandelt wurde, ist die

Frage, ob mit der Bejahung des Anfangsverdacht und der Bestandsdatenabfrage bereits die Phase des strafrechtlichen Ermittlungsverfahrens begründet ist.

Der Bundesrat hat in diesem Zusammenhang zu Recht darauf hingewiesen, dass mit der Implementierung der Meldepflicht für Plattformbetreiber verhindert werden soll, dass strafbare Inhalte im Netz gelöscht und damit der strafrechtlichen Würdigung und gegebenenfalls Verfolgung entzogen werden. Die Meldung ist damit gerade keine das Ermittlungsverfahren auslösende Strafanzeige gemäß § 158 StPO, denn sie enthält kein eigenes Prüfungsbegehren des Plattformbetreibers. Vielmehr erfolgt sie gleichsam „neutral“ in Erfüllung einer dem Plattformbetreiber auferlegten gesetzlichen Pflicht. Schließlich spricht auch der Wortlaut des § 3a Absatz 2 NetzDG-E, dass die Meldepflicht den Zweck verfolge, den zuständigen Behörden die Verfolgung etwaiger Straftaten zu „ermöglichen“, dafür, dass die Tätigkeit des BKA in dieser Phase reine Zentralstellentätigkeit im Sinne des § 2 BKAG mit der Folge darstellt, dass Sachverhalte, die als strafrechtlich irrelevant bewertet wurden, weder bei einer Staatsanwaltschaft erfasst, noch von dieser „zweitbewertet“ und auch keiner förmlichen Einstellung zugeführt werden müssen.

Der Befürchtung, dass durch das BKA aufgrund der Komplexität der Tatbestände Sachverhalte ausgeschieden werden, die mglw. durch Staatsanwaltschaften für strafrechtlich relevant erachtet werden könnten, ist durch umfangreiche Schulungsmaßnahmen zu begegnen. So hat sich die in diesem Bereich langjährig tätige und mit besonderer Expertise ausgestattete Zentral- und Ansprechstelle Cybercrime NRW (ZAC) der Staatsanwaltschaft Köln, die sich gemeinsam mit meiner Zentralstelle bereits zu Beginn des Gesetzgebungsverfahrens mit dem BKA ins Benehmen gesetzt hat, um eine möglichst reibungslose Umsetzung des Gesetzes zu gewährleisten bereit erklärt, durch umfassende und fortlaufende Aus- und Fortbildungsmaßnahmen unterstützend tätig zu werden.

II. Klarstellung der (unmöglichen) Effizienz der Strafverfolgung

Im Gegensatz zu der Auffassung der Bundesregierung, die davon auszugehen scheint, dass mit den dem BKA übermittelten Daten und der im Rahmen der Zentralstellenfunktion zulässigen Abfragemöglichkeiten ein hoher Prozentsatz der Poster rechtswidriger Inhalte identifizierbar sein wird, ist aus der hiesigen, langjährigen Praxis davon auszugehen, dass lediglich ein relativ geringer Anteil derjenigen Personen, die für solche

rechtswidrigen Inhalte verantwortlich sind, allein durch (qualifizierte) Bestandsdatenabfragen ermittelbar sein wird.

Die unter Artikel 5 Ziffer 3 vorgeschlagene Vorschrift des § 3a Abs. 4 Nr. 2 NetzDG-E, welche die Übermittlung von „vorhandenen“ IP-Adressen und Portnummern an das BKA vorsieht und die zur Identifizierung der Verantwortlichen führen soll, wird in der Praxis weitgehend leerlaufen.

Obwohl Telemediendiensteanbieter bereits bisher IP-Adressen grundsätzlich auch über das Ende des Nutzungsvorgangs hinaus speichern dürfen (vgl. BGH NJW 2017, 2416), wird jedenfalls die für die Zuordnung zu einem Anschluss so wichtige Portnummer nach hiesiger Kenntnis von den Telemediendiensten derzeit mangels gesetzlicher Verpflichtung auch nicht gespeichert, sodass aufgrund der Tatsache, dass die Telekommunikationsdienste bei mobilen Endgerätenutzung durch Nutzung des sog. NAT-Verfahrens eine IP-Adresse vielfach vergeben, eine Zuordnung zum Anschlussinhaber allein aufgrund der gem. § 3a Abs. 4 Nr. 1 NetzDG-E übermittelten IP-Adresse ohne Portnummer nicht möglich sein wird. Aber selbst, wenn Portnummern erhoben und übermittelt werden würden, wäre eine Zuordnung schon deshalb nicht möglich, da die deutschen Telekommunikationsdiensteanbieter aufgrund mangelnder gesetzlicher Verpflichtung eine Speicherung von Portnummern nicht vornehmen. Schließlich besteht auch für den Fall, dass bei der Nutzung von Desktop-PCs vereinzelt Diensteanbieter kein Carrier-grade NAT verwenden, grundsätzlich die Problematik, dass aufgrund nicht erfolgter Umsetzung des § 100g Abs. 2 StPO, der aber ohnehin viele Tatbestände des § 3a Abs. 2 Nr. 3 NetzDG-E nicht enthält, eine Speicherung von IP-Adressen auf der Grundlage des § 100 TKG für höchstens 6 Tage vorgenommen wird, wobei viele Diensteanbieter die Verkehrsdaten unmittelbar nach Beendigung der Telekommunikationsverbindung löschen.

Diese rechtliche Einschätzung wird untermauert durch die Erkenntnisse aus den sog. „NCMEC-Verfahren“, in denen – sehr vergleichbar mit dem hiesigen Gesetzesvorhaben - durch amerikanische Diensteanbieter (u.a. auch soziale Netzwerke wie Facebook oder WhatsApp) nicht nur Login-IP-Adressen, sondern darüber hinaus gehend auch die Bestandsdaten von Nutzern, die für die Verbreitung von Kinderpornographie verantwortlich sind, über die private, gemeinnützige Organisation NCMEC dem BKA stellt zur Verfügung gestellt werden. Obgleich mangels umgesetzter Vorratsdatenspeicherung dem BKA als einziger Polizeibehörde weltweit der unmittelbare Zugriff auf die Datenbank von NCMEC zusteht, scheitert in über der Hälfte der Fälle die Identifizierung bereits von

vornherein daran, dass die IP-Adresse durch Zeitablauf nicht mehr zuzuordnen ist oder mobile Endgeräte genutzt wurden.

Um eine solch hohe Quote an nichtidentifizierten Postern zu vermeiden und dem Legalitätsprinzip zu entsprechen, wird daher in einem zweiten Schritt das BKA die strafrechtlich relevanten, aber nicht ermittelbaren Sachverhalten „von Amts wegen“ einer oder mehrerer Staatsanwaltschaften vorlegen müssen, damit diese eine Identifizierung mit den über die Möglichkeiten des BKAG hinausgehenden Ermittlungsinstrumentarien der Strafprozessordnung versuchen.

Da zu diesem Zeitpunkt weder Täter noch Tatort feststehen, besteht gem. § 143 I 2 GVG die Möglichkeit, dass das BKA eine Staatsanwaltschaft „erstbefasst“, die in diesen Fällen als „Identifizierungsstaatsanwaltschaft“ tätig wird und nach erfolgreicher Ermittlung das Verfahren an die örtlich zuständige Staatsanwaltschaft abgibt.

Meine Zentralstelle, die diese Funktion in unterschiedlichsten Kriminalitätsfeldern seit vielen Jahren in enger Zusammenarbeit mit dem BKA ausfüllt und die Verfahrensabläufe im Bereich der Massenkriminalität strukturiert und automatisiert hat, hat sich auch in den Fällen der Hasskriminalität bereit erklärt, identifizierend tätig zu werden.

Allerdings – und insoweit muss eindringlich gewarnt werden – wird eine Identifizierung auch mit den Mitteln der Strafprozessordnung weder flächendeckend oder auch nur überwiegend möglich sein.

Zwar könnten sich weitere Ermittlungsansätze aus den bei den sozialen Netzwerken hinterlegten Bestandsdaten ergeben. § 15a TMG-E schafft auch die Voraussetzung für die Beauskunftung von Bestands- und Nutzungsdaten gegenüber Telemediendiensteanbietern. Im Gegensatz zu den Anbietern von Telekommunikationsdienstleistungen, die gemäß § 111 TKG verpflichtet sind, Kundendaten zu erheben und diese bei Prepaid-Produkten auf ihre Richtigkeit hin zu überprüfen, findet sich eine solche Datenspeicherungs- und Überprüfungsverpflichtung in den Gesetzentwürfen betreffend das TMG jedoch nicht vor. Im Ergebnis bedeutet dies, dass bei Telemediendiensten, die von einer Erhebung von Bestands- und Nutzungsdaten absehen, eine Zuordnung der Beweismittel (bspw. der Screenshots der strafrechtlich relevanten Postings) zu einem Tatverdächtigen von vornherein ausgeschlossen sein wird. Erhebt der Telemediendienst zwar Bestandsdaten, sieht aber – zulässigerweise und wie derzeit üblich – von einer Identitätsprüfung des Nutzers ab, ist auch der Auskunftsanspruch gemäß § 100j Abs. 1 Satz 1 Nr.2 TMG-E nicht zielführend, denn der Tatverdächtige, der seinen Ac-

count nutzt, um strafbare Inhalte zu posten, wird diesen in aller Regel unter Falschpersonalien anlegen.

Zudem ist zu berücksichtigen, dass die NetzDG-relevanten Anbieter sozialer Netzwerke diese Bestandsdaten jeweils im Ausland vorhalten, so dass eine unmittelbare Beauskunftung an das BKA oder andere Strafverfolgungsbehörden ausschließlich im Rahmen einer freiwilligen Kooperation erfolgen kann. Aus den Erfahrungen meiner Zentralstelle bei der Verfolgung von Hasskommentaren im Internet ist dabei allerdings festzustellen, dass die Anbieter Sozialer Netzwerke nur in wenigen Ausnahmefällen Bestandsdaten ihrer Kunden freiwillig herausgeben. Anderenfalls müsste die Erhebung der Bestandsdaten bei den Anbietern sozialer Netzwerke im Wege der förmlichen internationalen Rechtshilfe erfolgen, was in vielen Fällen der Massenkriminalität kaum verhältnismäßig sein dürfte.

Da sich aus der hiesigen Praxis im Rahmen der NCMEC-Verfahren jedoch gezeigt hat, dass sich aus den hinterlegten Bestandsdaten immer wieder Ermittlungsansätze zur Identifizierung der Nutzer (bspw. Kontakt-E-Mail-Adressen; hinterlegte Telefonnummern) ergeben haben, wäre es absolut wünschenswert, wenn diese Daten neben den Inhalten und der IP-Adresse mit ausgeleitet werden würden. Durch das BKA könnten diese Datenabfragen dann aufgrund der Erweiterung des § 10 BKAG auf Telemediendienste dann auch im Rahmen der Zentralstellentätigkeit erfolgen. Eine Abfrage der Nutzungsdaten durch Staatsanwaltschaften wäre durch die beabsichtigte Änderung des § 100g StPO, die einen Richtervorbehalt vorsieht, erheblich erschwert und verzögert.

Andere grundsätzlich denkbare Ermittlungsmaßnahmen, insbesondere verdeckte technische oder personale Ermittlungshandlungen sind bereits wegen des damit verbundenen Aufwandes zur Bekämpfung der Massenkriminalität ungeeignet und allenfalls bei herausragenden Fällen einsetzbar.

Es wird daher – zusammenfassend – gebeten,

a) zu Klarstellungszwecken im weiteren Gesetzgebungsvorhaben festzustellen, dass das BKA nach den Vorgaben des NetzDG-E im Rahmen der sich aus § 2 BKAG ergebenden Zentralstellenfunktion tätig wird, die auch eine Bewertung der übermittelten Inhalte auf deren strafrechtliche Relevanz umfasst.

Die vom Bundeskriminalamt als nicht strafbar bewerteten Inhalte, sind - da die Phase des Ermittlungsverfahrens nicht eröffnet ist - weder einer Staatsanwalt-

schaft zur Prüfung oder Erfassung vorzulegen und auch keiner förmlichen Einstellung zuzuführen

b) zu prüfen, ob § 3a Abs. 4 NetzDG-E um eine Verpflichtung der Sozialen Netzwerke zur Übermittlung der dort hinterlegten Bestandsdaten erweitert werden könnte.

Frankfurt am Main, den 05.05.2020

gez. May

Leitender Oberstaatsanwalt

Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität

Hier: Öffentliche Anhörung des Ausschusses für Recht und Verbraucherschutz

am Mittwoch, 6. Mai 2020, 11:00 Uhr

- Eingangsstatement Jürgen Peter, Vizepräsident beim Bundeskriminalamt -

1. Notwendigkeit des Gesetzentwurfs

- Die Fallzahlen im Phänomenbereich PMK -rechts- stellen seit Jahren mit mehr als der Hälfte des Gesamtaufkommens den mit Abstand größten Anteil der Straftaten innerhalb der Politisch motivierten Kriminalität (PMK). Der aktuelle Verfassungsschutzbericht beziffert das gewaltbereite Personenpotenzial rechts auf 12.700 Personen. Der Mord am Regierungspräsidenten Dr. Walter Lübcke am 02.06.2019, der antisemitisch motivierte/fremdenfeindliche Anschlag am 09.10.2019 in Halle sowie der fremdenfeindlich und rassistisch motivierte Anschlag in Hanau am 19.02.2020 sind traurige und entsetzliche Höhepunkte einer bedenklichen Entwicklung.
- Neben fremdenfeindlich motivierter Aggression richten sich die Angriffe zunehmend gegen engagierte Vertreterinnen und Vertreter der Zivilgesellschaft und Repräsentantinnen bzw. Repräsentanten der Bundesrepublik. Das Internet bietet dabei Raum für Verbalradikalismus, Outings politischer Gegner oder Hasspostings. 2018 wurden fast 1.800 Delikte im Bereich der Hasskriminalität und knapp 1.500 sog. Hasspostings festgestellt. Das tatsächliche Volumen ist viel größer, das Entdeckungs- und Verfolgungsrisiko ist gering!
- Auch bei der Verbreitung kinderpornografischer Inhalte spielt das Internet eine bedeutende Rolle, Tendenz steigend! Im Jahr 2019 wurden fast 13.000 Fälle von Verbreitung, Erwerb und Besitz kinderpornografischer Schriften (§ 184 b StGB) in der Polizeilichen Kriminalstatistik erfasst. Dies entspricht einem Zuwachs von 64,6 % im Vergleich zum Vorjahr.

- Zum Umgang mit strafbaren Inhalten auf sozialen Plattformen markiert das am 01.10.2017 in Kraft getretene NetzDG einen Schritt in die richtige Richtung, diese Plattformen von strafbaren Inhalten zu befreien, indem diese vom Anbieter gelöscht werden.
- Ausweislich der Transparenzberichte wurden vom ersten Halbjahr 2018 bis zum zweiten Halbjahr 2019 rund 2,9 Mio. Beschwerden erfasst, von denen im Durchschnitt ca. 28 % gelöscht wurden.
- Damit werden zwar Inhalte gelöscht, die Verursacher bleiben in der Regel anonym und haben keine Strafverfolgung zu fürchten. Ziel muss sein, strafrechtlich relevante Sachverhalte künftig der Strafverfolgung zuzuführen. Dies sieht der vorliegende Gesetzentwurf vor.

2. Allgemeines zum Gesetzentwurf

Die Inhalte des Gesetzentwurfs, u. a.

- die Verpflichtung sozialer Netzwerke mit mehr als 2 Millionen in Deutschland registrierten Nutzern, bestimmte strafbare Inhalte an das BKA weiterzuleiten, die den sozialen Netzwerken zuvor im Rahmen einer Beschwerde gemeldet und von ihnen gesperrt oder entfernt wurden und
- die Ergänzung einer expliziten Befugnis zur Erhebung von Bestandsdaten auch bei Telemediendiensten für die Aufgabe des BKA als Zentralstelle nach § 2 BKAG.

sind wichtige Fortschritte bei der Bekämpfung von Straftaten im Internet. Mit diesen Regelungen ist die Grundlage geschaffen, die ausgeleiteten Inhalte im Bundeskriminalamt zentral zu sichten und die Voraussetzung zu schaffen, dass Strafverfolgungsmaßnahmen sowie gefahrenabwehrende Maßnahmen durch die örtlich zuständigen Behörden eingeleitet werden können. So lassen sich Sachverhalte aus der Anonymität des Netzes systematisch und effektiv in die Strafverfolgungszuständigkeiten eines föderal aufgebauten Systems der Strafverfolgung transferieren. Gleiches gilt für festgestellte Gefährdungssachverhalte. Die Zuständigkeiten von Polizeien und Justiz der Länder bleiben gewahrt, das BKA nimmt seine gesetzliche Rolle als Zentralstelle

wahr, Informationen zu sammeln und auszuwerten, um dann die Strafverfolgungsbehörden des Bundes und der Länder über die sie betreffenden Informationen und in Erfahrung gebrachten Zusammenhänge von Straftaten zu unterrichten (§ 2 II Nr. 1, 2 BKAG). In Ausnahmefällen ist die dann erforderliche Strafverfolgung durch das BKA selbst gem. § 4 BKAG genauso gesichert wie die Bewertung, ob Maßnahmen zum Schutz von Verfassungsorganen (§ 6 BKAG) oder solche zur Abwehr von Gefahren des internationalen Terrorismus (§ 5 BKAG) zu treffen sind.

Für den Bereich der Verbreitung kinderpornografischer Inhalte haben wir bereits einen solchen Geschäftsprozess zusammen mit der ZIT der GenStA Frankfurt am Main etabliert, um die vom US-amerikanischen National Center of missing and exploited Children (NCMEC) übermittelten Inhalte zu bearbeiten.

Auch die übrigen vorgesehenen Änderungen in der StPO (explizite Befugnis zur Erhebung von Bestands- und Nutzungsdaten beim Telemediendienst), Änderungen (Präzisierungen, tatbestandliche Schärfungen) im StGB, Änderungen im TMG sowie dem BMG werden begrüßt.

3. Forderungen des BKA

Gleichwohl besteht aus Sicht des BKA darüber hinaus folgender Rechtssetzungsbedarf:

a. BKAG: Schaffung einer Befugnisnorm zur Erhebung der IP-Adresse beim Telemediendienst im Rahmen der Zentralstellenaufgabe des BKA.

Begründung:

- Es sollte dem BKA möglich sein, im Rahmen seiner Aufgabenwahrnehmung proaktiv – d. h., wenn das BKA selbst rechtswidrige Inhalte feststellt - bei Telemediendiensten die zu Identifizierungszwecken wichtige IP-Adresse erheben zu dürfen.
- Es entstünde ein Widerspruch, wenn das BKA den Urheber eines strafbaren Inhalts aufgrund einer NetzDG-Meldung ermitteln kann, nicht

aber, wenn es bei eigenen Recherchetätigkeiten im Rahmen seiner gesetzlichen Aufgaben oder durch Hinweise Dritter auf strafbare Inhalte stößt.

b. StPO/BKAG: Erhebung der IP-Adresse beim Telemediendienst im Rahmen der Strafverfolgung sowie Zentralstellenaufgabe des BKA ohne Richtervorbehalt:

- Die Erhebung der IP-Adresse in seiner Eigenschaft als Nutzungsdatum nach dem TMG erfolgt bislang im Rahmen der Strafverfolgung in aller Regel über die Generalklausel (§§ 161, 163 StPO).
- Nach dem aktuellen Gesetzentwurf unterfiele diese Maßnahme § 100g StPO und wäre damit unter Richtervorbehalt gestellt.
- Die Befugnis sollte als Standardmaßnahme im Bereich der Internetermittlungen auch weiterhin ohne Richtervorbehalt durchgeführt werden können.
- Gleiches gilt für eine entsprechende noch zu regelnde Befugnis im BKAG, s.o. schon unter a).

Begründung:

- Die IP-Adresse selbst gibt – anders als die in § 15 Abs. 1 S. 1 Nr. 3 des TMG genannten Daten – keinen Aufschluss über den inhaltlichen Gegenstand der konkreten Inanspruchnahme der Telemediendienstleistung, so dass aufgrund der geringeren Eingriffstiefe diese eher einem Bestandsdatum entsprechen und ein Auskunftersuchen daher keiner richterlichen Anordnung bedarf.
- Sie ist zudem Vorstufe der sich hieran anschließenden Bestandsdatenabfrage beim TK-Dienst nach § 100j StPO anhand der erhobenen IP-Adresse, welche ebenfalls nicht unter Richtervorbehalt steht.
- Dies gilt im Besonderen auch vor dem Hintergrund der Zeitkritikalität, da derzeit die IP-Adressen durch die TK-Dienstleister nur wenige Tage gespeichert werden.

c. StGB: Schaffung eines Straftatbestandes, der Fallkonstellationen wie etwa das Erstellen und Verbreiten von sogenannten „Feindeslisten“ oder ähnlicher Listen erfasst

Begründung:

- Der Gesetzesentwurf sieht Änderungen vor, die dem Phänomen der sog. „Feindeslisten“ begegnen sollen. Das ist deshalb zu begrüßen, weil die Veröffentlichung solcher Listen geeignet ist, die Betroffenen erheblich einzuschüchtern
- Problematisch bleibt allerdings, dass diese Gesetzesänderungen nicht alle Konstellationen erfassen werden.
- Insbesondere bliebe die bloße Veröffentlichung einer Liste mit personenbezogenen Daten ohne weitergehende Bedrohung bzw. Billigung einer in § 140 StGB aufgenommenen Katalogtat in der Regel straffrei, weil diese Handlung von der Rechtsänderung nicht erfasst ist. Zur Schließung dieser Strafbarkeitslücke bedarf es eines neuen Straftatbestandes, der unter Strafe stellt, personenbezogene Daten zu veröffentlichen, um bei anderen die Bereitschaft zu wecken, Straftaten gegen die betroffenen Personen zu begehen.

Die im aktuellen Gesetzgebungsverfahren vorliegenden Rechtsänderungen sind erforderlich und geeignet, strafrechtliches Handeln aus der scheinbaren Anonymität des Netzes in die Realwelt unserer Rechts- und Werteordnung zu transportieren. Allein dieser Umstand kann generalpräventiv wirken. Gehalt, Volumen und Reichweite der Inhalte, die ich beschrieben habe, sind ansonsten geeignet, Vertrauen in die Fähigkeiten des Staates zum Schutz seiner Bürger sowie der freiheitlichen und demokratischen Rechtsordnung zu beeinträchtigen. Lassen Sie mich abschließend an die von Hass erfüllte Agitation gegen Flüchtlinge erinnern, die den Nährboden für Angriffe auf Flüchtlingsunterkünfte erst geschaffen hat, die Bedrohungen und Einschüchterungen von Kommunalpolitikern, die sich nicht mehr zu helfen wussten, als ihre Mandate aufzugeben, die Veröffentlichung sog. „Feindeslisten“ mit der Diskussion um die damit verursachte Verunsicherung der Betroffenen und nicht zuletzt an das im

Netz geteilte und weiter verbreitete kinderpornografische Material. Die Opfer von Missbrauch werden dauerhaft viktimisiert.



Deutscher Landkreistag, Postfach 11 02 52, 10832 Berlin

Ulrich-von-Hassell-Haus
Lennéstraße 11
10785 Berlin

Herrn
Prof. Dr. Heribert Hirte, MdB
Vorsitzender des Ausschusses für Recht
und Verbraucherschutz
Deutscher Bundestag
Platz der Republik 1
11011 Berlin

Tel.: 0 30 / 59 00 97 – 3 21
Fax: 0 30 / 59 00 97 – 4 00

E-Mail: Klaus.Ritgen
@Landkreistag.de

AZ: II/21

Datum: 4.5.2020

Nur per Mail an: rechtsausschuss@bundestag.de

Stellungnahme zum

- a) **Gesetzentwurf der Fraktionen der CDU/CSU und SPD**
Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität
BT-Drucksache 19/17741
- b) **Gesetzentwurf der Bundesregierung**
Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität
BT-Drucksache 19/18470

Sehr geehrter Herr Prof. Dr. Hirte,
sehr geehrte Damen und Herren,

der Deutsche Landkreistag bedankt sich für die Einladung zur öffentlichen Anhörung über die o.g., inhaltlich gleichlautenden Gesetzentwürfe und die Möglichkeit, dazu vorab eine Stellungnahme abzugeben. Von dieser Möglichkeit machen wir gerne Gebrauch, wobei wir uns im Folgenden auf die vorgeschlagenen Änderungen in §§ 115, 185, 188, 194 und 241 StGB konzentrieren werden.

Mit diesen Änderungen soll klargestellt werden, dass der Tatbestand des § 188 („Üble Nachrede und Verleumdung gegen Personen des politischen Lebens“) auch dem Schutz von Personen dient, die auf kommunaler Ebene politisch aktiv sind. Durch die Änderung in § 194 StGB soll erreicht werden, dass Taten nach § 188 StGB – vorbehaltlich eines Widerspruchs der berechtigten Person – auch von Amts wegen zu verfolgen sind. In § 241 StGB schließlich soll der Tatbestand der Bedrohung ausgeweitet werden. Bedeutsam sind aus unserer Sicht ferner die zu den §§ 115 und 185 vorgeschlagenen Änderungen. Durch die Änderung des § 115 Abs. 3 Satz 1 StGB sollen Hilfeleistende eines ärztlichen Notdienstes und in Notaufnahmen besser als bislang geschützt werden. § 185 StGB schließlich soll durch einen Qualifikationstatbestand ergänzt werden, wonach mit bis zu zwei Jahren Freiheitsstrafe bestraft werden kann, wer beleidigende Äußerungen öffentlich, in einer Versammlung oder durch Verbreiten von Schriften – also insbesondere auch über das Internet – äußert.

Alle diese Änderungen sind aus Sicht des Deutschen Landkreistages zu begrüßen, weil damit der strafrechtliche Schutz von Kommunalpolitikern vor Hass und Bedrohung verbessert werden soll.

Wir betrachten mit großer Sorge, dass sich die Zahl der verbalen und körperlichen Angriffe gegen öffentliche Bedienstete deutlich erhöht hat. Landräte, ehrenamtliche Mitglieder der Kreistage, aber auch Mitarbeiter in den Sozial- und Jugendämtern, den Ausländerbehörden, den Veterinärämtern und anderer Stellen der Kreisverwaltung werden immer öfter Opfer von Beleidigungen, Drohungen und auch tätlicher Gewalt. All dies ist auch Ausdruck eines zunehmenden Werteverfalls in unserer Gesellschaft. Sachlichkeit, Respekt dem Mitmenschen gegenüber, die Fähigkeit des Zuhörens, des persönlichen Gesprächs und Auseinandersetzens mit der Meinung des anderen gehen zusehends verloren. Sachbeschädigungen, Beleidigungen und Drohungen jeglicher Art, vor allem in den Social-Media-Kanälen und meist in anonymisierter Form nehmen nicht zuletzt seit der Flüchtlingskrise zu und dürften im Zuge der aktuellen Corona-Pandemie ebenfalls wieder an Relevanz gewinnen.

Derartige Attacken sind unerträglich. Wir müssen daher im täglichen Miteinander immer wieder deutlich machen, dass wir so etwas in unserer Gesellschaft keinesfalls dulden. Schon Anfang 2018 hat das Präsidium des Deutschen Landkreistages die Resolution „Keine Gewalt gegen öffentlich Bedienstete“ beschlossen, die ihre Aktualität nicht eingebüßt hat und dieser Stellungnahme als **Anlage** beigefügt ist.

Neben die soziale bzw. gesellschaftliche Ächtung eines entsprechenden Verhaltens müssen derartige verbale und tätliche Angriffe auch mit dem rechtsstaatlichen Instrumentarium konsequent geahndet werden. Dort, wo dieses Instrumentarium (noch) nicht ausreicht, muss es nachgeschärft werden, wie das mit den vorliegenden Gesetzentwürfen sowohl durch Änderungen im materiellen Strafrecht (insbesondere §§ 115, 185, 188, 194, 241 StGB) wie durch Änderungen im Netzwerkdurchsetzungsgesetz und flankierender Bestimmungen in der Strafprozessordnung, dem Bundeskriminalamtsgesetz und dem Telemediengesetz geschehen soll. Auch die Änderung des Bundesmeldegesetzes, durch die insbesondere Personen besser geschützt werden sollen, die durch ihr berufliches oder ehrenamtliches Engagement – bspw. im kommunalpolitischen Bereich – in den Fokus gewaltbereiter Personen oder Gruppen geraten, ist zu begrüßen.

Im Einzelnen ist auf folgende Änderungen besonders hinzuweisen:

- **Artikel 1 Nr. 7 (§ 188 StGB)**

Durch die Änderung in § 188 StGB wollen die Fraktionen der CDU/CSU und SPD sowie die Bundesregierung sicherstellen, dass der Schutzbereich der Vorschrift sich auch auf die auf kommunaler Ebene politisch Aktiven erstreckt. Dies soll dadurch erreicht werden, dass § 188 Abs. 1 StGB um den Satz „Das politische Leben des Volkes reicht bis hin zur kommunalen Ebene“ ergänzt wird. Demgegenüber schlägt der Bundesrat vor, dem § 188 StGB einen klarstellenden Absatz beizufügen, aus dem sich ergibt, dass „eine im politischen Leben des Volkes stehende Person im Sinne von Absatz 1“ auch eine Person ist, die „auf Ebene einer für ein Teilgebiet eines Landes oder einer kommunalen Gebietskörperschaft gebildeten Verwaltungseinheit aktiv tätig ist“.

Das Anliegen des Änderungsvorschlags der Fraktionen sowie der Bundesregierung wird seitens des Deutschen Landkreistags ausdrücklich unterstützt. Wir regen allerdings an, die vom Bundesrat vorgeschlagene Regelungsvariante zu übernehmen, da diese schon sprachlich klarer und eindeutiger ist und Abgrenzungsprobleme vermeidet.

- **Artikel 1 Nr. 8 (§ 194 StGB):**

Der Deutsche Landkreistag begrüßt es, dass Delikte nach § 188 StGB in der geänderten Fassung auch von Amts wegen verfolgt werden können. Durch das Widerspruchsrecht in § 194 Abs. 1 Satz 4 StGB-E ist ausreichend gewährleistet, dass der Verletzte eine Ermittlung von Amts wegen verhindern kann.

- **Artikel 1 Nr. 9 (§ 241 StGB):**

Die Fraktionen von CDU/CSU und SPD sowie die Bundesregierung schlagen vor, den Tatbestand der Bedrohung auszuweiten und auch die Androhung einer rechtswidrigen Tat gegen die sexuelle Selbstbestimmung, die körperlicher Unversehrtheit, die persönliche Freiheit oder gegen eine Sache von bedeutendem Wert in diesen einzubeziehen. Der Bundesrat regt demgegenüber an, diese Ausweitung – soweit es um die sexuelle Selbstbestimmung und die körperliche Unversehrtheit geht – unter den Vorbehalt zu stellen, dass die Tat mit einer im Mindestmaß erhöhten Freiheitsstrafe bedroht sein muss oder – soweit es um die Drohung mit Straftaten gegen eine Sache bzw. die körperliche Unversehrtheit geht – von der Bedingungen abhängig zu machen, dass die Drohung öffentlich, in einer Versammlung oder durch Verbreiten von Schriften begangen wird.

Der Deutsche Landkreistag begrüßt die von den Fraktionen und der Bundesregierung vorgeschlagene Ausweitung des Bedrohungstatbestandes. Wir sehen darin ein wirksames Mittel, um mit den Mitteln des Strafrechts gegen entsprechende Bedrohungen von Kommunalpolitikern, über die uns immer wieder berichtet wird, vorzugehen. Die vom Bundesrat vorgeschlagenen Beschränkungen erachten wir nicht für erforderlich.

Mit freundlichen Grüßen

Im Auftrag

Dr. Ritgen

Resolution

des Präsidiums des Deutschen Landkreistages
vom 9./10.1.2018

Keine Gewalt gegen öffentlich Bedienstete!

- Das Präsidium des Deutschen Landkreistages nimmt mit großer Besorgnis zur Kenntnis, dass sich die Zahl der verbalen und körperlichen Angriffe gegen öffentlich Bedienstete deutlich erhöht hat. Landräte, aber auch die Mitarbeiter in den Sozial- und Jugendämtern, den Ausländerbehörden, den Veterinärämtern und anderer Stellen der Kreisverwaltung werden immer öfter Opfer von Beleidigungen, Drohungen und auch tätlicher Gewalt.
- Das Präsidium des Deutschen Landkreistages lehnt solche Übergriffe auf das Entschiedenste ab. Sie müssen mit allen zur Verfügung stehenden Mitteln des Strafrechts konsequent verfolgt werden, insbesondere aber auch – als Ausdruck einer nicht hinzunehmenden Verrohung – gesellschaftlich klar verurteilt werden.
- Die Anwendung und Androhung körperlicher Gewalt ist unter keinen denkbaren Umständen gerechtfertigt. Dies gilt auch und gerade dann, wenn sich die Bedrohung nicht nur gegen die Amtsträger selbst, sondern auch gegen ihre Familienangehörigen richtet. Der Rechtsstaat und die Gesellschaft müssen sich in solchen Fällen schützend vor die Amtsträger und ihre Familien stellen. Die Landkreise stehen für eine bürgeroffene und frei zugängliche Verwaltung. Trotzdem ist es im Lichte der jüngsten Entwicklung nachvollziehbar, wenn in besonders gefährdeten Bereichen verstärkt auf Einlasskontrollen und ähnliche Schutzmaßnahmen gesetzt wird.
- Die Mitarbeiter der öffentlichen Verwaltungen nehmen für das Gemeinwesen wichtige Aufgaben mit großem persönlichen Engagement wahr. Sie verdienen dafür besondere Achtung, und zwar auch dann, wenn aus Sicht der Betroffenen unliebsame Entscheidungen getroffen werden müssen. Kränkungen, ehrverletzende Äußerungen oder Verleumdungen sind daher nicht hinnehmbar. Sie wiegen besonders schwer, wenn sie in der Öffentlichkeit verbreitet werden.
- Das Internet bietet viele Möglichkeiten, Beleidigungen, Drohungen oder Aufrufe zur Gewalt in anonymer Form zu kommunizieren. Damit das Internet nicht zu einem rechtsfreien Raum verkommt, sind insbesondere die Betreiber entsprechender Plattformen und der sozialen Medien aufgefordert, solche Inhalte ggf. auch zu löschen.
- Der politische Meinungskampf lebt nicht zuletzt von zuspitzenden, abgrenzenden Formulierungen. Auch in der verbalen Auseinandersetzung mit dem politischen Gegner sind aber dessen Persönlichkeitsrechte zu achten. Das Präsidium des Deutschen Landkreistages bekennt sich zur grundgesetzlich geschützten Meinungsfreiheit, die ein hohes Gut ist. Aus der Meinungsfreiheit folgt jedoch kein Freibrief für beleidigende oder verleumderische Äußerungen oder gar für die Drohung mit Gewalt.

Deutscher Bundestag
19. Wahlperiode

Ausschuss für Recht und Verbraucherschutz

Deutscher Bundestag Ausschuss für Recht und Verbraucherschutz Ausschussdrucksache 19(6)134 27. April 2020

24. April 2020

Änderungsantrag 1 (Strafrecht)
der Fraktion BÜNDNIS 90/DIE GRÜNEN im 6. Ausschuss

zu dem Gesetzentwurf der Fraktionen der CDU/CSU und SPD

- Drucksache 19/17741 -

Entwurf eines Gesetzes zur Bekämpfung von Rechtsextremismus und Hass-
kriminalität (Entwurf eines Gesetzes zur Bekämpfung von Rechtsextremismus und
Hasskriminalität – Drucksache 19/18470 – der Bundesregierung)

1. Artikel 1 (Änderung des Strafgesetzbuches) wird wie folgt geändert:

a) Folgende neue Nummer 1. wird eingefügt:

„1. In der Inhaltsübersicht wird die Angabe zu § 188 durch folgende Angabe ersetzt:

„§ 188 Schwere Beleidigung, schwere üble Nachrede, schwere Verleumdung““

b) Die bisherigen Nummern 1. und 2. werden zu den neuen Nummern 2. und 3.

c) Die bisherige Nummer 3. (zu § 126 StGB) wird zur neuen Nummer 4. und wie folgt gefasst:

„4. § 126 Absatz 1 wird wie folgt geändert:

a) In Nummer 6 wird das Wort ‚oder‘ am Ende durch ein Komma ersetzt.

b) Der Nummer 7 wird nach der Angabe ‚§ 318 Absatz 1‘ das Wort ‚oder‘ angefügt.

c) Nach Nummer 7 wird folgende Nummer 8 eingefügt: ‚8. einen sexuellen Übergriff, eine sexuelle Nötigung oder eine Vergewaltigung (§ 177 Absatz 4 bis 8)““

d) Die bisherige Nummer 4. (zu § 140 StGB) wird gestrichen.

e) Die Nummern 5. bis 8. (§§ 185 bis 194 StGB) werden durch folgende Nummern 5. bis 9. ersetzt:

”

5. In § 185 werden die Wörter ‚und, wenn die Beleidigung mittels einer Tötlichkeit begangen wird, mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe‘ gestrichen.
6. In § 186 werden die Wörter ‚und, wenn die Tat öffentlich oder durch Verbreiten von Schriften (§ 11 Abs. 3) begangen ist, mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe‘ gestrichen.
7. In § 187 werden die Wörter ‚und, wenn die Tat öffentlich, in einer Versammlung oder durch Verbreiten von Schriften (§ 11 Abs. 3) begangen ist, mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe‘ gestrichen.
8. § 188 wird wie folgt gefasst:

,§ 188 Schwere Beleidigung, schwere üble Nachrede, schwere Verleumdung

- (1) In den Fällen der Beleidigung (§ 185) ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe, wenn die Tat
 1. öffentlich, in einer Versammlung oder durch Verbreiten von Schriften (§ 11 Abs. 3) begangen ist,
 2. einen rassistischen, fremdenfeindlichen, antisemitischen oder sonstigen menschenverachtenden Inhalt hat oder von derartigen Beweggründen getragen ist,
 3. sich gegen eine im politischen, auch kommunalpolitischen, Leben des Volkes stehende Person richtet und in Beziehung zu deren politischer Betätigung steht,
 4. Bestandteil einer über längere Zeit fortgesetzten erheblichen und systematischen Belästigung der beleidigten Person ist oder
 5. mittels einer Tötlichkeit begangen ist.
- (2) In den Fällen der üblen Nachrede (§ 186) ist die Strafe Freiheitsstrafe bis zu drei Jahren oder Geldstrafe, wenn die Tat unter den Voraussetzungen des Absatzes 1 Nummern 1, 2, 3 oder 4 begangen ist.
- (3) In den Fällen der Verleumdung (§ 187) ist die Strafe Freiheitsstrafe von drei Monaten bis zu fünf Jahren, wenn die Tat unter den Voraussetzungen des Absatzes 1 Nummern 1, 2, 3 oder 4 begangen ist.
- (4) Eine im politischen Leben des Volkes stehende Person im Sinne von Absatz 1 Nummer 3 ist eine Person, die auf europäischer Ebene, Bundes- oder Landesebene oder auf Ebene einer für ein Teilgebiet eines Landes oder einer kommunalen Gebietskörperschaft gebildeten Verwaltungseinheit aktiv tätig ist.‘

9. § 194 Absatz 1 wird wie folgt geändert:

- a) Nach Satz 1 wird folgender Satz eingefügt:

,Dies gilt nicht in den Fällen des § 188 Absatz 1 Nummern 2 und 3, auch in Verbindung mit Absatz 2 und 3, wenn die Strafverfolgungsbehörde wegen des besonderen öf-

fentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.’

- b) Die bisherigen Sätze 2 bis 4 werden die Sätze 3 bis 5.
- c) In dem neuen Satz 4 werden nach dem Wort ‚kann‘ die Wörter ‚in den vorgenannten Fällen‘ eingefügt.“
- f) Die bisherige Nummer 9. (zu § 241) wird zur neuen Nummer 10. und wird zu Änderungsbefehl Buchstabe a) wie folgt gefasst:

„a) Dem Absatz 1 wird folgender Absatz 1 vorangestellt:

„(1) Wer einen Menschen mit der Begehung einer gegen ihn oder eine ihm nahestehende Person gerichteten rechtswidrigen Tat gegen die sexuelle Selbstbestimmung oder die körperliche Unversehrtheit, wenn die Tat mit einer im Mindestmaß erhöhten Freiheitsstrafe bedroht ist, oder gegen die persönliche Freiheit bedroht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.““

2. In Artikel 2 (Änderung der Strafprozessordnung) wird die Nummer 6. wie folgt gefasst:

„§ 374 Absatz 1 wird wie folgt geändert:

- a) In Nummer 2 werden nach den Wörtern ‚gerichtet ist‘ die Wörter ‚und nicht einen Fall des § 188 Absatz 1 Nummer 2 oder 3, auch in Verbindung mit Absatz 2 oder 3, des Strafgesetzbuches betrifft‘ angefügt.
- b) In Nummer 5 wird die Angabe ‚§ 241‘ durch die Wörter ‚§ 241 Absatz 1 bis 3‘ ersetzt.“

Begründung

Die dem Gesetzentwurf der Bundesregierung zugrunde liegende Zielsetzung, den zunehmenden Rechtsextremismus, die anhaltenden Angriffe auf Demokratinnen und Demokraten und die zu beobachtende Verrohung der Diskussionskultur im Netz zu bekämpfen, wird ausdrücklich begrüßt. Im Übrigen wird zu dem Gesetzentwurf der Bundesregierung insgesamt und zu der nötigen Gesamtstrategie zur Bekämpfung von Rechtsextremismus, der Bedrohung ganzer Bevölkerungsgruppen sowie von Hass und Hetze im Netz auf den Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Drucksache 19/17750 verwiesen (Hass und Hetze wirksam bekämpfen, Betroffene stärken und Bürgerrechte schützen – siehe Anhang).

Allerdings schießt der Gesetzentwurf der Bundesregierung mehrfach über das Ziel hinaus – und damit auch am Ziel vorbei. Im Zusammenhang dieses auf das Strafrecht beschränkten ersten Änderungsantrages geht es dabei um die fehlende konsequente Beachtung des Grundsatzes, dass das Strafrecht nur dann einzusetzen ist, „wenn ein bestimmtes Verhalten über sein Verboten sein hinaus in besonderer Weise sozial-schädlich und für das geordnete Zusammenleben der Menschen unerträglich, seine Verhinderung daher besonders dringlich ist“ (BVerfGE 120, 224 (240, Rz 35)). Das Strafrecht darf eben nicht zur Erreichung

jedes grundsätzlich unterstützenswerten Zwecks eingesetzt werden, sondern nur unter der vorgenannten Voraussetzung. Mängel bei Rechtssicherheit und Praxistauglichkeit des Gesetzentwurfs der Bundesregierung kommen hinzu. Im Einzelnen:

Zu Nummer 1. (Artikel 1 Änderung des Strafgesetzbuches)

Nummer 1 a)

Anpassung der Inhaltsübersicht an den neugefassten und neu bezeichneten § 188 StGB (Schwere Beleidigung, schwere üble Nachrede, schwere Verleumdung).

Nummer 1 b)

Folgeänderung.

Nummer 1 c) (Änderung § 126 StGB- Störung des öffentlichen Friedens durch Androhung von Straftaten)

Die Aufnahme der gefährlichen neben der schweren Körperverletzung in den Straftatenkatalog des § 126 Absatz 1 StGB entfällt (so auch DAV-Stellungnahme 6/2020 zu 2.b mit dortiger Begründung):

Die Erweiterung des Straftatenkatalogs auf Fälle der gefährlichen Körperverletzung (§ 224 StGB) führt zu einer nicht gerechtfertigten Ausdehnung der Strafbarkeit auf Fälle, in denen eine Eignung zur Störung des öffentlichen Friedens von vornherein fraglich erscheint. Geschütztes Rechtsgut des § 126 StGB ist der "öffentliche Friede" im Sinne eines objektiven Zustands allgemeiner Rechtssicherheit und des subjektiven Bewusstseins der Bevölkerung, in Ruhe und Frieden zu leben (vgl. Fischer, StGB, 67. Auflage 2020, § 126 Rn. 2). Obwohl der Katalog des § 126 Absatz 1 Nummer 1 bis 7 StGB zahlreiche Delikte enthält, die auf den Schutz von Individualrechtsgütern gerichtet sind, steht dieser Schutz nicht im Vordergrund. Maßgebend ist insoweit vielmehr, dass die Androhung oder das Vortäuschen der dort aufgeführten Taten zu einer besonderen Beunruhigung in der Bevölkerung führen kann (vgl. Schäfer in: Münchner Kommentar zum StGB, 2. Auflage, § 126 Rn. 2). Sämtliche bisher in § 126 Absatz 1 Nummer 1 bis Nummer 7 StGB aufgeführte Taten zeichnen sich dadurch aus, dass es sich bei diesen um Straftaten handelt, die vom Gesetzgeber als besonders "schwerwiegend" eingestuft worden sind (vgl. BT-Drucksache 7/4549, S. 8). Bereits im damaligen Gesetzgebungsverfahren wurde bewusst darauf verzichtet, die Befürwortung von Gewalttätigkeiten gegen Menschen und Sachen insgesamt zu pönalisieren.

Die Erweiterung des § 126 Absatz 1 StGB auch auf Fälle des § 224 StGB widerspricht diesen Erwägungen und der bisher bestehenden Gesetzessystematik und bezieht Fälle ein, bei denen weder die besondere Schwere der Tatfolgen, noch die über den Lebenskreis des Verletzten hinausgehende Wirkung der Tatbegehung derart schwerwiegend erscheint, dass dies insoweit eine Strafbarkeit rechtfertigt. Die vom Bundesverfassungsgericht geforderte besondere Dringlichkeit für den Einsatz des Strafrechts besteht auch unter Berücksichtigung des gesetzgeberischen Entscheidungsspielraums – insbesondere im Hinblick auf die bisher geringe praktische Relevanz (vgl. NK-StGB/ Ostendorf, 5. Auflage, § 126 Rn. 7) der Vorschrift insgesamt – nicht.

In den Straftatenkatalog aufgenommen werden dagegen entsprechend der Stellungnahme des Bundesrates (Drs 87/20(Beschluss) Ziffer 4.) die Delikte zu sexuellen Übergriffen, sexueller Nötigung sowie Vergewaltigung (§ 177 Absatz 4 bis 8 StGB). Um einen ausreichenden strafrechtlichen Schutz für Frauen zu erreichen, müssen auch Ankündigungen zu solchen Straftaten ausdrücklich erfasst werden. Bei Straftaten nach § 177 Absatz 4 bis 8 StGB handelt es sich um Verbrechen, also Delikte, die mit einer Freiheitsstrafe von mindestens einem Jahr bestraft werden. Da Opfer von sexuellen Übergriffen, sexueller Nötigung und Vergewaltigung nahezu ausschließlich Frauen sind, ist die Aufnahme der Norm im Katalog des § 126 StGB ein weiterer Schritt zum wirksamen Schutz vor Gewalt gegen Frauen.

Nummer 1 d) (§ 140 StGB – Belohnung und Billigung von Straftaten)

Die vorgesehene Tatbestanderweiterung um die Billigung noch nicht erfolgter Straftaten entfällt. Damit soll erreicht werden, dass die geltende Rechtslage fortbesteht.

Anders als in der Gesetzesbegründung auf Drs.19/17741 S. 32 behauptet, bestehen hier keine tatsächlichen Strafbarkeitslücken. Der DAV führt in seiner Stellungnahme (aaO sub.2. c)bb)) zutreffend aus, dass der sozialschädliche Kern der Befürwortung von und der Anleitung zu Gewalttaten von anderen bestehenden Straftatbeständen hinreichend erfasst wird. Soweit der Täter öffentlich dazu auffordert eine bestimmte – wenngleich nicht in allen Einzelheiten feststehende – rechtswidrige Tat zu begehen, greift die Vorschrift der öffentlichen Aufforderung zu Straftaten gemäß § 111 StGB einhergehend mit einer im Verhältnis zu § 140 StGB erhöhten Strafandrohung. Im Übrigen siehe § 126 StGB – Störung des öffentlichen Friedens durch Androhung von Straftaten; § 130 StGB – Volksverhetzung; § 131 StGB – Verherrlichung von Gewalt; § 140 StGB – Billigung von Straftaten; § 21 in Verbindung mit § 6 des Gesetzes über die Verbreitung jugendgefährdender Schriften, § 53 Abs. 1 Nr. 5 des Waffengesetzes.

Der Entwurf der Bundesregierung sieht vor, die Tathandlung der Billigung vom Erfordernis der begangenen beziehungsweise versuchten Straftat zu lösen, so dass bereits das Billigen einer möglichen künftigen Straftat, bei der Täter und Tatumstände nicht bestimmbar sind und gar nicht feststeht, ob sie jemals begangen wird, strafbewehrt wäre. In der Konsequenz würde diese Erweiterung zu einer weitreichenden Vorverlagerung strafbaren Handelns führen.

Damit entfernt sich der Entwurf vom Grundgedanken der Vorschrift des § 140 StGB, wonach der öffentliche Friede als überindividuelles Rechtsgut zu schützen ist und die Entstehung eines „psychischen Klimas“, in dem „gleichartige Untaten gedeihen können“, verhindert werden soll (vgl. BGHSt 22, 282). Stattdessen soll nun schon „aggressives Maulheldentum“ strafbewehrt sein, wobei sich die Äußerungen nicht mehr auf hinreichend konkrete Handlungen beziehen müssen. Auch wenn einzelne Äußerungen der gesellschaftlichen Moral zuwiderlaufen und auf eine bedenkliche Gesinnung des Äußernden schließen lassen, würde die strafrechtliche Verfolgung zu einer nicht mehr hinnehmbaren Vorfeldkriminalisierung führen. Denn die Billigung noch nicht begangener, nur ihrer Art nach beschriebener Straftaten liegt so weit im Vorfeld der Verletzung eines individuellen Rechtsguts, dass ihr Unwertgehalt auf ein die Strafwürdigkeit unterschreitendes Niveau herabgesetzt ist.

Dass das von § 140 StGB in dem Gesetzentwurf umschriebene Verhalten derart schwer wiegt, dass ohne seine Verhinderung mit den Mitteln des Strafrechts ein sozialetisches Minimum, dessen Einhaltung für ein geordnetes Zusammenleben der Gesellschaft erforderlich ist, nicht eingehalten werden kann, ist jedoch nicht ersichtlich.

Auch ein Blick auf die Historie des und ein Vergleich mit dem alten § 88a StGB belegen, dass die vorgeschlagene Änderung des § 140 StGB nicht zu begründen ist:

§ 88a StGB alte Fassung war durch das am 1. Mai 1976 in Kraft getretene 14. Strafrechtsänderungsgesetz vom 22. April 1976 (BGBl. I, S. 1056) in das StGB eingefügt worden und bis zum 13. August 1981 geltendes Recht. Darin wurde die Verbreitung einer Schrift unter Strafe gestellt, die bestimmte schwere Taten befürwortet und die dazu bestimmt und geeignet ist, die Bereitschaft anderer zu fördern, sich durch die Begehung solcher Taten für Bestrebungen gegen den Bestand oder die Sicherheit der Bundesrepublik Deutschland oder gegen Verfassungsgrundsätze einzusetzen. Diese Norm ist materiell fast vollständig inhaltsgleich mit § 140 StGB in der geplanten Fassung.

§ 88a StGB alte Fassung wurde 1981 aus mehreren Gründen wieder abgeschafft. Zum einen war die Norm nicht praxistauglich, was sich in der Bilanz von einer einzigen Verurteilung innerhalb von über fünf Jahren Geltungsdauer zeigte. Vor ihrer Abschaffung wurde der Norm bescheinigt, dass für sie kein Bedürfnis bestehe, sie aber gleichzeitig die Meinungsfreiheit einschränke (vgl. Dreher/Tröndle, StGB, 40. Aufl. 1981, § 130a Rn. 1; Ausarbeitung der Wissenschaftlichen Dienste des Deutschen Bundestages „Öffentliches Billigen oder Gutheißen von Straftaten“ v. 8. Juni 2018 [WD 7 – 3000 – 128/18], S. 14). Der Rechtsausschuss bezeichnete die Norm in seiner Beschlussempfehlung zu deren Abschaffung als „überflüssig und schäd-

lich“ (vgl. BT-Drucksache 9/135, Seite 3). Er verwies zudem darauf, dass die Vorschrift „für das Ansehen des Strafrechts und das Ansehen des Staates mehr Schaden angerichtet als Nutzen gebracht“ hätte, was er insbesondere damit erklärt, dass sich im Rahmen der zahlreichen Ermittlungsverfahren Personen mit den Beschuldigten gegen den Staat solidarisiert haben, die zuvor keine Sympathie für die „Verfasser von Gewaltliteratur“ gehabt hätten (vgl. BT-Drucksache 9/135, Seite 3). Damit stünden „die negativen Wirkungen [...] der Vorschriften, insbesondere auf das geistige Klima, und die Gefahren für die Meinungsfreiheit in keinem angemessenen Verhältnis zum kriminalpolitischen Nutzen“ (vgl. BT-Drucksache 9/135, Seite 3).

Zwar steht außer Frage, dass die insbesondere in den sozialen Medien sinkende Hemmschwelle bei der Verbreitung verachtenswerter Äußerungen geeignet ist, das gesellschaftliche Klima zu vergiften. Dennoch lässt sich der Verrohung des gesellschaftlichen Klimas mit den Mitteln des Strafrechts, die ultima ratio sein sollen, nicht allumfassend begegnen.

Nummer 1 e) (§§ 185-194 StGB Beleidigungstatbestände)

Die Beleidigungstatbestände werden neu geordnet in Anlehnung an den Diskussionsentwurf des Bayerischen Staatsministeriums der Justiz für ein „Gesetz zur nachdrücklichen strafrechtlichen Bekämpfung der Hassrede und anderer besonders verwerflicher Formen der Beleidigung“ (Stand 04.11.2019 - <https://www.justiz.bayern.de/ministerium/gesetzgebung/>). Auf die dortige Begründung wird verwiesen. Diese Neuordnung hatte sowohl bereits die antragstellende Fraktion gefordert (Drs.19/17750 v. 10.03.2020 – Hass und Hetze wirksam bekämpfen, Betroffene stärken und Bürgerrechte schützen, sub II.7.a) als auch nunmehr der Bundesrat empfohlen (BR-Drs.87/20 (Beschluss) Ziffer 5.). Präzisierend ist zur rechtssicheren Einbeziehung auch der Kommunalpolitiker und Kommunalpolitikerinnen in § 188 StGB-E (Schwere Beleidigung, üble Nachrede, schwere Verleumdung) eine dem Bestimmtheitsgebot genügende Erfassung der auf Europäischer Ebene, Bundes-, Landes- oder Kommunalebene oder auf Ebene einer für ein Teilgebiet eines Landes oder einer kommunalen Gebietskörperschaft gebildeten Verwaltungseinheit aktiv tätigen Politiker und Politikerinnen erfolgt, wie das auch der Bundesrat vorgeschlagen hat (BR-Drs.87/20 (Beschluss) Ziffer 6 – auf die dortige Begründung wird verwiesen).

Nummer 1 f) (Änderung § 241 StGB Bedrohung)

Die Ausdehnung des Bedrohungstatbestandes über die Bedrohung mit Verbrechen hinaus auf die Bedrohung mit Vergehen ist abzulehnen. Die im Gesetzentwurf der Bundesregierung vorgeschlagene pauschale Erweiterung des Tatbestandes würde zu erheblicher Rechtsunsicherheit führen. Die uferlose Ausweitung des Bedrohungstatbestands führt zudem zu einem Aufweichen der Deliktsskizzen, insbesondere in Abgrenzung zur Nötigung, wenn mehr oder weniger jede Drohung mit einem empfindlichen Übel auch als Bedrohung unter Strafe gestellt wird.

Artikel 1 Nummer 9 Buchstabe a (§ 241 Absatz 1 StGB-E) wird daher über den Vorschlag des Bundesrates (Drs 87/20(Beschluss) Ziffer 7) hinaus begrenzt auf schwerere Straftaten.

Durch die äußerst weitgehende Fassung des Tatbestandes im Gesetzentwurf der Bundesregierung besteht die Gefahr einer nicht gewünschten Ausuferung der Strafbarkeit von Alltagsäußerungen und Alltagskonflikten (z.B. im Straßenverkehr, in der Kneipe, unter Jugendlichen). Künftig würden auch umgangssprachliche und eher niedrigschwellige Drohungen wie „Ich zieh dir die Ohren lang“ oder „Gleich knall ich dir eine“ vom Tatbestand erfasst (so auch der DAV in seiner Stellungnahme, aaO sub 2.d). Derartige Äußerungen werden sich durch drohende strafrechtliche Ahndung nicht verhindern lassen, indes zu einer noch weitergehenden Überlastung der Strafverfolgungsbehörden und -justiz führen. Sie werden unfreiwillig außerdem zum unzutreffenden Narrativ vermeintlich kaum beherrschbarer Kriminalitätszunahme gerade auch im Jugendbereich beitragen, die in Wahrheit nur das Resultat der Ausweitung normativer Strafbarkeit durch den Gesetzgeber wäre (DAV aaO). Soweit der Gesetzentwurf der Bundesregierung auch eine Strafbarkeit von Drohungen mit rechtswidrigen Taten gegen Sachen von bedeutendem Wert vorsieht, ist folgendes zu beachten: In der Praxis wird es sich am häufigsten um Drohungen mit der Zerstörung von Kraftfahr-

zeugen und Immobilien durch Brandstiftung handeln („Ich fackele dir die Hütte ab“ oder „Ich jage Dein Auto hoch“). Diese Drohungen sind jedoch bereits jetzt vom Tatbestand erfasst, da die Brandstiftung nach § 306 StGB in entsprechenden Fällen ein Verbrechen darstellt. Deshalb ist das von der Bundesregierung vorgeschlagene Tatbestandsmerkmal der Bedrohung mit rechtswidrigen Taten gegen Sachen von bedeutendem Wert zu streichen.

Geschütztes Rechtsgut des § 241 StGB ist der individuelle Rechtsfrieden, indem die Norm das Vertrauen des Einzelnen auf seine durch das Recht gewährleistete Sicherheit vor besonders gravierenden Bedrohungen schützen soll (Sinn, MüKoStGB, 3. Aufl. 2017, § 241 Rn. 2). Die Bedrohung muss jedoch nur objektiv geeignet sein, den Effekt einer derartigen Beunruhigung bei einem „normal“ empfindenden (weder besonders ängstlichen noch besonders unerschrockenen oder leichtsinnigen) Menschen auszulösen (vgl. BVerfG, Beschl. v. 19.12.1994 – 2 BvR 1146/94 = NJW 1995, 2776, 2777; Sinn, MüKoStGB, § 241 Rn. 2; Eisele, Schönke/Schröder, § 241 Rn. 2). § 241 StGB ist daher ein abstraktes Gefährdungsdelikt (statt Vieler Eisele, Schönke/Schröder, § 241 Rn. 2).

Im Vergleich zur Rechtsgutsbeeinträchtigung durch die angedrohte Tat liegt die Strafbarkeit bei der Bedrohung weit im Vorfeld, noch vor dem Versuchsstadium der angedrohten Tat. Der Gesetzgeber hat diese Hürde überwunden, indem er das Rechtsgut des individuellen Rechtsfriedens geschaffen hat. Denn die Bedrohung einer Person mit besonders gravierendem Unrecht ist „in besonderer Weise sozialschädlich und für das geordnete Zusammenleben der Menschen unerträglich“ (vgl. BVerfG aaO), sodass die Bewahrung der Bürgerinnen und Bürger vor den damit einhergehenden psychologischen Beeinträchtigungen besonders dringlich und die Bedrohung in diesen Fällen folglich strafwürdig ist.

Die bisherige konsequente und sinnvolle Anknüpfung an Verbrechen, also Straftaten, die im Mindestmaß mit Freiheitsstrafe von einem Jahr oder darüber bedroht sind (§ 12 Absatz 1 StGB) wird deshalb lediglich in geringem Umfang erweitert.

§ 241 StGB ist als abstraktes Gefährdungsdelikt ausgestaltet. Das Rechtsgut des individuellen Rechtsfriedens muss daher nicht tatsächlich verletzt werden; § 241 StGB umschreibt lediglich ein typisiertes Verhalten, das den individuellen Rechtsfrieden in der Regel verletzt. Die Strafbarkeit liegt – wie bereits ausgeführt – im Vergleich zur Rechtsgutsbeeinträchtigung durch die angedrohte Tat bei der Bedrohung weit im Vorfeld, und zwar noch vor dem Versuchsstadium der angedrohten Tat. Schon wegen dieser Entfernung zu einer tatsächlichen Rechtsgutsverletzung kommt nur eine sehr behutsame Ausweitung des Tatbestands von § 241 StGB um bestimmte Vergehen in Betracht. Nur die Bedrohung mit besonders gravierenden Taten vermag den individuellen Rechtsfrieden in einer Erheblichkeit zu stören, die mit dem Schutz durch das Strafrecht gerechtfertigt werden kann.

Zu Nummer 2. (Artikel 2 – Änderung der Strafprozessordnung)

Änderungsbefehl zu Buchstabe a:

Die Änderung greift auch hier den Diskussionsentwurf des Bayerischen Staatsministeriums der Justiz für ein „Gesetz zur nachdrücklichen strafrechtlichen Bekämpfung der Hassrede und anderer besonders verworflicher Formen der Beleidigung“ (Stand 04.11.2019 - <https://www.justiz.bayern.de/ministerium/gesetzgebung/>) auf. Zur Begründung siehe dort S. 30.

Änderungsbefehl zu Buchstabe b:

Folgeänderung aus der Änderung von § 241 StGB (unverändert).

Anhang siehe Drs 19/17750

Antrag

der Abgeordneten Renate Künast, Dr. Irene Mihalic, Dr. Konstantin von Notz, Tabea Rößner, Luise Amtsberg, Canan Bayram, Katja Dörner, Erhard Grundl, Britta Haßelmann, Katja Keul, Monika Lazar, Steffi Lemke, Cem Özdemir, Filiz Polat, Claudia Roth (Augsburg), Dr. Manuela Rottmann, Ulle Schauws, Charlotte Schneidewind-Hartnagel, Kordula Schulz-Asche, Margit Stumpp, Beate Walter-Rosenheimer und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Hass und Hetze wirksam bekämpfen, Betroffene stärken und Bürgerrechte schützen

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Zur wirksamen Bekämpfung von Rechtsextremismus, der Bedrohung ganzer Bevölkerungsgruppen sowie von Hass und Hetze im Netz bedarf es einer koordinierten Gesamtstrategie, die das Problemfeld auf seinen sämtlichen Ebenen bearbeitet: als rechtsextreme Strategie zur Aushöhlung der Demokratie, als gesamtgesellschaftliches Phänomen einer Verrohung der Debattenkultur und als Fortsetzung wie Befeuerung analoger Formen von Diskriminierung und Gewalt.

Rassistischer, antisemitischer, antiziganistischer, muslimfeindlicher, völkischer, antifeministischer, homo- und transfeindlicher Propaganda und Agitation muss mit aller Entschlossenheit begegnet werden. Menschenverachtenden Ideologien der Ungleichwertigkeit muss entschieden widersprochen und der Strategie einer Normalisierung des vormals Unsagbaren entschlossen begegnet werden.

Die dem Gesetzentwurf der Bundesregierung zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (BR-Drs. 87/20) zugrunde liegende Zielsetzung, den zunehmenden Rechtsextremismus, die anhaltenden Angriffe auf Demokratinnen und Demokraten und die zu beobachtende Verrohung der Diskussionskultur im Netz zu bekämpfen, wird daher ausdrücklich begrüßt. Er greift aber einerseits zu kurz und weitet andererseits Befugnisse in weder zielführender noch verhältnismäßiger Weise aus. Damit die Maßnahmen aber effizient wirken, müssen sie zielgenau ausgerichtet sein, um Behörden und Justiz nicht mit unnötigen Aufgaben zu überlasten.

So steht nach derzeitigem Stand des Regierungsentwurfs unter anderem zu befürchten, dass das Bundeskriminalamt (BKA) mit der zusätzlichen Aufgabe als zentrale Meldestelle, mit der Aufgabe der Aufarbeitung der Meldungen und ihrer Weiterleitung an die zuständigen Stellen der Länder angesichts der nicht überschaubaren Meldemenge überfordert sein könnte. Dann würde die dringend notwendige Effektivierung der

Strafverfolgung nicht erreicht, sondern sogar konterkariert und die Rechtsunsicherheit erhöht.

Rechtsextremisten wollen Demokratie, Gewaltenteilung, freie Meinungsäußerung, Gleichheit vor dem Gesetz und Rechtsstaatlichkeit generell beseitigen. Umso mehr müssen Maßnahmen gegen Rechtsextremismus und Hasskriminalität fest auf dem Boden der Rechtsstaatlichkeit verankert sein und die Bürgerrechte und grundrechtlich geschützten Beteiligungsrechte der davon potentiell Betroffenen müssen jederzeit gewährleistet bleiben.

Hass und Hetze im Netz sind nicht vorrangig ein strafrechtliches Problem. Gerade rechtsextreme Gruppen wissen genau, wie sie an der Grenze zur Strafbarkeit legale, wenn auch hasserfüllte Kommentare formulieren können. Genauso dringlich braucht es daher einen gesamtgesellschaftlichen Ansatz, Verbesserungen für Prävention, Forschung, Beratung und Opferschutz.

Nach wie vor fehlt es an einer kohärenten medien- und netzpolitischen Gesamtstrategie auf den unterschiedlichen politischen Ebenen. Mit dem auf Länderebene von der Ministerpräsidentenkonferenz verabschiedeten Medienstaatsvertrag werden zwar erstmals Intermediäre in die Regulierung aufgenommen, jedoch werden die für die Aufsicht zuständigen Landesmedienanstalten für die zusätzliche Aufgabe nicht mit zusätzlichen Mitteln ausgestattet. Auf Länder- wie auf Bundesebene fehlt es an Regelungen zur wirksamen Verhinderung von Medienkonzentrationsentwicklungen. Darüber hinaus gibt es kein Konzept für eine altersübergreifende Medienkompetenzförderung, wobei das für die Bekämpfung der Wirksamkeit von Hass, Hetze und Falschinformationen so dringend notwendig ist.

Zu der notwendigen Gesamtstrategie gehört auch, das historisch als Gegenbegriff zur NS-Rasseideologie gemeinte, aber – weil es beim Menschen keine Rassen gibt – in der Sache falsche Wort „Rasse“ bei den Diskriminierungsverboten in Artikel 3 Absatz 3 GG zu ersetzen durch den Begriff „rassistisch“ und das Grundgesetz zu ergänzen durch die ausdrückliche Pflicht des Staates, Schutz gegen alle Formen gruppenbezogener Menschenfeindlichkeit zu gewährleisten.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. die Zivilgesellschaft und Prävention gegen Rechtsextremismus nachhaltig zu stärken und zu fördern und dazu insbesondere die folgenden Maßnahmen umzusetzen:

- a) Die Förderung zivilgesellschaftlicher Arbeit zur Demokratiestärkung, gegen Rechtsextremismus, Rassismus und andere Formen gruppenbezogener Menschenfeindlichkeit muss als Daueraufgabe über ein Demokratiefördergesetz nachhaltig gestaltet und finanziell strukturell abgesichert werden, wobei die Unabhängigkeit zivilgesellschaftlichen Engagements nicht ausgehöhlt werden darf. Die Bundesregierung soll dafür einen Entwurf für eine bundesgesetzliche Grundlage zur Demokratieförderung vorlegen (s. Antrag „Rechtsextremismus umfassend bekämpfen“ auf Drs. 19/1851).
- b) Das Gemeinnützigkeitsrecht muss dringend reformiert werden. Dazu muss die Bundesregierung Rechtssicherheit bei den förderfähigen Zwecken in § 52 der Abgabenordnung bei gemeinnützigem bürgerschaftlichem Engagement gegen Rassismus, für Grund- und Menschenrechte und unsere Demokratie über einen entsprechenden Gesetzentwurf schaffen (s. Antrag „Gemeinnützigkeit braucht Rechtssicherheit statt politischer Willkür“ auf Drs. 19/7434).
- c) Es soll ein unabhängiges Institut zum Schutz der Verfassung (s. Antrag „Rechtsextremen Netzwerken entschlossen entgegentreten“ auf Drs. 19/14091 und Antrag „Neustart des Verfassungsschutzes des Bundes“ auf

Drs. 19/8700) errichtet werden. Mithilfe des Instituts sollen insbesondere Radikalisierungsprozesse erforscht und die Expertise aus Wissenschaft und Zivilgesellschaft strukturiert einbezogen werden.

- d) Die Bundesregierung muss die zur Bekämpfung von Hasskriminalität und Rechtsextremismus als Grundlage evidenzbasierter Kriminalpolitik und zur Erforschung dieser Phänomene erforderlichen statistischen Daten systematisch erheben (s. Entwurf Kriminalitätsstatistikgesetz auf Drs. 19/2000) und gemeinsam mit den Ländern die Aussagekraft der Strafrechtspflege-Statistiken nachhaltig stärken.
2. Betroffene von Hasskriminalität, Rassismus und Rechtsextremismus durch Verbesserungen des Opferschutzes, den Ausbau von Beratungsangeboten und Erleichterungen bei ihrem Vorgehen gegen Hasskriminalität, Rassismus und Rechtsextremismus zu stärken, insbesondere durch folgende Maßnahmen:
 - a) Der Schutz vor rassistischer Diskriminierung sowie vor Diskriminierung wegen des Geschlechts, der Religion oder Weltanschauung, einer Behinderung, des Alters oder der sexuellen Identität im Allgemeinen Gleichbehandlungsgesetz (AGG) muss deutlich verbessert werden. Dazu soll die Bundesregierung einen Gesetzentwurf vorlegen, der den Anwendungsbereich erweitert, Ausnahmeregelungen eingrenzt, die viel zu kurzen Klagefristen verlängert und ein echtes Verbandsklagerecht einführt, damit gegen Diskriminierungen strukturell und nachhaltig vorgegangen werden kann.
 - b) Die Ausstattung der Antidiskriminierungsstelle des Bundes (ADS) muss deutlich aufgestockt werden. Zudem ist seit nunmehr zweieinhalb Jahren die Leitung der ADS nur kommissarisch besetzt. Diesen unverantwortlichen Zustand muss die Bundesregierung unverzüglich beenden, damit die ADS ihre Aufgaben wieder in vollem Umfang und unabhängig wahrnehmen kann. Die Stärkung der ADS ist auch deshalb dringend notwendig, um zu einer Stabsstelle zur Bekämpfung von jeder Form von Rassismus zu kommen. Darüber hinaus muss die Bundesregierung eine unabhängige Expertinnen- und Expertenkommission zum Thema Rassismus einsetzen.
 - c) Das Waffenrecht muss noch wirksamer ausgestaltet werden, damit sich gewaltbereite Personen und Bewegungen, die sich gegen die verfassungsmäßige Ordnung wenden, nicht auch noch legal bewaffnen können (siehe die Anträge auf Drs. 19/17520 und 19/14092).
 - d) Es muss eine „Task Force Rechtsextremismus“ im Geschäftsbereich des Bundesinnenministeriums eingerichtet werden, die eine koordinierende Funktion einnimmt und die Prüfung zentralisierter Informationsmöglichkeiten und vor allem eines erleichterten Zugangs zu Beratungs- und Hilfsangeboten garantiert. Dazu soll sie unter anderem folgende Eckpunkte (s. auch Antrag „Netzwerkdurchsetzungsgesetz weiterentwickeln – Nutzerrechte stärken, Meinungsfreiheit in sozialen Netzwerken sicherstellen“ Drs. 19/5950) umsetzen:
 - Die Förderung und den Ausbau flächendeckender, unabhängiger und kostenfreier Informations- und Beratungsstellen zum Umgang mit Phänomenen wie „Hate Speech“ und „Desinformation“. Dabei ist eine (Teil-)Finanzierung durch eine verpflichtende Abgabe von Diensteanbietern von Telemedien ab einer festzulegenden Größenordnung zu prüfen.
 - Die Prüfung, wie existente Beratungsstellen, etwa gegen Rechtsextremismus, Frauenberatungsstellen, Migrantenorganisationen oder Einrichtungen von Lesben, Schwulen, Bisexuellen, trans- und intergeschlechtlichen Menschen bei der Qualifizierung zu Phänomenen wie „Hate Speech“ und „Desinformation“ unterstützt werden können.

-
- Die Sicherstellung, dass alle Informations- und Beratungsstellen niedrigschwellig auch Kindern und Jugendlichen zur Verfügung stehen, diese explizit ansprechen und Beraterinnen und Berater in Jugendschutzfragen geschult sind.
 - Die Einrichtung einer zentralen Anlaufstelle für Menschen, die von rechter Gewalt bedroht sind, u. a. indem sie auf „Feindeslisten“ geführt werden.
 - Gemeinsam mit den Ländern eine Bundeszentrale für digitale und Medienbildung auf den Weg zu bringen. Mit ihr sollen unter anderem altersgerechte schulische und außerschulische Bildungsangebote für alle Menschen in Deutschland geschaffen bzw. zur Verfügung gestellt werden, die Fähigkeiten fördern, (im Internet) verbreitete Inhalte kritisch zu hinterfragen, bewusst verfälschte Inhalte als solche zu erkennen und für persönlichkeitsverletzende Inhalte sensibilisieren (Medienkompetenz). Vorhandene Initiativen und Angebote sollen ausgebaut, gebündelt und besser vernetzt werden.
 - Politische Bildung sowohl als Unterrichtsfach als auch als Querschnittsaufgabe gemeinsam mit den Ländern auszubauen und zu fördern. Dazu gehört auch die feste fächerübergreifende Verankerung in allen Schulformen, eine deutlich stärkere Priorisierung in den Bildungsplänen sowie ein verbessertes Angebot zur Demokratie- und Werteerziehung in allen Phasen der Lehreraus- und -fortbildung.
 - Die Bundeszentrale für politische Bildung finanziell und organisatorisch zu stärken und eine engere Zusammenarbeit und Vernetzung mit den Landeszentralen für politische Bildung zu befördern.
 - Das vielfältige zivilgesellschaftliche Engagement und die Gegenrede zu unterstützen.
- e) Mit Hass, Hetze und Bedrohung konfrontierte Personen muss leichter ermöglicht werden, Auskunftssperren ihrer Meldeadressen vorzunehmen. Die Bundesregierung muss einen Entwurf für eine entsprechende Änderung des Bundesmeldegesetzes (BMG) vorlegen.
- f) Gemeinsam mit den Ländern ist ein zentrales Online-Portal für Strafanzeigen bei Hass und Hetze, auf das Plattformbetreiber nach § 3 NetzDG bereits bei der Meldung von Inhalten unmittelbar erreichbar hinweisen sollen, mit automatischer Weiterleitung an die zuständigen örtlichen/regionalen Staatsanwaltschaften einzurichten.
- g) Es ist ein gegen Persönlichkeitsrechtsverletzungen nutzbares beschleunigtes Online-Verfahren zu schaffen durch einen entsprechenden Entwurf zur Änderung der Zivilprozessordnung.
3. im Hinblick auf die beim Bundeskriminalamt (BKA) geplante Zentralstelle (s. BR-Drs. 87/20) einen Entwurf für eine gesetzliche Regelung vorzulegen, die folgende Eckpunkte gewährleistet:
- a) Für sämtliche Informationen und Daten, die zu einem Meldevorgang gehören, muss eine strenge Zweckbindung bestehen.
 - b) Infolge der strengen Zweckbindung und kurzen Löschfristen im Hinblick auf sämtliche Informationen und Daten darf beim BKA weder infolge Nichtbearbeitung noch aus anderen Gründen eine Datensammlungen entstehen, die über eine rein statistische Auswertung im Hinblick auf die Erstellung eines (phänomenbezogenen) Lagebildes hinausgehen.
 - c) Sämtliche Informationen und Daten, die zu einem Meldevorgang gehören, dürfen aufgrund der strengen Zweckbindung beim BKA nur in Erfüllung der

die Staatsanwaltschaften unterstützenden Funktion der Vorprüfung eines Anfangsverdachts, gespeichert und verarbeitet werden und sind unverzüglich nach ihrer Weiterleitung an die zuständigen Stellen der Länder zu löschen, sofern nicht das BKA im konkreten Einzelfall aufgrund von § 4 Absatz 1 Satz 1 BKAG selbst die polizeilichen Aufgaben im Hinblick auf die Strafverfolgung wahrzunehmen hat. Jede weitere Nutzung oder Auswertung dieser Informationen und Daten ist ausgeschlossen.

- d) Das geplante Meldeverfahren ist mehrstufig auszugestalten, sodass zunächst nur die nach Auffassung der Provider Straftatbestände erfüllenden Inhalte (in anonymisierter Form) an das BKA übermittelt werden. Diese werden dort einer Vorprüfung auf einen Anfangsverdacht unterzogen. Erst bei Vorliegen und nach Feststellung eines solchen Verdachts kann das BKA in einem zweiten Schritt die vorhandenen, dem Schutz als TK-Verkehrsdaten unterliegenden IP-Adress- und Portdaten bei den Providern anfragen.
- 4. in dem geplanten Meldeverfahren (s. BR-Drs. 87/20) einen Entwurf für eine spezielle gesetzliche Benachrichtigungspflicht für Betroffene vorzulegen, damit Nutzerinnen und Nutzer beim BKA unabhängig von im Übrigen bestehenden Auskunftsansprüchen einen unbeschränkten Anspruch haben, um zu erfahren,
 - a) inwiefern eigene Äußerungen (Kommentare, Posts, Bilder usw.) vom BKA im Rahmen der neu geschaffenen Zentralstellenfunktion gegenwärtig auf strafrechtliche Relevanz geprüft werden und
 - b) ob und inwiefern zur eigenen Person Daten im Rahmen der neu begründeten Zentralstellenfunktion gespeichert oder verarbeitet wurden und zu welchem Zweck.
- 5. gemeinsam mit den Ländern die angemessene Ausstattung, Fortbildung und Aufstellung der relevanten Behörden sicherzustellen und dazu insbesondere folgende Maßnahmen umzusetzen:
 - a) Polizei und Justiz müssen technisch wie auch personelle hinreichend für die effektive Verfolgung von Hasskriminalität und Rechtsextremismus (im Netz) ausgestattet werden. Sie müssen systematische und regelmäßige Fortbildungen in diesem Bereich erhalten. Auch muss sichergestellt werden, dass ein abgestimmtes Vorgehen stattfindet.
 - b) Gemeinsam mit den Ländern ist die Einrichtung von Sonderdezernaten für Hasskriminalität bei den örtlichen/regionalen Staatsanwaltschaften und, mit Zuständigkeit für das jeweilige Land insgesamt, von Beauftragten für Hasskriminalität zur Beratung und Koordinierung der örtlichen Staatsanwaltschaften und zur Gewährleistung einheitlicher Maßstäbe der Rechtsanwendung zu vereinbaren. Solche Stellen sollten zugleich als leicht zugängliche Beratungsstellen für Betroffene organisiert und ausgestattet sein, mit vorhandenen anderen Beratungsstellen kooperieren und unter Wahrung von deren Autonomie einen geschützten Raum für Betroffene bilden.
 - c) Die Polizei braucht Vertrauen und jede und jeder soll Vertrauen in die Polizei haben können. Es ist daher notwendig, dass wissenschaftlich untersucht wird, wie verbreitet verfassungsfeindliche Einstellungen bei Beamtinnen und Beamten sind. Außerdem müssen Vorkommnisse wie menschenfeindliche, rassistische und antisemitische Äußerungen in Chatgruppen in den Behörden konsequent disziplinar- und strafrechtlich aufgearbeitet und statistisch erfasst werden. Auch muss Vorsorge getroffen werden, damit insbesondere das Disziplinarrecht seine Funktion in diesem Bereich erfüllen kann und rechtsextreme Bestrebungen in den Sicherheitsbehörden zuverlässig aufgedeckt und unterbunden werden. Im Übrigen soll die Fehlerkultur in den Sicherheitsbehörden allgemein verbessert werden (siehe dazu insbesondere

den Gesetzentwurf zur Schaffung einer unabhängigen Polizeibeauftragten, Drs. 19/7928).

- d) Auf die Länder hinzuwirken, die Aufsicht durch die Landesmedienanstalten zu stärken, das Medienkonzentrationsrecht dringend weiterzuentwickeln.
 - e) Gemeinsam mit den Ländern wirksame Instrumente zur Kontrolle von algorithmischen Entscheidungssystemen im Sinne des Medienstaatsvertrages sowie eine medien- und netzpolitische Gesamtstrategie zu entwickeln.
6. im Hinblick auf alle geplanten Auskunftsansprüche (s. BR-Drs. 87/20), die sich auf das Telekommunikationsgesetz (TKG) und zukünftig auch das Telemediengesetz (TMG) beziehen, einen Entwurf für eine gesetzliche Regelung in den Polizeigesetzen des Bundes und der Strafprozeßordnung vorzulegen, die die folgenden Eckpunkte gewährleistet:
- a) eine grundrechtskonforme Ausgestaltung mit entsprechenden grundrechtlich gebotenen, der Tiefe des jeweilig betroffenen Grundrechts (IT-Grundrecht, Recht auf informationelle Selbstbestimmung, Kernbereichsschutz) entsprechenden Schutzwerten gemäß der Rechtsprechung des Bundesverfassungsgerichts;
 - b) einschließlich einer gesetzlichen Pflicht zur Protokollierung (seitens der staatlichen Stelle), die mindestens die ersuchende Stelle, den Zeitpunkt des Ersuchens sowie (für eine genau definierte Dauer) die tragenden Gründe und den Inhalt des Ersuchens erkennbar macht sowie
 - c) eine explizite Ausnahme für alle Dienstleistungen, die eine inhaltliche Nähe zu einem besonders geschützten Vertrauensverhältnis (insbesondere im ärztlichen, anwaltlichen, journalistischen, steuerrechtlichen und im Bankbereich) haben;
 - d) von den so geregelten Auskunftsbeugnissen ausdrücklich auszunehmen sind alle besonders zu schützenden und auch nach geltendem Datenschutzrecht besonders IT-sicherheitsrechtlichen Vorkehrungen unterliegenden Passwörter und andere Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird.
7. geplante Änderungen des Strafgesetzbuches (s. BR-Drs. 87/20) wie folgt zu überarbeiten:
- a) Die Beleidigungsdelikte in Anlehnung an den Diskussionsentwurf des Bayerischen Staatsministeriums der Justiz für ein „Gesetz zur nachdrücklichen strafrechtlichen Bekämpfung der Hassrede und anderer besonders verwerflicher Formen der Beleidigung“ (Stand 04.11.2019 – www.justiz.bayern.de/ministerium/gesetzgebung/) regeln mit der Maßgabe, bei der Einbeziehung der Kommunalpolitiker und Kommunalpolitikerinnen in § 188 StGB-E (schwere Beleidigung, üble Nachrede, schwere Verleumdung) eine dem Bestimmtheitsgebot genügende Einbeziehung auch der in den Untergliederungen der Stadtstaaten tätigen sicherzustellen.
 - b) Bei der Änderung des § 140 StGB (Belohnung und Billigung von Straftaten) und des § 241 StGB (Bedrohung) muss der Grundsatz beachtet werden, dass das Strafrecht nur dann einzusetzen ist, „wenn ein bestimmtes Verhalten über sein Verbotensein hinaus in besonderer Weise sozialschädlich und für das geordnete Zusammenleben der Menschen unerträglich, seine Verhinderung daher besonders dringlich ist“ (BVerfGE 120, 224 (240, Rz 35)). Deshalb und mit Blick auf das geschützte Rechtsgut (den öffentlichen Frieden bzw. den individuellen Rechtsfrieden), die Rechtssicherheit und die Praxistauglichkeit muss die Bundesregierung

-
- die Tatbestanderweiterung auf das Billigen noch nicht begangener Straftaten (§ 140 StGB-E) und
 - die Tatbestanderweiterung auf die Bedrohung mit Vergehen (§ 241 StGB-E) anstatt wie bisher nur Verbrechen
- einer kritischen Überprüfung unterziehen.
- c) Die vorgeschlagene Meldepflicht (§ 3a Abs. 2 NetzDG-E) ist auf schwere Straftaten zu beschränken.
8. einerseits die Vermeidung von widersprüchlichen Doppelstrukturen mit Regelungen auf Länderebene, beispielsweise mit dem Online-Intermediäre regulierenden, neuen Medienstaatsvertrag und die Vereinbarkeit des Gesetzentwurfs mit dem Recht der Europäischen Union, beispielsweise die Ausweitung von Auskunftsansprüchen mit der E-Commerce-Richtlinie, zu gewährleisten. Andererseits sich insbesondere in den Trilogien sowie im Rahmen der deutschen Ratspräsidentschaft einzusetzen für eine rechtsstaats- und grundrechtskonforme Fassung a) des EU-Verordnungsentwurfs zur Verhinderung der Verbreitung terroristischer Inhalte b) des EU-Verordnungsentwurfs über Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen c) des geplanten Digital Services Act zur Ablösung der E-Commerce-Richtlinie sowie insgesamt für eine kohärente Regulierung in der EU sowie Vereinfachung der internationalen Rechtshilfe.
9. eine Evaluierung der im Rahmen des Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität getroffenen Regelungen zwei Jahre nach deren Inkrafttreten vorzusehen und den Deutschen Bundestag über die Ergebnisse zu unterrichten. Die Evaluierung soll unabhängig unter Einbeziehung wissenschaftlichen Sachverständigen erfolgen und die Wirkung, Anwendung, Umsetzung und Praxis der getroffenen Regelungen untersuchen.

Berlin, den 10. März 2020

Katrin Göring-Eckardt, Dr. Anton Hofreiter und Fraktion

Begründung

Organisierte Shitstorms gegen JournalistInnen, Beleidigungen der Ex-Freundin auf ihren Profilen in den sozialen Netzwerken, das Verbreiten von Sharepics mit Falschzitaten über PolitikerInnen, Gewaltdrohungen an Organisationen und Menschen, die sich in Projekten für Geflüchtete engagieren, das Erstellen und Zirkulieren von rechtsextremen „Feindeslisten“ - Hass und Hetze im Netz ist ein ebenso drängendes wie vielschichtiges Problem. Die bisherigen Antworten der Bundesregierung sind jedoch nicht ausreichend und weisen gravierende Mängel auf.

2017 wurde nach kontroverser öffentlicher Debatte das Netzwerkdurchsetzungsgesetz (NetzDG) verabschiedet und eine rasche Evaluierung angekündigt. Verbesserungsvorschläge dazu liegen seit langem auf dem Tisch (s. Antrag „Netzwerkdurchsetzungsgesetz weiterentwickeln – Nutzerrechte stärken, Meinungsfreiheit in sozialen Netzwerken sicherstellen“, BT-Drs. 19/5950 und Antrag „Transparenz und Recht im Netz – Maßnahmen gegen Hasskommentare, Fake News“ und Missbrauch von „Social Bots“, Drs. 18/11856).

Bislang ist noch nicht einmal die angekündigte Evaluation des Netzwerkdurchsetzungsgesetzes vorgelegt worden, obwohl teilweise weiter erhebliche Bedenken im Hinblick auf die schon geltenden Regelungen bestehen und es Diskussion und Überarbeitungsbedarf gibt. Dies gilt teilweise umso mehr für jene Regelungen, die nun durch den Gesetzentwurf der Bundesregierung zur Bekämpfung des Rechtsextremismus und der Hasskriminalität

(BR-Drs 87/20) hinzukommen sollen. Doch auch eine konsequente Reformierung des NetzDG kann das Problem von Hass im Netz allein nicht lösen. Dazu bedarf es einer Gesamtstrategie, die das Problem wirksam bekämpft, dabei Betroffene stärkt und Bürgerrechte wahrt.

Der jetzt vorliegende Gesetzentwurf der Bundesregierung bietet keine Gesamtstrategie, geht aber andererseits bei vielen seiner Maßnahmen weit über das wichtige und von uns geteilte Ziel der Bekämpfung von Rechtsextremismus und Hasskriminalität hinaus. Vielmehr nutzt der Entwurf wie so oft in der Großen Koalition den Anlass, um undifferenziert eine Symbolpolitik der Sicherheit zu betreiben. Das betrifft vor allem, aber nicht nur die ausufernde Erweiterung von Auskunftsbefugnissen nahezu aller Sicherheitsbehörden gegenüber Telemedien-diensten. Sogar Kunden-Passwörter müssten von Unternehmen herausgegeben geben und bestehende Schutzstandards der IT-Sicherheit und des Datenschutzes würden potentiell geschwächt. Und das gewählte Konzept der Übermittlungspflicht durch private Telemedienunternehmen führt zu erheblich in die Grundrechte eingreifenden Maßnahmen, weil schon im Vorfeld eines behördlichen Verdachts persönliche Informationen und Daten an das Bundeskriminalamt gelangen.

Die daraus entstehenden Probleme werden insbesondere in der Vielzahl ausführlicher kritischer Stellungnahmen unterschiedlichster Akteure zum Regierungsentwurf aufgezeigt. Auf deren zahlreiche gewichtige Argumente ist die Bundesregierung bisher nicht hinreichend eingegangen.

Ein zentrales Problem bei der Bekämpfung von Hass im Netz ist das fehlende Verständnis der Komplexität des Phänomens. Hass und Hetze im Netz können nicht als von der analogen Welt losgelöstes Problem betrachtet werden. Die Attentate von Hanau, Halle, Christchurch oder der Mord an Walter Lübcke haben in unterschiedlicher Weise die Verbindungen zwischen rechtsextremer Hetze und Vernetzung im Internet und physischen Gewalttaten aufgezeigt. Dabei lassen sich verschiedene Ebenen von Hass und Hetze im Netz erkennen.

Zum einen ist Hass eine Strategie des organisierten Rechtsextremismus mit dem Ziel demokratische Strukturen zu zerstören. Dazu werden wohl orchestrierte Hass-Kampagnen gegen Organisationen, PolitikerInnen, JournalistInnen oder zivilgesellschaftlich engagierte Menschen gefahren, die darauf abzielen, diese mundtot zu machen oder aus dem Engagement für die Demokratie zu drängen. Dies geschieht durch Beleidigungen, Verleumdungen, Drohungen oder das Erstellen von „Feindeslisten“ im Netz. Das rechtsextreme Spektrum greift dabei auf verschiedene Strukturen und Organisationsformen, von geschlossenen Gruppen und Foren bis zu losen offenen Kanälen zurück, in denen sich Menschen radikalisieren und vernetzen können oder inspirieren lassen, wie zuletzt bei der Aufdeckung der „Gruppe S.“ deutlich wurde.

Zusätzlich zum organisierten Rechtsextremismus erleben wir eine allgemeine Verrohung der Kommunikations- und Debattenkultur im Internet, bei der Beleidigungen und Herabwürdigungen anderer auf der Tagesordnung stehen. Dieser Hass ist häufig eine Fortsetzung von Gewalt aus der analogen Welt und mit Formengruppenbezogener Menschenfeindlichkeit verknüpft. Hier brechen sich Rassismus, Antisemitismus, Antiziganismus, Muslimfeindlichkeit, Homo- und Transfeindlichkeit, Antifeminismus oder Behindertenfeindlichkeit Bahn. Nicht erst seit den rechtsterroristischen Anschlägen von Hanau und Halle ist offensichtlich, dass rechtsextreme Täter nicht nur ein rassistisches sondern auch ein zutiefst antifeministisches Weltbild teilen. Der besonderen Betroffenheit von Frauen von Hass im Netz Rechnung zu tragen, ist unerlässlich.

Aktuell sehen wir eine Gleichzeitigkeit verschiedener Initiativen zu Hass (im Netz) und Rechtsextremismus durch die Bundesregierung, die sich jedoch nur Teilbereichen des Problems annehmen.

Die Perspektive der von Hass und Hetze Betroffenen und die Frage, wie wir sie stärken können, finden in den aktuellen Vorhaben zu wenig Beachtung. Die Betroffenen haben nicht nur mit den unmittelbaren Folgen von Hass und Hetze zu kämpfen. Zusätzlich werden sie durch immer noch umständliche Meldewege auf den Plattformen, einen Mangel an Beratungsangeboten, die sie z. B. über rechtliche Möglichkeiten informieren vor große Herausforderungen gestellt. Auch bei Opferschutzmaßnahmen besteht großer Verbesserungsbedarf.

Hass und Hetze im Netz sind zudem nicht nur ein strafrechtliches Problem. Gerade rechtsextreme Gruppen wissen genau, wie sie an der Grenze zur Strafbarkeit legale, wenn auch hasserfüllte Kommentare formulieren können. Genauso dringlich braucht es daher auch Verbesserungen für Prävention, Forschung, Beratung und Opferschutz.

Nicht zuletzt machen Hass und Hetze im Netz nicht vor Landesgrenzen Halt. Sämtliche Vorhaben müssen mit EU-Recht und Vorgaben vereinbar und das Ziel ein EU-weit koordiniertes Vorgehen sein.

gierung, der parallel auch von den Koalitionsfraktionen in den Deutschen Bundestag eingebracht wurde, im Einzelnen nach Vorliegen der Stellungnahme des Bundesrates und im Lichte öffentlicher Anhörung sowie im Zusammenhang mit den von der Bundesregierung geplanten weiteren, bislang nur als Referentenentwurf vorliegenden Änderungen des Netzwerkdurchsetzungsgesetzes (NetzDG) in weiteren Anträgen zu behandeln.



BfDI

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Entwurf 19915/2020

Prof. Ulrich Kelber
Bundesbeauftragter
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

1. An den
stv. Vorsitzenden
Ausschusses für Recht und Verbraucher-
schutz des Deutschen Bundestages
Herrn Dr. Heribert Hirte

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn

FON (0228) 997799-5000

FAX (0228) 997799-5550

Deutscher Bundestag E-MAIL referat32@bdi bund.de
Ausschuss für
Recht und Verbraucherschutz
www.datenschutz.bund.de
Ausschussdrucksache
19(6)121
Ausschuss
GESCHÄFTS
Bonn, 02.03.2020
32-642/041#1435

2. An die
Vorsitzende
Ausschusses für Inneres und Heimat
Frau Andrea Lindholz

Bitte geben Sie das vorstehende Geschäftszeichen
bei allen Antwortschreiben unbedingt an.

10. März 2020

3. An den Vorsitzenden
des Ausschusses Digitale Agenda
Herrn Manuel Höferlin

4. An den
Vorsitzenden
des Ausschusses für Wirtschaft und Energie
Herrn Klaus Ernst

VERANLAGT	FE	MAI
MAI	05. März 2020	12.03.20
MAI	Prof. Dr. Heribert Hirte 3248	20A
Telefonüberschreibband		

Platz der Republik 1
11011 Berlin

BETREFF Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität

BEZUG BR-Drucksache 87/20

ANLAGEN 1

Sehr geehrter Herr Vorsitzender,

der Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität dürfte in Kürze in Ihrem Ausschuss beraten werden. Vor diesem Hintergrund übersende ich Ihnen meine Stellungnahme zu diesem Gesetzentwurf und wäre Ihnen für eine Einbeziehung in Ihre Beratungen dankbar.



BfDI

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Seite 2 von 2

Für weitere Fragen stehe ich Ihnen gerne zur Verfügung..

Mit freundlichen Grüßen

Ulrich Kelber

**BfDI**

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 26.02.2020

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit teilt die dem Gesetzentwurf zugrunde liegende Auffassung, nach der Betroffene vor Bedrohungen effektiv geschützt werden sollten. Hierbei hilft aber in erster Linie ein effektiver Gesetzesvollzug durch die Sicherheitsbehörden. Zudem helfen nur solche Sicherheitsgesetze, die mit Bedacht erlassen und zielgerichtet ausgestaltet werden. Der vorliegende Entwurf enthält zahlreiche Vorschläge, die deutlich über den Bereich von Hasskriminalität und Rechtsextremismus hinausgehen. Ob der Entwurf seine verfolgten Ziele erreicht, erscheint mir mehr als fraglich.

I. Allgemein

Der Entwurf enthält erhebliche Eingriffe in Grundrechte der Bürgerinnen und Bürger. Es ist zweifelhaft, ob diese in jeder Hinsicht erforderlich und damit verhältnismäßig sind. Bereits die Grundkonzeptionen der Meldepflicht und der Rolle des Bundeskriminalamtes (BKA) werfen erhebliche Fragen auf. Insgesamt ist fraglich, ob überhaupt ein schlüssiges Konzept vorliegt, um dem Phänomen der rechtsextremistischen Hasskriminalität effektiv zu begegnen. Ich rege an, zunächst empirisch zu untersuchen, wie die zuständigen Einrichtungen und Behörden in Bund und Ländern aufgestellt sind. Denn neue gesetzliche Vorschriften helfen nicht bei bestehenden Vollzugsdefiziten. Möglicherweise ist es ohnehin nicht nötig, die bestehende Praxis völlig neu zu gestalten. Beispielsweise haben einzelne Länder

Husarenstraße 30
53117 Bonn

Fon: 0228 / 997799-0

Fax: 0228 / 997799-550

E-Mail: poststelle@bfdi.bund.de

Schwerpunktstaatsanwaltschaften eingerichtet, die als zentrale Anlaufstellen bereits jetzt tätig werden.

In der jüngeren Vergangenheit sind mir zahlreiche Gesetzentwürfe vorgelegt worden, die in kurzen Abständen zum Beispiel immer wieder die Strafprozessordnung betrafen. Zu nennen sind etwa die Entwürfe für ein „Gesetz zur Modernisierung des Strafverfahrens“, für ein „Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679“ oder für ein „Gesetz zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze“. Deshalb stellt sich die Frage, welchem durchgängigen Konzept diese Gesetzgebungstätigkeit folgt.

II. Meldesystem

Mit der föderalen Struktur in Deutschland wurde ein Schlussstrich unter die vormalige „Sicherheits“-architektur gezogen und die ausführende Verantwortung für die innere Sicherheit den Ländern zugewiesen. Auf der Ebene des Bundes sollte es nach dem Willen des Grundgesetzes keine starke Bundespolizeibehörde mehr geben. Die Polizeigewalt sollte in den Ländern liegen. Parallel wurden im Bereich von Rundfunk und Presse Aufsichtsstrukturen geschaffen, die möglichst nur Eingriffe durch unabhängige Gremien regeln sollten, nicht jedoch durch Vollzugsbehörden im klassischen Sinne. Deshalb entstanden Rundfunkräte und Institutionen der freiwilligen Selbstkontrolle, wie z.B. der Presserat, später in dieser Tradition die Medienanstalten der Länder.

Über diese könnte heute ebenfalls ein „Meldewesen“ für problematische Inhalte organisiert werden – sofern dies überhaupt erforderlich und nicht bereits vorhanden ist. Zudem gibt es auf der strafrechtlichen Ebene bereits in den Ländern zentrale Anlaufstellen. Dass derartige Alternativen nicht umfassend untersucht und gegebenenfalls evaluiert worden sind, ist bereits strukturell zu kritisieren.

Geplant ist nun, dass Anbietern von Telemediendiensten – insbesondere sozialen Netzwerken – eine Meldepflicht an das BKA auferlegt wird. Nach Beschwerden müssen diese zunächst intern prüfen, ob die von Nutzern hochgeladenen und über die Mediendienste verbreiteten Inhalte gegen bestimmte im Gesetz genannte Vorschriften verstoßen. Anschließend sollen sie an das BKA melden.

Damit wird der Schwerpunkt der praktischen Tätigkeit zunächst nicht bei den Ländern liegen, sondern zentral zum Bund verschoben. Die betroffenen Straftaten – bzw. hier: Sachverhalte mit strafrechtlichem Anfangsverdacht – bewegen sich aber in einem rechtsdogmatisch höchst komplexen Umfeld. So ist zu hinterfragen, in welchen Fällen „konkrete Anhaltspunkte“ für die genannten Straftaten vorliegen und wie die Anbieter der sozialen Netzwerke dies künftig beurteilen sollen.

§ 3a Abs. 4 Nr. 2 NetzDG-E sieht für die Übermittlung der Anbieter unter anderem vor, die IP-Adresse einschließlich Portnummer, die der Nutzer verwendet hat, an das BKA zu übermitteln, soweit diese vorhanden sind. Diese Daten sind herauszugeben, bevor überhaupt das Vorliegen eines Anfangsverdachts von einer Strafverfolgungs- bzw. Polizeibehörde geprüft wurde. Zu bevorzugen wäre eine Regelung, nach der die Verpflichteten zunächst nur den Inhalt übermitteln und erst nach der Feststellung eines Anfangsverdachts bzw. einer Gefahrenlage die IP-Adresse einschließlich Portnummer übermitteln. Bis dahin könnten die Daten zunächst im „quick freeze“ Verfahren gespeichert werden.

III. Auskunftsverfahren und weitere Datenverarbeitung

1. Ausgangspunkt: Telemedienanbieter („Übermittlungstür“)

Neben dieser Meldepflicht will der Entwurf die Auskunft zu Nutzungs- und Bestandsdaten in § 15a TMG neu definieren und erweitern. Dies ist eine allgemeine Regelung, die nicht nur die Meldungen nach dem Netzdurchsetzungsgesetz betrifft, also nicht nur den in der Überschrift genannten Rechtsextremismus und die Hasskriminalität. Sie regelt vielmehr alle Bereiche bis hin zu allgemeinen Ordnungswidrigkeiten.

Nach dem sog. Doppeltürmodell des Bundesverfassungsgerichts sind die geplanten §§ 15a, 15b TMG nur Übermittlungsnormen („Übermittlungstür“). Sie setzen bei den Empfängerbehörden als Gegenstück eine Erhebungsnorm voraus („Empfängertür“). Allgemeine „Übermittlungstür“ für die Anbieter von Telemediendiensten ist der neue § 15a TMG-E. Der Zugriff auf Passwörter und andere Daten, die den Zugriff auf Endgeräte oder Speichereinrichtungen ermöglichen, wird in einer eigenen Vorschrift, dem § 15b TMG-E geregelt.

a) Allgemeine Auskunftsregelung, § 15a TMG-E

Der geplante § 15a TMG-E gilt niedrighschwellig für alle Ordnungswidrigkeiten, Straftaten, Gefahren für die Öffentliche Sicherheit und die Übermittlung an Nachrichtendienste. Anders als § 113 Abs. 1 TKG rechtfertigt er es nicht nur, Bestandsdaten zu übermitteln, sondern auch Nutzungsdaten. Das stellt eine höhere Eingriffsqualität dar.

Die Vorschrift enthält eine Formulierung, nach der „alle unternehmensinternen Datenquellen“ zu berücksichtigen sind. Damit können umfangreiche Nutzungsprofile herausverlangt werden. Wann dies verhältnismäßig ist, wird sich letztlich anhand der Vorschriften für den Zugriff auf diese Daten entscheiden („Empfängertür“). Gleichwohl wirft die weite Öffnung des § 15a TMG, der auch die Übermittlung bei Ordnungswidrigkeiten zulässt, erhebliche Fragen auf.

b) Zugangsdaten (Passwörter etc.), § 15b TMG-E

Positiv zu bewerten ist zwar, dass der Entwurf in § 15b Abs. 2 TMG-E nun deutlich höhere Übermittlungsschwellen vorsieht. Gleichwohl sehe ich die Regelung weiterhin kritisch.

Zugangsdaten sind vor allem – aber ggf. nicht nur – Passwörter, Access Tokens, Geheimnisse für Zwei-Faktor-Authentifizierungs-Apps (2FA) und andere Daten, die dazu dienen, die nutzende Person zu authentifizieren oder ihr Zugang zu Angeboten und Diensten zu ermöglichen.

Nach dem geplanten § 15b TMG stellen sich bereits auf der Übermittlungsebene verschiedene Fragen. Zunächst ist darauf hinzuweisen, dass eine Vielzahl von Diensten erfasst sein kann. Neben E-Mail-Diensten und Cloud-Speichern kann dies etwa auch Online-Händler oder Angebote von Online-Banking betreffen. Auch deren Passwörter wären herauszugeben. Hier stellt sich besonders die Frage der Datensicherheit.

Technisch gesehen müssen gesetzeskonform arbeitende Anbieter die Passwörter als Hash speichern und können sie deshalb nicht in einer einfach verwendbaren Form herausgeben. Sie können deshalb nicht unmittelbar für den Zugriff auf Endgeräte oder Speichereinrichtungen verwendet werden.

Nach Kritik in der Ressortabstimmung regelt § 15b Abs. 3 Satz 2 nunmehr, dass die Verschlüsselung „unberührt“ bleibt. Wenn das ernst gemeint ist, stellt sich aber die Frage, welchen Sinn die Herausgabe der Zugangsdaten hat. Eine gute Verschlüsselung ist so gestaltet, dass der Provider die Daten ohne Eingabe durch den Kunden nicht selbst entschlüsseln kann. Gemeint sein dürfte also möglicherweise Folgendes:

Gemäß dem geplanten § 15b Abs. 1 S. 2 TMG-E sollen die Provider auch an dieser Stelle „sämtliche unternehmensinternen Datenquellen“ nutzen, um den Behörden Zugangsdaten zur Verfügung zu stellen. Danach müssten ggf. alle technischen Daten mit herausgegeben werden, mit denen die Kundenschlüssel generiert werden (z.B. also etwa Verschlüsselungsalgorithmen oder der sog. Pepper-Wert). Diese Informationen ermöglichen insbesondere erleichterte brute-force-Entschlüsselungen der übermittelten Passwort-Hashes.

Auch dies könnte die Datensicherheit über den Einzelfall hinaus beeinträchtigen. Werden solche Daten herausgegeben, kann das gegebenenfalls nicht nur die Zielperson des Verfahrens, sondern alle Kunden betreffen.

Letztlich müsste man dann in all diesen Fällen fragen, ob die nach der Zahlungsdiensterichtlinie notwendige Sicherheit der Authentifizierung noch gewährleistet ist. Da sich das TMG nicht nur an Verbraucher richtet, ist zudem fraglich, ob etwa Banken dann noch un-

tereinander sicher kommunizieren könnten oder sich die Bundesrepublik aus dem elektronischen Bankenverkehr zurückziehen müsste.

Eine – ggf. mittelbare – Pflicht zu einer einfach aufzuhebenden Verschlüsselung lehne ich ab. Neben anderen Argumenten (Missbrauchsgefahr, Ermittlungsbehörde könnte unter der Identität des Beschuldigten auftreten) verstieße diese gegen höherrangiges Recht. Gemäß Art. 32 DSGVO müssen Anbieter technische und organisatorische Maßnahmen zur Datensicherheit treffen. Hierzu gehört auch die unter Berücksichtigung des Stands der Technik sichere verschlüsselte Speicherung und Übermittlung von Passwörtern. Dies hat auch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in der "Orientierungshilfe „Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung“ vom 29.03.2019 klargestellt.

Unklar ist im Übrigen, wie etwa in Fällen der zwei-Faktor-Authentifizierung vorzugehen ist, die z.B. beim Online-Banking durch die neue Zahlungsdiensterichtlinie nunmehr verpflichtend vorgesehen ist. Ebenfalls ist unklar, ob sich die Vorschriften auch auf etwaige temporär gespeicherte Session-Cookies o.ä. beziehen, mit denen sich Zugang erlangen lässt. Auch dafür könnte die Formulierung im geplanten § 15b Abs. 1 S. 2 TMG-E sprechen. Dazu müssten auch Sicherungs- oder Protokolldatenserver einbezogen werden. Selbst Dateien des betrieblichen Datenschutzbeauftragten blieben nicht verschont. Unklar ist, wie die im Ausland gespeicherten Daten betroffen sind. Zu dieser Problematik hat die DSK in einer Entschließung zum Entwurf einer e-Evidence-VO kritisch Stellung genommen.¹

2. Verarbeitung beim BKA („Erhebungstür“ und weitere Schritte)

a) Erweiterte Auskunftsbefugnisse

Mit der neuen Regelung im TMG korrespondiert die geänderte Erhebung zu Zwecken der Zentralstelle. Diese war bislang für Telekommunikations-Bestandsdaten in § 10 BKAG geregelt und wird jetzt auf Telemediendaten erweitert. Für sie ist ein Anfangsverdacht im Sinne der Strafprozessordnung nicht erforderlich. Auch sonst werden keine besonderen Verdachts- oder Gefahrenmomente gefordert. Es genügt, dass die Daten für folgende Aufgaben erforderlich sind: „Aufgaben als Zentralstelle nach § 2 Absatz 2 Nummer 1 und Absatz 6 zur Ergänzung vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung“, daneben Zeugenschutz und Personenschutz. Aus diesem Grund hatte ich bereits in der Vergangenheit die bisherigen Vorschriften kritisiert, zuletzt in meiner Stellungnahme ge-

¹

https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/20181107_EntschliessungE_Evidence.pdf; siehe dazu auch https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/Stellungnahmen/Opinion23_2018_eevidence.pdf

genüber dem Bundesverfassungsgericht. Schon nach alter Rechtslage konnte das BKA Passworte zu Telekommunikationsdiensten herausverlangen (betrifft PIN und PUK).

Die Erhebungen in der Zentralstellenfunktion hatte ich im Jahr 2017 kontrolliert und dabei insbesondere die unzureichende Dokumentation kritisiert. Allerdings hatte ich mit Verweis auf die anstehende Prüfung des Vorgangsbearbeitungssystems beim BKA keine Beanstandung ausgesprochen. Zu weiteren Punkten verweise ich auf den Bericht.²

Für die TMG-Daten soll nach dem Entwurf jetzt eine ähnliche Regelung gelten.

Anders als in einem ersten Entwurf soll der geplante § 10 BKAG-E nach erheblicher Kritik nicht mehr den Zugriff auf die Zugangsdaten einschließlich Passwörter regeln. Das ist zu begrüßen. Anwendbar sind deshalb allein die Vorschriften der sog. Online-Durchsuchung.

b) Empfang der Meldungen der Anbieter

Übermitteln die Anbieter ihre Meldungen nach dem NetzDG-E, ist dafür ebenfalls der genannte § 10 BKAG die Rechtsgrundlage. § 10 BKAG setzt keinen Anfangsverdacht voraus. Das BKA soll also unabhängig davon Daten erheben dürfen, ob ein strafrechtlicher Anfangsverdacht vorliegt oder nicht. Das BKA wird insofern nicht als strafrechtliche Ermittlungsbehörde tätig, sondern soll sich auf die Vorschriften zur Zentralstellenaufgabe stützen.

Dazu, wie das BKA mit den Meldungen weiter verfahren soll, enthält der Gesetzestext keine Regelungen. Das BKA könnte auf der einen Seite nur kurz prüfen, welche Landesbehörde zuständig ist, den Sachverhalt an das Land abgeben und gleichzeitig die Daten aus dem eigenen Bestand löschen. Auf der anderen Seite könnte das BKA die Daten aber nach dem im Jahr 2018 neu gefassten BKAG – z.B. als „Prüffall“ gemäß § 18 Abs. 3 BKAG, ggf. auch nach §§ 18 Abs. 1 und 2 BKAG – in das Informationssystem eingeben und Querverbindungen suchen. Die Datenverarbeitung würde dadurch ein höheres Gewicht erhalten. Für die zukünftige beim BKA geführte bundesweite informationstechnische Basis „Polizei 2020“ ist eine Speicherung aller Daten in einem „Datenpool“ vorgesehen, der umfassende Querverbindungen erlaubt. Welche Datenanalysen möglich sein werden, ist derzeit noch unklar.

Das Verfahren sollte m.E. in der Praxis so ausgestaltet werden, dass das BKA zunächst prüft, ob überhaupt ein Anfangsverdacht vorliegt. Kann dies bejaht werden, sollte es den Sachverhalt sofort an die zuständige Landespolizei bzw. Staatsanwaltschaft abgeben. Nur wenn diese aufgrund der fehlenden Bestandsdaten nicht bestimmt werden kann, sollte

² Der Bericht ist unter folgendem Link verfügbar: https://fragdenstaat.de/anfrage/kontrolle-beim-bka/403928/anhang/BfDI_Prfrbericht_BKA_geschwaerzt_geschwaerzt.pdf; siehe dazu auch 27. TB Nr. 9.3.6.1

das BKA befugt sein, weitere Daten zu erheben, soweit dies erforderlich ist, um die zuständige Polizeibehörde zu bestimmen. Der geplante Gesetzestext enthält hierzu aber keine Vorgaben.

3. Strafverfolgung

Zur Strafverfolgung werden insbesondere die §§ 100g, 100j StPO für Telemediennutzungs- bzw. Bestandsdaten ergänzt.

a) § 100g StPO (Artikel 2 Nr. 2)

Die Vorschrift über Telekommunikationsverkehrsdaten wird es in Zukunft auch erlauben, Telemediennutzungsdaten zu erheben. Beide werden tatbestandlich gleichgestellt. Es ist aber die Frage zu stellen, ob beides dieselbe Eingriffsintensität hat. Zwar ließe sich hier ein unterschiedlicher Anwendungsbereich des Art. 10 GG diskutieren. Zu bedenken ist aber, dass Telemediennutzungsdaten unter Umständen stärkere Aufschlüsse darüber zulassen, mit welchen Inhalten sich die betroffene Person beschäftigt hat. Anders als Telekommunikationsverkehrsdaten lassen Telemediennutzungsdaten ggf. nicht nur den Schluss auf die an einer Kommunikation beteiligten Personen zu, sondern zum Beispiel auch über aufgerufene Webseiten oder Angebote. Daraus lassen sich im Einzelfall umfangreiche Rückschlüsse über die Persönlichkeit der betroffenen Person ziehen.

b) § 100j (Artikel 2 Nr. 3)

Schwelle für die Erhebung von Passwörtern und anderen Zugangsdaten ist nur, dass die Herausgabe „für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist“. Materiell ist damit ein Anfangsverdacht einer beliebigen Straftat Voraussetzung. Ein Straftatenkatalog ist nicht vorgegeben. Damit ist die Erhebungstür in § 100j StPO prinzipiell weiter gefasst als die Übermittlungstür in § 15b TMG.

Diese Divergenz ist erklärungsbedürftig. Nicht nachvollziehbar ist, aus welchen Gründen die Ermittlungsbehörde unter niedrigeren Voraussetzungen auf die Daten zugreifen können soll, als die Übermittlungsregelung dies zulässt. Zutreffend verweist § 15b TMG-E auf die Voraussetzungen des § 100b StPO.

Allerdings ist die vom BVerfG für den Bereich der Telekommunikation geforderte Formulierung enthalten, nach der zusätzlich die *gesetzlichen Voraussetzungen für die Nutzung der Daten* vorliegen müssen.

Bei den bislang von § 100j StPO umfassten Telekommunikationsdaten ist immerhin klar, dass die Inhalte nur über eine gesetzliche Befugnis zur Telekommunikationsüberwachung erhoben werden können. Hier aber sehe ich das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme betroffen. Denn der Sache nach geht es um den Zugriff auf die auf einem solchen System gespeicherten Daten. Insofern verweist § 15b TMG folgerichtig auf § 100b StPO, der die Online-Durchsuchung regelt.

Denkbar wäre zwar auch der offene Zugriff. Dafür könnten insoweit wohl die Regelungen zur Beschlagnahme in der StPO in Betracht kommen. Die Maßnahme muss dafür der betroffenen – d.h. den Account besitzenden – Person gegenüber bekannt sein. Heimlich ist ein solcher Zugriff nur als Online-Durchsuchung vorstellbar. Heimlich ist der Zugriff etwa dann, wenn er nur dem Diensteanbieter mitgeteilt wird, nicht hingegen dessen betroffener Kundin oder dem Kunden gegenüber. Möglicherweise ist aber ein solcher offener Zugriff kaum denkbar. Denn die den Zugang ermöglichenden Daten liegen der Behörde in einer Weise vor, die tatsächlich eine heimliche Nutzung von Beginn an ermöglicht. Im Falle nur offener Maßnahmen wäre dies zwar rechtlich unzulässig, aber technisch nicht ausgeschlossen. Solange dies aber nicht ausgeschlossen oder zumindest kontrollierbar ist, kommen hier allein die Vorschriften zur Online-Durchsuchung für den Zugriff in Betracht. Deshalb ist unverständlich, weshalb die Regelung nicht in § 100b StPO verankert ist.

Bei der klassischen Online-Durchsuchung besteht die rechtliche Anforderung, dass alle Ermittlungsschritte und Datenzugriffe zu protokollieren sind. Es muss stets nachvollziehbar sein, welche Daten die Behörde ausgelesen oder gar verändert hat. So muss technisch ausgeschlossen werden, dass etwa die Polizeibehörde selbst – sei es absichtlich oder versehentlich – Beweise verändert oder Daten „im Namen“ des Beschuldigten gespeichert oder irgendwohin weitergeleitet hat. All dies ist aber nicht möglich, sobald der Behörde Benutzerkennung und Passwort im Klartext vorliegen und der Zugriff hierauf nicht technisch streng reglementiert ist. Es würde dann für die betroffene Person kaum je praktisch nachweisbar sein, dass sie nicht selbst gehandelt hat. Sobald das Passwort mehr als einer Person bekannt wird, kommen im Übrigen alle diese Personen als Tatverdächtige in Betracht, sobald danach Straftaten mit dem betreffenden Account begangen werden. Dies schließt Polizeibeamte, Staatsanwälte und Richter nicht aus. Insofern betreffen die Fragen der Datensicherheit auch den Schutz der Mitarbeitenden von Polizei, Staatsanwaltschaften und Gerichten. Deshalb stellt sich die Frage, wo das Passwort bei der Ermittlungsbehörde hinterlegt werden soll. Wer erhält innerhalb der beteiligten Behörden Kenntnis? An welche weitere Behörde darf die erhebende Behörde das Passwort reversibel verschlüsselt oder gar im Klartext übermitteln? An welcher Stelle bzw. in welchem Informationssystem legt die Behörde es ab? Wie wird revisionssicher protokolliert, von wem, wann, in welcher Form und zu welchem Zweck das Passwort eingesetzt wurde und welche Daten im Zielsystem dabei erhoben, verändert, gelöscht oder übermittelt wurden?

Wenn überhaupt müsste die Übergabe und Nutzung von Passwörtern oder sonstigen Zugangsmöglichkeiten für die Online-Durchsuchung deshalb in der jeweiligen Spezialbefugnis geregelt werden, also insb. in § 100b StPO. Dann würden zumindest die Protokollierungspflichten nach § 100c Abs. 6 StPO i.V.m. § 100b Abs. 4 StPO frühzeitiger greifen. Im vorliegenden Entwurf ist das Passwort – unabhängig von den Vorgaben des § 100b StPO – nach § 100j StPO zu übermitteln. Damit entstehen die genannten Probleme der Datensicherheit.

Es ist zwar –für Passwörter – in § 100j Abs. 2 StPO ein Richtervorbehalt vorgesehen. Jedoch hat etwa eine im Auftrag des BMJV durchgeführte Evaluation der besonders eingriffsintensiven Telekommunikationsüberwachung gezeigt, dass nur 23,5 Prozent der richterlichen Beschlüsse als substantiiert begründet gewertet werden können.³ Entscheidend sind im Übrigen nicht die verfahrensmäßige Absicherung, sondern die materiellen Schwellen, die eingezogen sind. Insbesondere kann der Richtervorbehalt Bestimmtheitsdefizite nicht kompensieren (BVerfGE 113, 348, 378). Vor allem umfasst die richterliche Kontrolle nicht, in welcher Form die Passwörter bei den Ermittlungsbehörden verarbeitet werden und wie ihre Verwendung revisionssicher protokolliert wird.