Berlin, 16. Januar 2020

Digitale Gesellschaft e. V.
Groninger Str. 7
D - 13347 Berlin

(030) 450 840 18

info@digitalegesellschaft.de
www.digitalegesellschaft.de

Stellungnahme

der Digitalen Gesellschaft e.V.

an das Bundesministerium der Justiz und für Verbraucherschutz

zum

Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität

Die Digitale Gesellschaft e.V. begrüßt, dass die Bundesregierung gegen rassistische, antisemitische und nationalistische Straftaten und Hasskriminalität vorgehen möchte. Die im oben genannten Gesetzesentwurf vorgeschlagenen Maßnahmen sind jedoch nicht nur ungeeignet, sondern letztlich kontraproduktiv. Sie bringen enorme Eingriffe in die informationelle Selbstbestimmung und die Informationssicherheit mit sich, die nicht nur Straftäter und Straftäterinnen betreffen werden und insgesamt nicht gerechtfertigt sind. Die Digitale Gesellschaft e.V. kritisiert, dass das Ministerium den Fokus seines Vorgehens gegen „Rechtsextremismus“ auf Strafverfolgungs- und Überwachungsmaßnahmen im Raum sozialer Medien legt. Dies reduziert das gesamtgesellschaftliche Problem des Erstarkens von Nationalismus, Rassismus und Antisemitismus und von Straftaten gegen Andersdenkende insgesamt auf einen kleinen Teil des kommunikativen Raums. Hingegen mangelt es an Maßnahmen, die den Schutz der Betroffenen erhöhen und die gesellschaftlichen Ursachen bekämpfen.

Im Folgenden soll zu einigen ausgewählten Vorschlägen Stellung genommen werden.

Verschärfung von Strafnormen

Der Referentenentwurf beinhaltet umfangreiche Verschärfungen von Strafnormen.

Das Strafrecht muss in einem Rechtsstaat ultima ratio sein und darf nur fragmentarisch besonders schwere sozialschädliche Verhaltensweisen ahnden. Insofern ist die im Entwurf erkennbare Tendenz, als für das gesellschaftliche Klima schädlich eingestufte Äußerungen möglichst umfangreich unter Strafe zu stellen, rechtsstaatswidrig und gefährlich für die Demokratie. Dies gilt insbesondere, als es sich regelmäßig um öffentliche Äußerungen handelt, bei deren Klassifizierung als erlaubt oder verboten die verfassungsrechtlich geschützte Meinungsfreiheit besonders zu beachten ist.

Aus kriminalpolitischer Sicht stellt sich zudem die Frage, ob die Erweiterung bestehender Straftatbestände und Strafmaßverschärfungen präventive Wirkungen versprechen oder aber im Sinne einer Vergeltungsfunktion des Strafrechts zum sozialen Frieden beitragen können. Derzeit werden bestehende Strafgesetze im Bereich Hasskriminalität auf Social Media in der Regel nicht konsequent durchgesetzt. Eine Vielzahl von Betroffenen berichtet, dass sie regelmäßig Anzeigen erstatten, aber eine Strafverfolgung in den seltensten Fällen stattfindet. Dies könnte darauf zurückzuführen sein, dass die angezeigten Äußerungen keine Straftaten darstellen. Ein wesentlicher Grund für die Nichtverfolgung ist jedoch auch in mangelnden Ressourcen und fehlender Ausbildung sowie Spezialisierung bei den Strafverfolgungsbehörden zu sehen. Ein Ausbau von Strafvorschriften kann für die Normeinhaltung in dieser Situation kontraproduktiv sein: Die Schaffung neuer Straftatbestände, deren Anwendung nicht gewährleistet ist, birgt die Gefahr einer weiteren Erosion des Vertrauens von Bürgerinnen und Bürgern in die Geltung von Strafgesetzen.

Auf der anderen Seite schafft die Veränderung des § 140 StGB in den sozialen Netzwerken eine tiefe Verunsicherung, da schon ein flüchtiger Like an der falschen Stelle zur Strafverfolgung führen kann. Die Streichung weniger Worte - „nachdem sie begangen oder in strafbarer Weise versucht worden ist," - führt, dazu, dass nicht nur die Billigung begangener oder versuchter Straftaten erfasst wird, sondern auch die Billigung noch nicht erfolgter Straftaten.

Auskunftspflichten für Telemedienanbieter

Die Pflichten von Telemedienanbietern zur Herausgabe von Bestands- und Nutzungsdaten sollen umfangreich neugeregelt werden. Diese Neuregelungen betreffen alle, die geschäftlich Telemediendienste erbringen. Dabei handelt es sich um eine Vielzahl von Onlinediensten, Websitebetreibern, Mailservices, Online-Shops, Instant-Messenger u.v.m.

Die erfassten Dienste haben demnach Bestands- und Nutzungsdaten an Sicherheitsbehörden, aber auch die Zollverwaltung und an für die Verfolgung von Ordnungswidrigkeiten zuständige Stellen unverzüglich und vollständig herauszugeben, sofern diesen die Erhebung der Daten gesetzlich gestattet ist.

Rechtsgrundlagen für die Erhebung werden für die Strafverfolgungsbehörden in den neuen §§ 100 g und j StPO bzw. für das Bundeskriminalamt in § 10 Abs. 1 S. 2 BKAG n.F. geschaffen.

1. Tiefe der Eingriffe in die informationelle Selbstbestimmung und Kreis der erfassten Dienste

Der weite Kreis der Herausgabepflichtigen führt dazu, dass personenbezogene Daten betroffen sind, die eine Vielzahl von Detailinformationen über die persönliche Lebensführung, auch über den Kernbereich persönlicher Lebensführung, umfassen. In der Folge sind Eingriffe in die informationelle Selbstbestimmung von besonderer Tiefe bis hin zum Kernbereich privater Lebensführung zu erwarten, für den keine Schutzvorkehrungen vorgesehen sind. Diese Befugnis ist, vor allem, da sie für die Verfolgung sämtlicher Straftatbestände vorgesehen und nicht etwa auf schwere Delikte – etwa Verbrechen - beschränkt ist, unverhältnismäßig. Besonders irritiert, dass von der datenschutzrechtlichen Befugnisnorm auch die potenzielle Herausgabe an Zoll- und Ordnungsbehörden erfasst ist.

Da nicht nur nach dem NetzDG verpflichtete soziale Medien betroffen sind, geht die Regelung weit über Auskunftspflichten, die zur effektiven Strafverfolgung von Hasskriminalität auf diesen Diensten erforderlich wären, etwa um die Autorin oder den Autor eines dort veröffentlichten Inhalts festzustellen, hinaus.

2. Die Pflicht zur Herausgabe von Passwörtern

Die Bestimmung in § 15a TMG n.F. umfasst dem Wortlaut nach eine Pflicht zu Herausgabe von Passwörtern.

Zum einen ist nicht ersichtlich, welchen legitimen Nutzen die Herausgabe von Passwörtern für die Strafverfolgungsbehörden haben kann. Sofern bestimmte Informationen, die auf einem Account gespeichert sein könnten, von Interesse für die Strafverfolgung sind, können diese herausverlangt werden. Ob der Erhalt von Passwörtern etwa zum verdeckten Weiterbetrieb eines Accounts durch Behörden führen soll, für den keine Rechtsgrundlage ersichtlich ist, oder zum Ausprobieren für andere Accounts der betreffenden Person – solche denkbaren Verwendungen der Passwörter wären verfassungswidrig.

Passwörter dürfen nach der DSGVO nicht im Klartext gespeichert werden, um Integrität und Vertraulichkeit zu gewährleisten. Gespeichert sind demnach bei Anbietern, die ihre datenschutzrechtlichen Pflichten einhalten, in der Regel Hashwerte von Passwörtern, mittels derer ermittelt werden kann, ob ein eingegebenes Passwort richtig ist, die jedoch nicht auf das Passwort als solches zurückgerechnet werden können. Deshalb stellt sich auch die Frage der Vereinbarkeit der vorgeschlagenen Regelung mit europäischem Datenschutzrecht.

Meldepflicht für Diensteanbieter nach dem NetzDG

Die vom NetzDG erfassten Anbieter sollen nach § 3a NetzDG n.F. verpflichtet werden, dem BKA sämtliche Inhalte zu übermitteln, die ihnen in einer Beschwerde über rechtswidrige Inhalte gemeldet worden sind, die er entfernt oder zu denen er den Zugang gesperrt hat und bei denen konkrete Anhaltspunkte dafür bestehen, dass sie mindestens einen der Tatbestände der §§ 86, 86a, 89a, 91, 126, 129 bis 129b, 130, 131 oder 140 StGB erfüllen und nicht gerechtfertigt sind. Neben dem Inhalt sollen auch die IP-Adresse sowie die Portnummer, die die nutzende Person beim Teilen des Inhalts verwendet hat, übermittelt werden.

1. Die pauschale Weiterleitung von IP-Adressen und Portnummern hat enorme Streubreite und kann nicht gerechtfertigt werden.

Bei der Herausgabe von IP-Adressen und Portnummern handelt es sich um einen Eingriff in die informationelle Selbstbestimmung, die das Grundgesetz in Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 schützt. Ohne Prüfung eines Verdachts durch die zuständigen Strafverfolgungsbehörden handelt es sich aufgrund der zu erwartenden Masse der Meldungen und Datenübertragungen um einen Eingriff von extrem großer Streubreite. Solange nicht geprüft wurde, ob ein solcher Verdacht besteht, kann ein solcher Eingriff nicht durch ein überwiegendes Allgemeininteresse gerechtfertigt werden. Diese Prüfung kann nicht auf Private übertragen werden, sondern sollte – angesichts der juristischen Komplexität insbesondere von Äußerungsdelikten – von der Staatsanwaltschaft durchgeführt werden.

2. Mit der Meldepflicht würde den Diensteanbietern eine bestimmende Rolle bei der essentiell staatlichen Aufgabe der Strafverfolgung zugeschrieben.

Die strafrechtliche Prüfung von Inhalten durch die Diensteanbieter würde zu einem Filter für all jene Sachverhalte, die der Strafverfolgung zugeführt werden. Im Ergebnis käme damit privaten Unternehmen und ihren internen Richtlinien eine eindrucksvolle Machtposition bei der Auswahl zu verfolgender Inhalte zu, der sie nicht gerecht werden können.

Die drohende Bußgeldverpflichtung setzt einen Anreiz dafür, im Zweifel eher Anhaltspunkte für das Vorliegen einer Straftat anzunehmen und einen Inhalt zu melden.

3. Es sind nicht nur Volksverhetzungen und Morddrohungen von der Meldepflicht erfasst, sondern eine Vielzahl von Delikten.

In der öffentlichen Kommunikation hat das BMJV bisher einen Schwerpunkt auf die Meldepflicht bei Morddrohungen und Volksverhetzungen gelegt. Betroffen ist nunmehr eine Auflistung von 13 Delikten, die auch deutlich weniger gravierende Vergehen umfasst, etwa die Störung des öffentlichen Friedens durch Androhung eines Brandstiftungsdelikts (§ 126 Absatz 1 Nr. 6 StGB). Auch die Einbeziehung von § 129 StGB (Bildung krimineller Vereinigungen) ist eine Strafnorm mit hohem Missbrauchspotenzial, wie das im letzten Jahr eingeleitete Verfahren gegen das Zentrum für politische Schönheit zeigt.

4. Die Meldepflicht ist nicht zweckmäßig zur besseren Strafverfolgung.

Bereits jetzt wird eine Vielzahl der Strafanzeigen im avisierten Deliktsbereich mangels dafür ausgebildetem Personal in den Behörden nicht oder nicht fachgerecht bearbeitet. Mit Einführung der geplanten Meldepflicht sind massenhafte Meldungen von Inhalten zu erwarten. Wie diese beim BKA bearbeitet werden sollen, bleibt unklar. Statt einer Fülle von Meldungen zu erzeugen, sollten die Staatsanwaltschaften mit hinreichend ausgebildetem und spezialisiertem Personal und entsprechenden Strukturen die schon jetzt gemeldeten Straftaten verfolgen.

5. Die extreme Rechte kann die Meldepflicht gegen ihre politischen Gegner strategisch verwenden.

Bisherige Erfahrungen mit der Sperr- und Löschpraxis sozialer Netzwerke deuten darauf hin, dass es Mechanismen gibt, die dazu führen, dass Beiträge, die von vielen Accounts gemeldet werden, bevorzugt gesperrt oder gelöscht werden. Es gibt Anzeichen dafür, dass diese Mechanismen bereits jetzt von rechten Trollarmeen strategisch genutzt werden, um die Löschung ihnen unliebsamer

Beiträge zu erreichen. Würden diese Mechanismen auf die Meldung von Beiträgen beim BKA übertragen, könnte es dort zu einer Häufung von Meldungen strafrechtlich irrelevanter Beiträge, die sich gegen Rechtsextremismus richten, samt IP-Adressen kommen. Das würde dem Ziel des Maßnahmenkatalogs diametral entgegenstehen und ist dringend zu vermeiden.

6. Schutzvorkehrungen betreffend die Verarbeitung sowie Löschvorschriften fehlen.

Der Entwurf trifft keine Vorkehrungen, die sicherstellen, dass die erlangten Daten beim BKA in einer mit den Anforderungen des Verfassungsrechts übereinstimmenden Weise behandelt werden. Insbesondere Kontrollmechanismen sind insofern nicht vorgesehen. Ohne klare Vorschriften betreffend die weitere Verarbeitung sowie klare Löschvorschriften fürchtet die Digitale Gesellschaft e.V. die Entstehung einer Sammlung der übermittelten Daten, die entgegen den Grundsätzen der Datensparsamkeit und Zweckbindung schlimmstenfalls zu einem späteren Zeitpunkt für andere Zwecke verwendet werden könnte.