



## STELLUNGNAHME

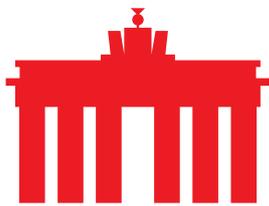
### **zum Referentenentwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität**

Berlin 17. Januar 2020

Am 18. Dezember 2019 hat das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) den Referentenentwurf eines „Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität“ veröffentlicht. Entgegen der bisherigen Diskussionen im politischen Raum zielt der vorliegende Entwurf nicht nur auf eine Stärkung des Netzwerkdurchsetzungsgesetzes (NetzDG) ab, sondern enthält darüber hinaus weitreichende Anpassungen und Neuregelungen im Strafgesetzbuch, in der Strafprozessordnung (StPO), im Telemediengesetz (TMG) und im Bundeskriminalamtgesetz. Die im Referentenentwurf enthaltenen Ausweitungen der geltenden Rechtsvorschriften gehen zum Teil mit tiefen Einschnitten 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 gem. Art. 10 GG für die Bürgerinnen und Bürger einher.

Nach Einschätzung von eco – Verband der Internetwirtschaft e.V. hat der vorliegende Entwurf insbesondere für Anbieter von Telemediendiensten tiefgreifende Folgen. Neben der Einführung einer Meldepflicht für die Betreiber sozialer Netzwerke im NetzDG sollen rechtliche Grundlagen für die Datenerhebung sowie Weitergabe im Telemediengesetz und Herausgabepflichten, u.a. zu Nutzerpasswörtern, für die Betreiber von Telemediendiensten geschaffen werden. Gleichzeitig werden die Befugnisse der Strafverfolgungs- und Sicherheitsbehörden erheblich ausgeweitet. Im Ergebnis bleibt festzuhalten, dass zentrale Aspekte des Gesetzesvorhabens erhebliche datenschutzrechtliche, verfassungsrechtliche und europarechtliche Fragen aufwerfen, die der kritischen Analyse bedürfen.

Insgesamt ist die Umsetzung des vorliegenden Gesetzesvorhabens als in höchstem Maße bedenklich einzustufen.



## I. Allgemeine Anmerkungen zum Gesetzesvorhaben

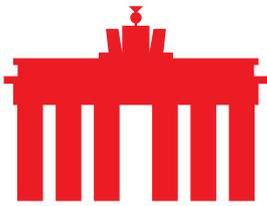
eco und die von ihm vertretenen Mitglieder begrüßen das politische Ziel der Bekämpfung von Rechtsextremismus und Hasskriminalität und unterstützen das Anliegen, gegen rechtswidrige Inhalte im Internet vorzugehen. Dazu betreibt eco u.a. eine Beschwerdestelle, deren Arbeit auf die Bekämpfung rechtswidriger Inhalte im Internet abzielt. Der vom BMJV veröffentlichte Entwurf erweckt jedoch den Eindruck übereilt und ohne angemessene Abwägung datenschutzrechtlicher und bürgerrechtlicher Konsequenzen verfasst worden zu sein. Die nachfolgende Analyse zeigt, dass aus den vorgeschlagenen Gesetzesänderungen starke Einschränkungen des Grundrechts auf informationelle Selbstbestimmung, des Grundrechts auf die Vertraulichkeit und Integrität von Kommunikationssystemen sowie des Fernmeldegeheimnisses resultieren. eco möchte in der Diskussion insbesondere auf die nachfolgend aufgeführten Punkte hinweisen, die von besonderer Brisanz sind und der eingehenden Betrachtung bzw. weiterer Beratungen bedürfen.

### ▪ **Auskunftspflichten für alle Betreiber von Telemediendiensten**

Der Gesetzentwurf sieht Auskunftsansprüche zu Informationen und Daten potenziell tatverdächtiger Nutzerinnen und Nutzer für die Strafverfolgungs- und Sicherheitsbehörden vor und schafft Regelungen für die Datenerhebung und Weitergabe von Bestands- und Nutzungsdaten für Telemediendiensteanbieter. Dabei werden in ganz erheblichem Umfang personenbezogene Daten wie z.B. Kommunikationsinhalte und Informationen zum Nutzungsverhalten von Nutzern herausgegeben. Dies ist grundsätzlich kritisch zu bewerten. Denn damit sind tiefgreifende Einschnitte in bürgerliche Freiheitsrechte, den Datenschutz und das Fernmeldegeheimnis verbunden.

### ▪ **Herausgabe von Passwörtern**

Auf Grundlage eines neu zu schaffenden § 15a im TMG sollen die Betreiber von Telemediendiensten insbesondere auch zur Herausgabe von Bestands- und Nutzungsdaten verpflichtet werden, die den Zugriff auf die Online-Identität der Nutzerinnen und Nutzer zulassen. Von dieser Regelung wären alle Sicherungssysteme für ganze Nutzerkonten betroffen, wie bspw. Passwörter. Unabhängig davon, dass i.d.R. solche Passwörter serverseitig verschlüsselt gespeichert werden und damit in der praktischen Verwendung ohne Ermittlungswert sind, ist ein derartiger Eingriff in die digitale Privatsphäre der Nutzerinnen und Nutzer unter Berücksichtigung von Verhältnismäßigkeit und technischer Umsetzbarkeit in höchstem Maß bedenklich.



- **Erfüllungsaufwand für Betreiber von Telemediendiensten**

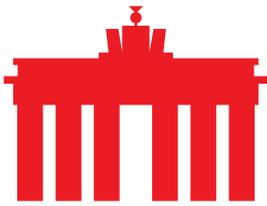
Die im Referentenentwurf aufgeführten Auskunfts- und Informationspflichten zu Bestands- und Nutzungsdaten ziehen nicht nur einen hohen administrativen Aufwand für die Betreiber von Telemediendiensten nach sich. Zur Umsetzung der Auskunftsansprüche müssen die Betreiber von Telemediendiensten neue technische und organisatorische Anforderungen erfüllen und die Voraussetzungen hierfür schaffen sowie speziell für diese Zwecke Fachkräfte bereitstellen. Zudem werden Telemediendienste ab 100.000 Kunden zur Einrichtung einer Schnittstelle verpflichtet (vgl. § 15a-neu Abs. 5 TMG). Aufgrund der breiten Betroffenheit bei den Betreibern von Telemediendiensten sind Gesamtkosten in Milliardenhöhe (siehe Anlage) zu erwarten.

- **Einführung einer Meldepflicht für Betreiber sozialer Netzwerke**

Auf Basis einer Meldepflicht im NetzDG sollen rechtsextreme und hasserfüllte Inhalte, die gleichzeitig als rechtswidrig einzustufen sind, im Internet eingeschränkt und die Täter gezielt verfolgt werden. Dazu sollen u.a. die IP-Adresse sowie Portnummer des betreffenden Nutzers über eine Schnittstelle an das Bundeskriminalamt (BKA) gemeldet werden. Diese Maßnahme ist vom Verfahren her zu kritisieren, da sensible Nutzerdaten ohne rechtsstaatliche Kontrolle, wie z.B. einen Richtervorbehalt, durch die Betreiber sozialer Netzwerke herauszugeben sind.

- **Datenübermittlung und Datenspeicherung beim BKA**

Durch die Meldepflicht wird binnen kürzester Zeit eine umfangreiche Datenbank zu gemeldeten Inhalten und Nutzerinnen bzw. Nutzern beim BKA entstehen. Der Referentenentwurf lässt offen, wie die Verarbeitung, Speicherung und Löschung der Daten beim BKA geregelt sein sollen. Weiter ist zu bedenken, dass die Meldepflicht und Datenübermittlung ohne Überprüfung eines konkreten Anfangsverdacht zu einer Straftat durch die jeweils zuständigen Behörden (z.B. eine Staatsanwaltschaft) erfolgen soll. Um einen rechtssicheren Datenumgang zu gewährleisten, müssen die Anforderungen an das Datenhandling zwingend vorab gesetzlich normiert werden.



### ▪ **Mangelnde rechtstaatliche Kontrolle**

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, 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.

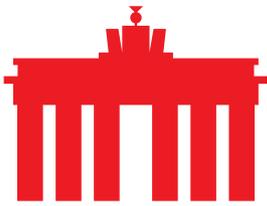
## **II. Bewertung des Gesetzesentwurfes**

### ▪ **Änderungen in der Strafprozessordnung**

Um rechtsextremistische und hasserfüllte Inhalte im Internet effektiv verfolgen und bestrafen zu können, sieht der Gesetzesentwurf Ausweitungen bzw. Ergänzungen der Rechtsvorschriften zur Herausgabe von Passwörtern, Bestands- und Nutzungsdaten, u.a. §§ 14-neu, 15, 15a-neu TMG sowie §§ 100g-neu und 100j-neu StPO zugunsten der zuständigen Stellen vor.

Auf Grundlage der §§ 100j-neu und 100g-neu StPO i.V.m. §§ 14-neu, 15 sowie 15a-neu TMG wird eine umfangreiche Rechtsgrundlage zur Identifizierung von Nutzerinnen und Nutzern für Ermittlungs- und Strafverfolgungsbehörden geschaffen. Die vorgeschlagenen Maßnahmen gehen damit weit über den Wirkungsbereich des NetzDG hinaus. Die Änderungen der §§ 100j-neu und 100g-neu StPO i.V.m. §§ 14-neu, 15-neu und §15a-neu TMG sind insgesamt kritisch zu bewerten. Eine Ausweitung der bestehenden Auskunftspflichten auf die Betreiber von Telemediendiensten wird auf Basis der im Referentenentwurf aufgeführten Ausgestaltung zu einer sehr breiten Betroffenheit bei den Betreibern von Telemediendiensten führen.

Hinsichtlich der Auskunft von Bestandsdaten bei Betreibern von Telemediendiensten gem. § 100j-neu Abs. 1 S. 1 StPO sind weitere Differenzierungen aus Sicht des eco zwingend erforderlich. Es ist nicht sachgerecht, eine Norm für die Betreiber von Telemediendiensten schlicht dem Telekommunikationsgesetz (TKG) nachgebildet zu schaffen. 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 ca. 2,3 Millionen Unternehmen als geschäftsmäßige Anbieter von Telemedien von diesen Regelungen potentiell betroffen sind (siehe Anlage). Zudem sollte bei Telemediendiensten beachtet werden, dass deren Anwendungen, im Gegensatz zu Telekommunikationsanbietern, auf einer heterogenen technischen Landschaft basieren und darüber hinaus auch unterschiedliche Formen von Informationen verarbeiten. Vor diesem Hintergrund erscheint 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 hinsichtlich ihres technischen Aufbaus, nicht zu weit greift.

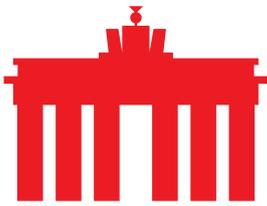
Gemäß den hier vorgenommenen Änderungen der Rechtsgrundlage soll jede Ermittlungsbehörde im Sinne der StPO Auskünfte von den Betreibern von Telemediendiensten verlangen dürfen. Ein unabhängiger und rechtsstaatlicher Sicherungs- bzw. Kontrollmechanismus ist an dieser Stelle im Entwurf nicht vorgesehen. Dabei entschied der Europäische Gerichtshof für Menschenrechte in der Sache Benedik gg. Slowenien, Az. 62357/14 im Juli 2018, dass eine Bestandsdatenauskunft, welche sich auf eine dynamische IP-Adresse bezieht, ohne unabhängige Kontrolle, wie eine gerichtliche Anordnung, gegen Art. 8 der Europäische Menschenrechtskonvention verstößt.<sup>1</sup>

Gänzlich unberücksichtigt bleibt im vorliegenden Referentenentwurf, dass neben den Regelungen der Strafprozessordnung eine Vielzahl bundes- und landesgesetzlicher Vorschriften eine Ermächtigungsgrundlage für die Abfrage von Bestandsdaten enthalten. Insbesondere ist hier auf die Landespolizeigesetze hinzuweisen – die ebenfalls auf § 14 TMG verweisen. In vielen dieser Gesetze werden das TKG und das TMG systematisch noch sehr unterschiedlich behandelt. Prozedurale Sicherungen gerade für besonders sensible Bestandsdaten wie Zugriffskennungen bzw. Passwörter sind in den meisten dieser Gesetze gerade nur für den Bestandsdatenbegriff des TKG vorgesehen. Für den Bereich der Telemediendienste besteht keine vergleichbare Differenzierung.

Für die Bestandsdatenabfragen an Telemedienanbieter wird hingegen vielfach noch auf die jeweiligen Generalklauseln der Gesetze zurückgegriffen. Der Entwurf problematisiert diese gängige Behördenpraxis bezeichnenderweise für die Ermittlungsgeneralklausel in §§ 161, 163 StPO, nicht aber für

---

<sup>1</sup> Vgl. EGMR, Application no. 62357/14 (Benedik vs. Slovenia) <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-182455%22%5D%7D> (zuletzt besucht am 17.12.2019)



andere Regelungen oder andere Bundesgesetze, auf welche die in § 15a-neu Abs. 3 TMG genannten Stellen regelmäßig zurückgreifen.

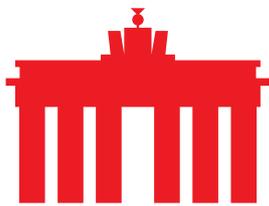
#### ▪ **Änderungen im Telemediengesetz**

Zentraler Baustein des Gesetzesentwurfs zur Bekämpfung von Rechtsextremismus und Hasskriminalität im Internet ist die Einführung eines § 15a-neu in das TMG. Dieser soll die Herausgabepflichten von Bestands- und Nutzungsdaten für die Betreiber von Telemediendiensten regeln. Nach dem Willen des Gesetzgebers erstreckt sich die Herausgabepflicht auch auf solche Daten, mit deren Hilfe auf Endgeräte oder Speicher zugegriffen werden kann, also auf Passwörter. Zur Bereitstellung der Informationen sollen sämtliche unternehmensinternen Daten herangezogen werden.

eco kritisiert den Entwurf des BMJV für einen § 15a-neu TMG scharf. Der Vorschlag greift tief in die Nutzerrechte und die Privatsphäre von Nutzerinnen und Nutzern ein, er belastet die Betreiber von Telemediendiensten und gefährdet möglicherweise die Sicherheit von IT-Systemen.

Nach Ansicht des eco sind die Auskunftspflichten nach § 15a-neu TMG unverhältnismäßig im Sinne von Art. 16 i. V. m. Art. 52 EU-Grundrechte-Charta. Die Delikte, deren Bekämpfung der Entwurf beabsichtigt, betreffen einige Nutzer einer geringen Anzahl von Telemedienanbieter. Indes sollen alle Anbieter von Telemediendiensten zu Auskünften verpflichtet werden. Der im Entwurf vorgesehene, zahlenmäßig uferlose Adressatenkreis der Auskunftspflichten steht nur in geringem Ausmaß im Zusammenhang mit den angesprochenen Delikten und ist somit nicht auf das absolut Notwendige zu deren Bekämpfung begrenzt.

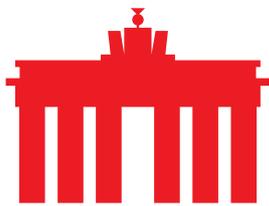
Die Herausgabe von unverschlüsselten Passwörtern ermöglicht den Ermittlungs- und Strafverfolgungsbehörden den Zugriff auf Online-Konten und damit auf die Online-Identität von Nutzerinnen und Nutzern. Mit diesen Daten werden umfangreiche Onlinedurchsuchungen ermöglicht, einschließlich des Zugriffs auf Kommunikationsinhalte wie E-Mails, in der Cloud hinterlegte Fotos, Dokumente, Chat- und Messengernachrichten. Im Ergebnis erfolgt auf dieser Grundlage ein Eingriff und somit auch eine Einschränkung des Kernbereiches der privaten Lebensgestaltung von Nutzerinnen und Nutzern. Dieser Eingriff betrifft nicht nur den angefragten Nutzer, sondern bei mehrseitiger Kommunikation auch außenstehende Personen, die in aller Regel keinen Anlass für die Datenherausgabe gegeben haben. Deshalb ist die Verhältnismäßigkeit der Herausgabe solch sensibler Daten grundsätzlich fragwürdig und sollte, wenn sie überhaupt statthaft ist, sehr strengen Auflagen und



bspw. auf Basis eines klar definierten Katalogs schwerer Straftaten unterworfen sein. Der § 15a-neu TMG nimmt aber eine entsprechende Einschränkung nicht vor, sondern führt eine ganze Reihe an Behörden und Stellen an, die befugt sind, entsprechende Anfragen zu stellen.

Weiterhin gilt es zu bedenken, dass die Herausgabe von Informationen, mit deren Hilfe auf Speicher des Telemedienanbieters sowie auf Speicher und Endgeräte der Nutzer zugegriffen werden kann, auch ein sicherheitskritisches Problem für die Betreiber von Telemediendiensten darstellt. So dürfen Passwörter aus Sicherheitsgründen u.a. wegen des Datenschutzes nur verschlüsselt gespeichert werden, sodass diese nicht unmittelbar für den Anbieter einsehbar sind. Der vorliegende Referentenentwurf lässt jedoch offen, inwieweit eine Verpflichtung für die Betreiber von Telemediendiensten, wie z.B. E-Mailprovider, Social-Media-Plattformen und Internetforen, abgeleitet werden kann, Passwörter im Klartext zu speichern oder das Verschlüsselungsverfahren für die Passwörter gegenüber den anfragenden Behörden offenzulegen, indem sie dazu verpflichtet werden, entsprechende Informationen unter Bereitstellung aller unternehmensinternen Datenquellen zu berücksichtigen. Aus Gründen der IT-Sicherheit und des Datenschutzes sowie des Grundrechts auf Vertraulichkeit der Kommunikation wären beide Schritte fatal. In diesem Kontext bedarf es weiterer Diskussionen, ob die Betreiber von Telemediendiensten grundsätzlich imstande wären, entsprechende Auflagen zur Offenbarung von Verfahren und Passwörtern zu erfüllen und ob solche Anforderungen Grundrechtskonform wären. Insbesondere bei kleinen Anbietern, die nicht mit eigenen technischen Entwicklungen arbeiten, dürfte dies nicht der Fall sein. Eine Mitwirkungspflicht für Betreiber von Telemediendiensten bei der Entschlüsselung von Passwörtern bzw. der Bereitstellung von Informationen zum Entschlüsseln oder Zurücksetzen von Passwörtern ist in jedem Fall entschieden abzulehnen.

Mit der im § 15a-neu TMG vorgeschriebenen Auskunftspflicht zu Bestands- und Nutzungsdaten geht ein enormer Aufwand für die Betreiber von Telemediendiensten einher. Dabei lässt der Referentenentwurf offen, ob den Diensteanbietern mögliche Mitwirkungspflichten bspw. bei der Identifizierung oder Zusammenführung von Daten obliegt. Zudem ist gemäß § 15a-neu Abs. 5 S. 3 TMG die Prüfung zur Rechtmäßigkeit einer Anfrage beim jeweiligen Diensteanbieter durch entsprechendes Fachpersonal durchzuführen. Gerade für kleine und mittelständische Betreiber von Telemediendiensten stellt der damit verbundene technische, organisatorische und personelle Erfüllungsaufwand eine enorme finanzielle Belastung dar. Grundsätzlich sollte der Erfüllungsaufwand nicht zulasten der Unternehmen gehen.

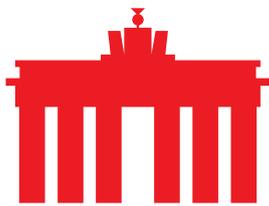


Darüber hinaus sieht § 15a-neu Abs. 5 S. 2 TMG vor, dass geschäftsmäßig tätige Telemediendienste, die mehr als 100.000 Kunden haben, zur Einrichtung einer elektronischen Schnittstelle verpflichtet werden, um die Auskunftersuchen der berechtigten Stellen entgegennehmen und beantworten zu können. Die technische Umsetzung und mögliche Maßgaben für den Einsatz einer solchen Schnittstelle lässt der Referentenentwurf unklar.

Das Angebot an Telemediendiensten in Deutschland ist sehr vielseitig, so dass sich die Frage stellt, inwieweit die Daten in Abweichung von den bekannten Abfrageformen des TKG für die Bereitstellung aufbereitet und standardisiert sein müssen bzw. sein können. Die Anforderungen und die individuellen Kosten zur Bereitstellung der Schnittstelle werden sich je nach Dienst und der eingesetzten Technologie sowie durch möglicherweise unterschiedliche Anforderungen an die einzelnen Dienste im Rahmen der unterschiedlichen Auskunftspflichten erheblich voneinander unterscheiden. Diese Unklarheiten erschweren zum aktuellen Zeitpunkt eine konkrete Bezifferung des Erfüllungsaufwandes, jedoch werden die zu erwartenden Investitionskosten aufgrund der äußerst hohen Zahl der betroffenen Unternehmen, die Telemediendienste anbieten, unter Berücksichtigung der bestehenden Datenschutzvorschriften und einer angenommenen Komplexität der technischen Maßgaben analog zu den Verfahren nach § 110 TKG in einem mittleren zweistelligen Milliardenbereich liegen sowie jährliche Betriebskosten im einstelligen Milliardenbereich bei den betroffenen Unternehmen entstehen. Der Aufwand, der mit dem Aufbau und Betrieb einer entsprechenden Schnittstelle verbunden ist, stellt aber nicht nur die Anbieter von Telemediendiensten vor enorme organisatorische und finanzielle Herausforderungen, sondern auch die berechtigten Stellen.

Zugleich ist die Bemessungsgrundlage von 100.000 Kunden zur Errichtung einer Schnittstelle für die Telemedienanbieter kein geeignetes Kriterium. Die Aufgreifschwelle ist schon deshalb problematisch, weil selbst kleine Online-Dienste und Plattformen große Reichweiten erzielen können und dementsprechend hohe Kundenzahlen aufweisen, welche regelmäßig die Zahl von 100.000 deutlich übersteigen. Aufgrund der Heterogenität der Dienste kann das Abstellen auf die Kundenzahl eines Dienstes keine vernünftige Bemessungsgrundlage darstellen.

Im Ergebnis würde das Gesetzesvorhaben bedeuten, dass aus den Anforderungen des TKG (§ 113 Abs. 5 TKG i.V.m. § 110 TKG) abgeleitet, im Gegensatz zu den bisher knapp 300 Teilnehmern des automatisierten Auskunftsverfahrens über eine Schnittstelle nunmehr geschätzt zumindest rund 25.000 Unternehmen sowie anstatt der bisher 6.500 Unternehmen rund 2,3 Millio-



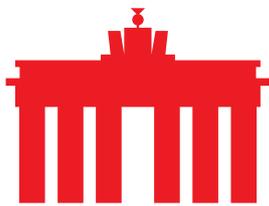
nen Unternehmen zu einer Auskunft im manuellen Auskunftsverfahren verpflichtet wären. Etwaige Rechtsvorschriften zur Erstattung der damit einhergehenden Kosten oder Entschädigungsregelungen zugunsten der Betreiber von Telemediendiensten sind nicht vorgesehen.

#### ▪ **Änderungen im Netzwerkdurchsetzungsgesetz**

Die Überarbeitung des NetzDG ist ein weiterer Punkt des Gesetzes gegen Rechtsextremismus und Hasskriminalität, der auch Gegenstand der öffentlichen Debatte ist. Das Gesetz soll durch die Einführung einer Meldepflicht für die Betreiber sozialer Netzwerke ein effizientes Vorgehen gegen Rechtsextremismus und Hass ermöglichen. Auf Grundlage dieser Meldepflicht nach § 3a-neu NetzDG werden die Betreiber sozialer Netzwerke dazu verpflichtet, zuvor von Nutzern gemeldete und als potenziell rechtswidrig eingestufte Inhalte, an eine zentrale Stelle beim Bundeskriminalamt (BKA) zu melden. Die Einführung einer Meldepflicht für die Betreiber sozialer Netzwerke gem. § 3 a-neu NetzDG ist aus folgenden Gründen kritisch zu bewerten.

#### Beschwerdeprüfung und Umgang mit Falschmeldungen

Der bestehende Rechtsrahmen sieht vor, dass den Betreibern sozialer Netzwerke nach § 3 Abs. 2 Nr. 1 NetzDG die Pflicht zur Überprüfung der eingehenden Beschwerden obliegt. Aus Sicht der betroffenen Unternehmen gilt es vor dem Inkrafttreten einer Meldepflicht zu klären, inwieweit die vorgenommene Inhaltsprüfung durch die Betreiber der Dokumentation bedürfen bzw. ob diese Vorabprüfung im Rahmen der Meldepflicht z.B. unter § 3 a-neu Abs. 2 NetzDG offengelegt werden muss. In diesem Zusammenhang bedarf es darüber hinaus einer Diskussion, wie mit möglichen „Falschmeldungen“ umgegangen wird. Eine Haftungsprivilegierung bei „Falschmeldungen“ ähnlich wie z.B. im Geldwäschegesetz ist nicht vorgesehen. Aus Sicht der Betreiber sozialer Netzwerke können im Kontext zum NetzDG unter dem Begriff der „Falschmeldung“ eine Fehleinschätzung bzw. –interpretation über den zu meldenden Inhalt allgemein oder eine zu enge Auslegung der zugrunde gelegten Rechtsnorm verstanden werden. Folglich bestehen rechtliche Fragestellungen bei den Betreibern sozialer Netzwerke, die im Vorfeld der Klarstellung bedürfen. eco hält es für dringend erforderlich, dass die drohenden Rechtsunsicherheiten, die aus der Einführung einer Meldepflicht resultieren, vor deren konkreter Umsetzung zur Klärung kommen.



### Präzisierung des Beschwerdebegriffs

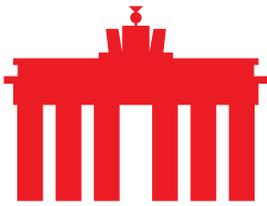
Voraussetzung für eine Meldung an das BKA ist gem. § 3a-neu Abs. 2 Nr. 1 NetzDG u.a. eine Beschwerde gegenüber dem Anbieter. Jedoch lässt der Referentenentwurf offen, von wem die Beschwerde eingereicht worden sein muss, auch wenn zahlreiche Passagen der Begründung darauf hindeuten, dass letztlich Nutzerbeschwerden gemeint sein dürften.

eco spricht sich dafür aus, an dieser Stelle die erforderliche Klarheit zu schaffen und für eine entsprechende Nachbesserung im Entwurf des Gesetztextes zu sorgen. Die Ergänzung sollte klarstellen, dass Nutzerbeschwerden gemeint sind. Letztlich wird das Risiko, dass derselbe Inhalt mehrfache an das BKA gemeldet wird (durch den Betreiber sozialer Netzwerke und beteiligte Beschwerdestellen), deutlich reduziert. Die Erfahrung der eco Beschwerdestelle zeigt, dass nicht selten auch Beschwerdestellen entsprechende Beschwerden an die Betreiber sozialer Netzwerke richten. Jedoch erstatten die Beschwerdestellen bei strafbaren Inhalten in diesen Fällen ihrerseits Anzeige.

### Klarstellung des Anwendungsbereiches für die Meldepflicht

Positiv ist anzumerken, dass auf Basis von § 3a-neu Abs. 2 Nr. 3 NetzDG Klarheit darüber geschaffen wird, dass die Meldepflicht nicht für alle unter § 1 Abs. 3 NetzDG genannten Straftatbestände gilt und Antragsdelikte, die jeweils nur selbst von den Geschädigten zur Anzeige gebracht werden können, ausgeschlossen sind. Jedoch bestehen zahlreiche technische und rechtliche Unklarheiten in Bezug auf die Meldepflicht für die Betreiber sozialer Netzwerke.

Eine erste Evaluation des § 3a-neu Abs. 2 Nr. 3 NetzDG zeigt, dass auch kinderpornographische bzw. Kindesmissbrauchsinhalte der Meldepflicht durch die Betreiber sozialer Netzwerke unterliegen sollen. Aus dem Betrieb der Beschwerdestelle beim eco ist anzumerken, dass zur Eindämmung von Kindesmissbrauchsinhalten bereits eine zentrale Stelle beim BKA existiert. Um eine effektive Eindämmung eben solcher Inhalte nach der Einführung einer Meldepflicht sicherzustellen und mögliche Doppelmeldungen beim BKA sowie den Diensteanbietern zu vermeiden, sollten die Zuständigkeiten innerhalb der Ermittlungsbehörde frühzeitig geklärt werden. Zudem sollte eine Meldepflicht für entsprechende Inhalte 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. Bei der Ausgestaltung der Meldepflicht im NetzDG ist



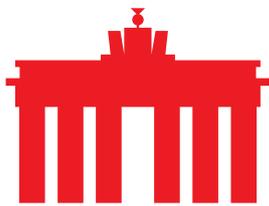
darauf zu achten, dass künftig keine Doppelmeldungen auftreten und daraus resultierende Doppelarbeit bei den Betreibern und den Strafverfolgungsbehörden entstehen.

#### Datenübermittlung im Zuge der Meldepflicht

Gemäß § 3a-neu Abs. 4 NetzDG muss die Meldung des Betreibers eines sozialen Netzwerkes an das BKA die IP-Adresse und die Portnummer (sofern vorhanden) des veröffentlichenden Nutzers enthalten. eco bewertet diesen Vorstoß, dass bereits durch die Meldung an das BKA die vorstehenden Informationen zugänglich gemacht werden sollen, als bedenklich. Weiterhin ist kritisch anzumerken, dass die Herausgabe der Daten in diesen Fällen ohne die Überprüfung eines konkreten Anfangsverdacht durch die jeweils zuständigen Behörden (z.B. Staatsanwaltschaft) erfolgt. In der Vergangenheit waren die Herausgabe bzw. der Zugang zu solch sensiblen Daten der Nutzerinnen und Nutzer an rechtsstaatliche Kontroll- und Sicherungsmechanismen, wie z.B. den Richtervorbehalt, geknüpft. Dass diese Schutzmechanismen in Anbetracht des vorliegenden Entwurfes entbehrlich sein sollen, kritisiert eco.

#### Umsetzung der Meldepflicht

Im Rahmen der Ausgestaltung der rechtlichen, technischen und organisatorischen Bedingungen des Meldeprozesses ist zu berücksichtigen, dass die Betreiber sozialer Netzwerke seit der Einführung des NetzDG große Anstrengungen und Investitionen zur Einrichtung des geforderten Beschwerdemanagements und dessen Optimierung aufgewendet haben. Die Unternehmen haben bereits Verfahren und Prozesse für die Strafverfolgungsbehörden etabliert, um Informationen abzufragen. Dies gilt insbesondere für im Inland ansässige Anbieter aber auch für Anbieter mit Sitz in einem anderen Land. Zur Beauskunftung stellen die Betreiber sozialer Netzwerke sog. law-enforcements Portale für die Auskunftserteilung und -abwicklung zur Verfügung, durch deren Einsatz die Behörden schnell, effektiv und verschlüsselt Daten abfragen können. Diese Portale haben sich bewährt und sollten 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 müssen jedoch Mindeststandard berücksichtigt werden, die für die Anfrage erfüllt sein müssen, um nicht im Heimatland der Betreiber für eine widerrechtliche Datenherausgabe in die Haftung genommen zu werden. Aus der nun angekündigten Ausweitung der Pflichten für die Betreiber sozialer Netzwerke werden weitere personelle und technische Investitionen erwachsen. Damit der Meldeprozess



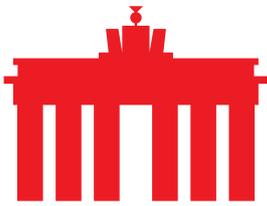
im Rahmen der rechtlich vorgesehenen Frist umgesetzt werden kann, müssen die Betreiber weiteres Personal vorhalten. Zur technischen Umsetzung der Meldepflicht soll eine durch das BKA definierte Schnittstelle zwischen den Betreibern sozialer Netzwerke und dem BKA geschaffen werden. Die finanziellen Verpflichtungen beider Maßnahmen obliegen ausschließlich den Betreibern sozialer Netzwerke.

Mit der im Referentenentwurf vorgeschlagenen Meldepflicht in Kombination mit der Weitergabe und Ausleitung über eine einzurichtende Schnittstelle an das BKA werden die Anbieter von sozialen Medien, also private Unternehmen, zum Erfüllungsgehilfen von Strafverfolgungsbehörden für Maßnahmen, die erhebliche Einschränkungen von Grundrechten zur Folge haben. Die Verfolgung von Straftaten zählt zu den ureigenen hoheitlichen Aufgaben des Staates und somit erscheint die Einbindung privater Anbieter in staatliche Aufgaben verfassungsrechtlich bedenklich. Insbesondere die Regelung zur Meldepflicht sowie deren Ausgestaltung u.a. durch einzurichtende elektronische Schnittstellen, der Ausleitung von IP-Adressen und Portnummern ist als systemfremd einzustufen

Insgesamt ist bei der Einführung und Diskussion von Meldepflichten darauf zu achten, dass sich deren Normierung nicht mit europäischer Gesetzgebung überschneidet oder mit dieser in Widerspruch gerät. Ein nationaler Alleingang Deutschlands ist angesichts der auf europäischer Ebene geführten Diskussionen nicht hilfreich. Entsprechende Doppelregulierungen könnten für die Betreiber sozialer Netzwerke problematisch werden.

#### Umgang mit Datensätzen aus der Meldepflicht

Grundsätzlich wird auf Grundlage der Meldepflicht im NetzDG binnen kurzer Zeit eine umfangreiche Datenbank über gemeldete Inhalte und als tatverdächtig geltende Nutzerinnen und Nutzer sozialer Netzwerke beim BKA entstehen. Aus Sicht des eco ist es als bedenklich einzustufen, dass der Referentenentwurf keine Vorgaben zum weiteren Umgang mit den von den sozialen Netzwerken übermittelten Daten in Bezug auf deren Verarbeitung, Speicherung und Löschung durch das BKA enthält. Aus der aktuell unklaren Rechtslage erwächst ein enormes Risiko über den Umgang mit den massenhaft auflaufenden Datensätzen und darüber hinaus über die Befugnisse der Ermittlungsbehörden. Ebenso bleibt unklar, wie die aus der Meldepflicht erlangten Datensätze für weitere Ermittlungen verwendet und zur Klärung anderer Delikte herangezogen werden dürfen. Vor diesem Hintergrund ist es zwingend erforderlich, dass die Anforderungen an den Datenumgang und



insbesondere an das Löschen der Datensätze durch das BKA vor der Einführung der Meldepflicht im NetzDG umfassend und abschließend gesetzlich normiert werden.

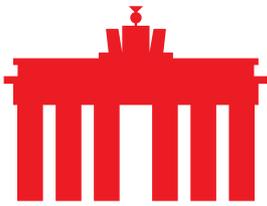
Grundsätzlich gilt es klarzustellen, dass eine Meldepflicht nur dann ein effektives und konsequentes Mittel im Kampf gegen Rechtsextremismus und Hasskriminalität sein kann, wenn die Ermittlungs- und Strafverfolgungsbehörden von Bund und Ländern mit den entsprechenden personellen und technischen Kapazitäten ausgestattet werden. Die grundsätzliche Notwendigkeit und die Dringlichkeit insbesondere des personellen Aus- und Aufbaus wird durch die Erfahrung der eco Beschwerdestelle bestätigt. Die Betreiber sozialer Netzwerke gehen zum gegenwärtigen Zeitpunkt davon aus, dass, sofern die Meldepflicht für alle eingehenden Beschwerden und nicht nur für Beschwerden gem. NetzDG gilt, Inhalte im Millionenbereich pro Jahr an das BKA zu melden sind. Schlussendlich ist eine effektive Ermittlung und Strafverfolgung im Zeitalter zunehmender Digitalisierung nur dann effektiv und zielführend möglich, wenn die jeweiligen bundes- und landespolitischen Akteure über die erforderlichen personellen und technischen Ausstattungen verfügen.

#### Unvereinbarkeit d. Meldepflicht mit EU-Recht

Nach Einschätzung des eco verstößt die vorgeschlagene Meldepflicht gem. § 3a-neu Abs. 4 Nr. 2 NetzDG bzgl. der Herausgabe von IP-Adresse und Portnummer gegen EU-Recht, insbesondere gegen die E-Commerce-Richtlinie (2000/31/EG). Deren Art. 15 Abs. 2, 2. Halbsatz gestattet den Mitgliedsstaaten Vorschriften zu erlassen, in denen zuständige Behörden auf Verlangen Informationen zur Nutzeridentifizierung erhalten können. § 3a-neu Abs. 4 Nr. 2 NetzDG konstituiert dem widersprechend eine Meldepflicht, ohne dass es ein Verlangen zur Ermittlung des Nutzers im Einzelfall der zuständigen Behörde, hier das BKA, gibt.

### **III. Fazit**

Der Gesetzentwurf des BMJV ist abzulehnen. Das Vorhaben ist datenschutzrechtlich, verfassungsrechtlich und europarechtlich in höchstem Maße bedenklich. Es ist mit tiefen Eingriffen in bürgerliche Freiheiten, die Vertraulichkeit und Integrität elektronischer Kommunikation und die Vertrauenswürdigkeit digitaler Dienste verbunden. Der Versuch, ähnlich gelagerte Regelungen



aus dem TKG auf Telemediendienste zu übertragen, zeugt von mangelnder Reflektion über die Tragweite und Auswirkungen.

Der Kreis der berechtigten Stellen ist deutlich zu weit gefasst, rechtsstaatlich gebotene Sicherungsmechanismen und -kontrollen – wie beispielsweise ein Richtervorbehalt und strenge Gefahr-im-Verzug-Befugnisse – sind nur unzureichend vorgesehen. Der Adressatenkreis der Regelungen – alle geschäftsmäßigen Erbringer von Telemediendiensten – ist zudem deutlich zu weit gefasst. Der Erfüllungsaufwand für die Wirtschaft für die geplanten Maßnahmen wird mit erheblichen einmaligen sowie laufenden finanziellen Belastungen für die verpflichteten Unternehmen in mehrstelliger Milliardenhöhe verbunden sein. Kostenerstattungs- oder Entschädigungsregelungen sind hingegen nicht vorgesehen.

Bedauerlicherweise erweckt der Gesetzentwurf den Eindruck, dass unter dem Rubrum der Bekämpfung von Hasskriminalität und Rechtsextremismus weitgehende Eingriffe – auch völlig unabhängig von den zuvor genannten Problemen – ermöglicht werden sollen. Es ist zu befürchten, dass hier – wie schon beim NetzDG im Jahr 2017 vorschnell gehandelt wird und die Bedenken von Wirtschaft und Zivilgesellschaft beiseite gewischt werden zu Lasten der politischen Debatte und der Meinungsfreiheit im Netz.

---

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