VERBAND DER INTERNETWIRTSCHAFT E.V.

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 Telemediengsetz (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 Stellungnahme[1] 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 Telemediendienstanbieter**

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 Telemediendienstanbietern 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 Telemediendienstanbieter gilt und

[1] Stellungnahme 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 Telemediendienstanbieter zu einer breiten Betroffenheit bei den Telemediendienstanbietern führen.

In Bezug auf die Beauskunftung von Bestandsdaten durch die Telemediendienstanbieter gem. § 100j Abs. 1 S. 1 StPO sind weitere Differenzierungen aus Sicht des eco unerlässlich. Es ist nicht sachgerecht, eine Norm für Telemediendienstanbieter 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 Telemediendienstanbieter**

Neben der Herausgabeverpflichtung von Bestands- und Nutzungsdaten durch die Telemediendienstanbieter sollen auf Grundlage von § 15b TMG auch Daten von Telemediendienstanbietern herausgegeben werden, mit deren Hilfe auf Endgeräte oder Speicher zugegriffen werden kann, also insbesondere Passwörter. Zur Bereitstellung der Informationen sollen Telemediendienstanbieter 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 Telemediendienstanbieter 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 Telemediendienstanbieter 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 Telemediendienstanbieter 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 Telemediendienstanbieter 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 Passwörtern 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 Telemediendienstanbieter 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 Dienstanbietern 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 Verlagen 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 Rechtgrundlage 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 Netzwerden und Plattformen beauskunften auf freiwilliger Basis die durch die Strafverfolgungsbehörden angefragten Daten ohne das 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 Gesetzgebungsverfahren 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

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