STELLUNGNAHME

Stellungnahme des Bundesverbands Digitale Wirtschaft e.V. zum Referentenentwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität

17. Januar 2020

Ansprechpartner:

Katharina Rieke
Referentin Digitalpolitik
T: +49 30 206 218 617
rieke@bvdw.org

Vorbemerkungen

Der Bundesverband Digitale Wirtschaft (BVDW) e.V. ist die Interessenvertretung für Unternehmen, die digitale Geschäftsmodelle betreiben oder deren Wertschöpfung auf dem Einsatz digitaler Technologien beruht. Als Impulsgeber, Wegweiser und Beschleuniger digitaler Geschäftsmodelle vertritt der BVDW die Interessen der digitalen Wirtschaft gegenüber Politik und Gesellschaft und setzt sich für die Schaffung von Markttransparenz und innovationsfreundlichen Rahmenbedingungen ein. Sein Netzwerk von Experten liefert mit Zahlen, Daten und Fakten Orientierung zu einem zentralen Zukunftsfeld.

Der Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) für ein Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität wurde an die Verbände zur Stellungnahme mit Frist zum 17. Januar 2020 versandt. Der BVDW bedankt sich für die Gelegenheit zur Stellungnahme und teilt nachfolgend seine Position.

1. Allgemeine Anmerkungen

Vor dem Hintergrund des furchtbaren Anschlags in Halle, „der Teil einer Reihe von besorgniserregenden Vorfällen in der jüngeren Vergangenheit ist", hat die Bundesregierung sich dazu entschlossen „sämtliche rechtsstaatlichen Mittel gegen Hass, Rechtsextremismus und Antisemitismus" einzusetzen und neue, umfangreichere Maßnahmen zur Bekämpfung von Hass und Hetze im Netz zu ergreifen.[1]
Das BMJV hat am 30. Oktober 2019 ein Maßnahmenpaket zur Bekämpfung von Rechtsextremismus und Hasskriminalität verabschiedet, das in einem ersten Schritt mit dem vorliegenden Referentenentwurf umgesetzt werden soll.[2]

Der Referentenentwurf schlägt Änderungen im Strafgesetzbuch (StGB), in der Strafprozessordnung (StPo), im Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKA-Gesetz), im Telemediengesetz (TMG) sowie im Netzwerkdurchsetzungsgesetz (NetzDG) vor.

Der BVDW stellt sich mit voller Kraft hinter das Ziel der Bekämpfung von Extremismus und Hasskriminalität und begrüßt somit die Auseinandersetzung der Bundesregierung mit der Thematik sowie die aktuelle Verbändekonsultation. Hass und Extremismus dürfen keinen Platz in unserer Gesellschaft haben. Der freie (politische)

[1] Referentenentwurf des BMJV für ein Gesetz zur Bekämpfung von Rechtsextremismus und Hasskriminalität
[2] Maßnahmenpaket des BMJV zu Rechtsextremismus und Hasskriminalität

Diskurs und somit das Recht auf freie Meinungsäußerung muss verteidigt werden. Eine effektive Strafverfolgung ist dafür von großer Bedeutung.

Gleichzeitig weist der BVDW aber auch darauf hin, dass das Ausmaß und die Konsequenzen der vorgeschlagenen Neuregelungen bedacht werden müssen. Nicht nur ist der vorliegende Referentenentwurf in seiner jetzigen Form aus datenschutzrechtlichen, rechtsstaatlichen und verfassungsrechtlichen Gesichtspunkten sehr bedenklich, sondern verfehlt unserer Auffassung nach auch zu großen Teilen sein Ziel.

Darüber hinaus ist ein nationaler Alleingang auch generell zu hinterfragen. Denn der Gesetzesentwurf behandelt Regulierungsaspekte, die aktuell intensiv innerhalb der EU diskutiert werden. Beispielsweise im Rahmen der Überlegungen zum E-Evidence Paket, aber auch im Rahmen des Digital Services Act, dessen Entwurf noch in diesem Jahr erwartet wird.

2. Im Einzelnen

2.1 § 15 a TMG (neu)

Alle Telemediendienste sind betroffen

Über die vorgeschlagenen Änderungen im TMG, in Verbindung mit den Änderungen in der StPo und im BKA-Gesetz, führt der Referentenentwurf bestehende Anforderungen aus dem Telekommunikationsgesetz (TKG) für alle Telemediendienste ein.

Der Entwurf des neuen § 15 a TMG vollzieht diese Erweiterung über die Einführung eines Auskunftsverfahrens. Liest man sich den Paragraphen durch, stellt man fest, dass hier das Verfahren des § 113 TKG nahezu wortgleich übernommen wurde. Das Verfahren, das bisher nur für Telekommunikationsanbieter gilt, wird nun auf alle Unternehmen erweitert, die „geschäftsmäßig Telemediendienste erbringen, daran mitwirken oder den Zugang zu Nutzung daran vermitteln". Das bedeutet, dass alle elektronischen Informations- und Kommunikationsdienste wie beispielsweise Online-Shops, Messenger und E-Mail-Dienste sowie Medienanbieter von der Änderung betroffen sind. Um die Auskunftspflicht des § 15 a zu erfüllen, müssen die Telemedienanbieter ihre, nach § 14 und § 15 TMG gesammelten, Bestandsdaten (Name, Anschrift, Kontodaten, Geburtsdatum etc.) und Nutzungsdaten (IP-Adresse, besuchte Seiten etc.) an die auskunftsersuchenden Behörden übermitteln und alle zur Verfügung stehenden Datenquellen dafür nutzen.

Auskunftsrecht über Bestands- und Nutzungsdaten für eine Großzahl von Behörden/keine Beschränkung der Straftatbestände

Auskunftsberechtigte Stellen sind, wie im TKG, die für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständigen Stellen sowie die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst. Neu hinzugefügt wurden sogar die Behörden der Zollverwaltung und die nach Landesrecht zuständigen Behörden für u.a. das Schwarzarbeitsbekämpfungsgesetz. Die Bestands- und Nutzungsdaten dürfen von all diesen Stellen, also beispielweise Polizeibehörden, bei den Telemedienanbietern

eingeholt werden, sofern sie diese Daten zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung, oder auch die Erfüllung ihrer gesetzlichen Aufgaben benötigen.

Dies ist eine Ausweitung der Befugnisse dessen Ausmaß in keinem Verhältnis zum gewünschten Ziel steht. Hier können Massen an personenbezogene Daten weitergeleitet werden, die einen tiefen Einblick in das persönliche Leben einer Person bieten, und das bereits für kleinere Delikte oder Ordnungswidrigkeiten. Zudem läuft der Richtervorbehalt an dieser Stelle weitgehend ins Leere.

Nach § 15 a Abs. 5 ist es zudem Aufgabe der Telemedienanbieter selbst über eine „verantwortliche Fachkraft" sicherzustellen, dass die Auskunftsverlangen der Behörden die formalen Voraussetzungen erfüllen und somit rechtmäßig sind. Alle Telemedienanbieter, die mehr als 100.000 Kunden haben, müssen zudem eine eigene gesicherte elektronische Schnittstelle für die Auskunftsverlange bereithalten. Dieses sachliche Kriterium der Kundenanzahl für die Anwendung des Gesetzes ist aus unserer Sicht sehr fragwürdig, denn für die tatsächliche Relevanz eines Angebots kommt es weniger auf die absolute Zahl der Kunden als auf seine Reichweite an. Hier werden zudem Anforderungen geschaffen, die gerade von klein- und mittelständischen Unternehmen kaum erfüllt werden können.

Auskunft über Passwörter

Neben der Auskunftspflicht für Bestands- und Nutzungsdaten schreibt § 15 a Abs. 1 Satz 2 auch vor, dass die Behörden Auskunft über Bestandsdaten verlangen können, mittels derer der Zugriff auf Endgeräte und Speichereinrichtungen geschützt wird. Dies bedeutet, dass auch ein Zugriff auf Passwörter für diese Stellen möglich ist. Eine Änderung im TMG, die aus datenschutzrechtlicher sowie verfassungsrechtlicher Sicht mehr als fragwürdigt ist.

Der Zugriff auf Passwörter ist zwar laut § 100j Abs. 1 Satz 2 (neu) StPo in Verbindung mit § 100j (3) StPo nur mit Richtervorbehalt möglich. Allerdings hat diese Auskunftsbefugnis, die bereits im TKG besteht, angewandt auf Telemediendienste, viel weitreichendere Konsequenzen in der Anzahl betroffener Unternehmen und dem Ausmaß des Einblicks in die Privatsphäre und des Lebens der betroffenen Person. Der Zugang zum Passwort liefert der Behörde den Zugang zum gesamten „Online-Leben" und wäre schlussendlich gleichzusetzen mit einer Online-Durchsuchung, die nur bei besonders schweren Straftatbeständen eingesetzt werden darf Dies hätte auch nicht nur Auswirkungen auf die Person selbst, sondern beträfe womöglich auch andere, ihr nahestehende Personen, wenn man beispielsweise an Passwörter zu Messenger-Diensten denkt. Aus diesem Grund macht in diesem Zusammenhang die Unterscheidung zwischen Bestands- und Nutzungsdaten auch keinen Sinn. Aufgrund der umfangreichen Berücksichtigung auch geringer Straftatbestände, kann der Richtervorbehalt bei Nutzungsdaten und Passwörtern den weitgehenden Eingriff in die Privatsphäre bei nur geringfügigen Vergehen nicht schützen. Der Straftatenkatalog muss daher dringend auf die gleiche Ebene wie die Online-Durchsuchung gesetzt werden und entsprechend nur bei besonders schweren Straftaten umfassen. Zudem sollte auch die Abfrage von Bestandsdaten unter Richtervorbehalt gestellt werden.

Der Referentenentwurf berücksichtigt zudem nicht, dass neben der StPO eine Vielzahl der bundes- und landesgesetzlichen Vorschriften eine Ermächtigungsgrundlage für

die Abfrage von Bestandsdaten enthalten - beispielsweise die Landespolizeigesetze – die ebenfalls auf § 14 TMG verweisen. In einer Vielzahl dieser Gesetze werden das TKG und das TMG aber 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.

Die Änderung ist darüber hinaus nicht nur aus rechtsstaatlichen und datenschutzrechtlichen Gründen abzulehnen, sondern sie ist auch kaum praktikabel, denn Unternehmen speichern Passwörter auf Grundlage des § 32 der DSGVO verschlüsselt. Die Telemedienanbieter sind somit gar nicht erst in der Lage Passwörter im Klartext mit den Behörden zu teilen. Vor diesem Hintergrund kann eine Pflicht zur entschlüsselten Speicherung von Passwörtern kaum Wille der Bundesregierung sein.
In jedem Fall entstünden hier Normungskonflikte, die mindestens zu Rechtsunsicherheit bzw. im schlimmsten Fall zu einer massiven Schwächung der Datensicherheit führen würde.

Fazit

Der BVDW lehnt die vorgeschlagene Ausweitung des Auskunftsverfahrens aus dem TKG auf Telemediendienste in der vorliegenden Form daher ab. Der weitreichende Anwendungsbereich, gekoppelt mit der stark erweiterten Auskunftsbefugnis einer Großzahl von Strafverfolgungsbehörden für teilweise kleinere Ordnungswidrigkeiten, führt zu einem Ausmaß an Datenherausgabe personenbezogener Daten und möglicher Überwachung von Nutzern, die aus datenschutzrechtlicher und rechtsstaatlicher Sicht nicht zu akzeptieren und nicht verhältnismäßig ist.

2.2 Änderungen des NetzDG

Das NetzDG ist, trotz aller Kritik, im Jahr 2017 beschlossen worden. Auch der BVDW hatte sich im Vorfeld kritisch geäußert und ist weiterhin der Meinung, dass bei einer Überarbeitung des NetzDGs im Frühjahr 2020 weitere Stellschrauben nötig sind, damit das Gesetz seine Ziele erreicht und gleichzeitig ein Schutz der Meinungsfreiheit gestärkt und die Gefahr eines overblockings verhindert werden kann. Der nun vorliegende Referentenentwurf hat zwar ein wichtiges Ziel, nämlich die effektive Strafverfolgung bei rechtswidrigen Inhalten im Netz, doch er greift in Teilen der anstehenden Evaluierung des NetzDGs vor und führt in seiner jetzigen Form weitere Risiken ein, indem eine Meldepflicht von Inhalten und IP-Adressen (inklusive Portnummern) für die sozialen Netzwerke gegenüber Strafverfolgungsbehörden festgeschrieben wird, die in einer umfangreichen Weiterleitung von personenbezogenen Daten resultieren wird.

Dabei ist nicht zu vergessen, dass es bereits etablierte Verfahren und Prozesse für Strafverfolgungsbehörden gibt, um Informationen abzufragen, insbesondere für im Inland ansässige Anbieter, aber auch für Anbieter mit Sitz in einem anderen Land. Der BVDW ist der Auffassung, dass das Verfahren für Auskunftsersuchen für Anbieter mit Sitz im Ausland nicht mehr zeitgemäß und zu langwierig ist. Das Verfahren bspw. über internationale Rechtshilfeersuche (MLAT) kann bis zu einem Jahr dauern – dann sind die von den Strafverfolgungsbehörden angefragten IP-Adressen bereits nicht mehr gespeichert – das System funktioniert also nicht zufriedenstellend. Die im

BVDW organisierten Unternehmen gehen deshalb bereits heute über das gesetzlich vorgeschriebene Maß der Verpflichtungen hinaus und erteilen auf freiwilliger Basis Auskunft bei Anfragen von Strafverfolgungsbehörden ohne auf das MLAT-Verfahren zu verweisen. Es bestehen dabei bereits Mindeststandards, die berücksichtigt werden müssen, um nicht am Heimatstandort bei einer widerrechtlichen Datenherausgabe zu haften. Diese freiwilligen Verfahren haben sich bewährt und sollten fortbestehen können trotz der anvisierten Gesetzesänderung.

Rechtsunsicherheiten, mangelnde rechtsstaatliche Kontrolle, tiefe Eingriffe in die Grundrechte

Der Referentenentwurf führt mit § 3 a eine neue Meldepflicht für die vom NetzDG betroffenen Anbieter sozialer Netzwerke ein, die die Strafverfolgung von Hass und Hetze im Netz verbessern soll. Die zugrunde liegende Idee des neuen Paragraphen, dass das Löschen und Sperren von Inhalten/Konten langfristig nicht ausreichen wird, sondern, dass Personen strafrechtlich verfolgt werden müssen, ist nachzuvollziehen. Allerdings ist der BVDW der Ansicht, dass das vorgeschlagene Verfahren zu weit geht und mit datenschutzrechtlichen Grundsätzen nicht zu vereinen ist, nicht genügend rechtsstaatliche Schutzmechanismen bietet und zugleich tiefe Eingriffe in die Grundfreiheiten der Nutzer ermöglicht.

Der neue § 3 a sieht vor, dass Anbieter sozialer Netzwerke, die in den Anwendungsbereich des NetzDGs fallen, Inhalte und IP-Adressen (inkl. Portnummern) über eine, vom Unternehmen selbst einzurichtende, technische Schnittstelle an eine zentrale Stelle des Bundeskriminalamts übermitteln sollen.
Die Meldung muss geschehen, wenn der Anbieter zu dem Ergebnis gekommen ist, dass der gemeldete Inhalt, den der Anbieter gelöscht oder gesperrt hat, auch gegen bestimmte StGB-Straftatbestände verstößt und nicht gerechtfertigt ist. Gelistet werden § 86, 86a, 89a, 91, 126, 129 bis 129b, 130, 131, 140, 184b in Verbindung mit 184d und 241 (in Form der Bedrohung mit einem Tötungsdelikt) des Strafgesetzbuches. Diese Prüfung muss unverzüglich nach der Entfernung eines Inhalts oder der Sperrung eines Zugangs geschehen und die Übermittlung hat elektronisch an eine vom BKA zur Verfügung gestellten Schnittstelle zu erfolgen.

Diese Form der proaktiven Meldepflicht wird dazu führen, dass eine Flut an Daten an das BKA übermittelt wird. Vor allem werden diese Daten übermittelt, ohne dass vorab eine fallbezogene Prüfung durch das BKA oder eine sonstige staatliche Stelle erfolgt ist. Nach § 3 a ist es ganz alleine die Entscheidung des Anbieters des sozialen Netzwerks, ob die Straftatbestände erfüllt scheinen oder nicht und somit eine Weiterleitung notwendig ist oder nicht. Macht das Unternehmen einen Fehler, drohen die Bußgelder nach § 4 des NetzDGs. Hiermit wird somit eine Verlagerung hoheitlicher Aufgaben von Strafverfolgungsbehörden auf private Unternehmen festgeschrieben, die der BVDW ablehnt.

Aus dem Text des § 3 a geht zudem nicht klar hervor wie genau diese Meldung auszusehen hat, was das BKA mit den übermittelten Daten machen kann, wie lange die Daten gespeichert werden können, wann und wie sie gelöscht werden müssen und für welche Fälle das BKA die Informationen nutzen darf. Es würden sich somit massive Bestände an Daten beim BKA sammeln und einen tiefen Eingriff in die Grundrechte der Menschen ermöglichen, ohne dass eine rechtstaatliche Kontrolle vorab vorgesehen ist und Strukturen geschaffen wurden, die die Grundrechte der

Nutzer schützt. Es kann darüber hinaus zu der Situation kommen, dass Anbieter sozialer Netzwerke Daten melden, sich im Nachhinein aber herausstellt, dass es sich um eine Fehleinschätzung gehandelt hat. In diesem Fall wurden Daten von Personen gemeldet, die sich aus rechtlicher Sicht nichts zuschulden haben kommen lassen. Fraglich ist zudem wie mit den Inhalten von Nutzern umgegangen werden soll, die nicht in Deutschland ansässig sind.

Nach § 3 a Abs. 6 hat das BKA 14 Tage Zeit einen vom sozialen Netzwerk gemeldeten Inhalt zu prüfen (Anbieter haben 24 Stunden dafür Zeit). In diesem Zeitraum der 14 Tage darf der Anbieter die betroffene Person nicht darüber informieren. Sollte das BKA der Meinung sein, dass eine Aufklärung des Betroffenen über den Vorgang, das Ermittlungsverfahren gefährdet, dürfen die Anbieter ihre Nutzer überhaupt nicht informieren. Auch diese Regelung ist nicht mit den datenschutzrechtlichen Voraussetzungen zu vereinen und hebelt die Rechte der Betroffenen völlig aus. Zudem scheint das Meldeverfahren nicht teil der Berichtspflicht des NetzDG (§ 2) zu sein. Ziel von Transparenzberichten ist jedoch gerade der Öffentlichkeit Einblicke in behördliches Handeln in Bezug auf die Privatwirtschaft zu geben.

Der Referentenentwurf schlägt des Weiteren die Einführung einer neuen Begriffsbestimmung in § 1 Abs. 4. des NetzDG vor - „Beschwerde über rechtswidrige Inhalte". Über diese neue Definition wird zwar nicht die Gruppe der vom NetzDG betroffenen Anbieter erweitert, aber sie löst eine Ausdehnung der betroffenen Beschwerden aus. Wenn eine „Beschwerde über rechtswidrige Inhalte" als „Beanstandung eines Inhalts mit dem Begehren der Entfernung des Inhaltes oder der Sperrung des Zugangs zum Inhalt" definiert wird, würde die Anzahl der Beschwerden in den Millionenbereich gehen, da nicht nur Meldungen nach dem NetzDG betroffen wären, sondern jegliche Beanstandungen in jeglicher Form. Dies würde sich entsprechend in der Meldepflicht des neuen § 3 a widerspiegeln. Die Begriffsbestimmung in § 1 Abs. 4 muss somit enger gefasst werden. Aus Sicht des BVDW muss sich der Umfang der Definition auf die Beschwerden nach dem NetzDG-Meldeweg des Unternehmens beschränken. Alles andere ist nicht leistbar, nicht für die Unternehmen selbst, aber auch nicht für die Strafverfolgungsbehörden. Generell kann das Ziel einer effektiveren Strafverfolgung nur dann erreicht werden, wenn die Kapazitäten des BKA, der LKAs, der Staatsanwaltschaften und Gerichte gestärkt werden. Mit einer massenhaften Weiterleitung von Daten ist allein aus Kapazitätsgründen sowohl den Unternehmen, als auch den Strafverfolgungsbehörden nicht geholfen.

Fazit

Der BVDW ist der Ansicht, dass hier klarer Nachbesserungsbedarf vorhanden ist, damit der richtige Interessensausgleich getroffen werden kann. Die Grundrechte sowie die Informationsfreiheit aller dürfen nicht aufgegeben werden, um eine Strafverfolgung rechtswidriger oder strafbarer Inhalte zu erreichen.