VERBAND DER INTERNETWIRTSCHAFT E.V.

STELLUNGNAHME

zum Referentenentwurf eines Gesetzes zur Bekämpfung des Rechtextremismus 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 Telemediendienstesanbieter. 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 Anfangsverdachtes 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 Gesetzentwurfes

- **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 Wirkungskreis 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.[1]

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

[1] Vgl. EGMR, Application no. 62357/14 (Benedik vs. Slovenia) https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-182455%22]} (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 Telemediendiesten 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 vorgeschrieben 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 Auskunftsersuchen 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, sodass 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.

<u>Beschwerdeprüfung und Umgang mit Falschmeldungen</u>

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 Gesetzestextes 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 Anfangsverdachtes 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 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 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 vom 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.

ANLAGE
Kostenaufwand der Anbieter von Telemediendiensten für Erfüllung geplanter Auskunftspflichten durch den Entwurf eines Gesetzes zur Bekämpfung des Rechtextremismus und der Hasskriminalität (Referentenentwurf vom 18. Dezember 2019)

Berlin, den 17.01.2020

Das Bundesministerium der Justiz und für Verbraucherschutz hat einen Referentenentwurf veröffentlicht, der eine Neuregelung von Auskunftspflichten nach dem Telemediengesetz vorsieht. Ein zentraler Baustein des Referentenentwurfs ist die Einführung eines § 15a-neu in das Telemediengesetz (TMG). Dieser soll zukünftig die Herausgabepflichten von Bestands- und Nutzungsdaten für die Anbieter von Telemediendiensten regeln. Hierzu sind Auskunftsansprüche für die Strafverfolgungs- und Sicherheitsbehörden und Regelungen für die Datenerhebung und Weitergabe von Bestands- und Nutzungsdaten für Telemediendienste-anbieter vorgesehen. Um die Verpflichtungen erfüllen zu können, müssen die Anbieter von Telemediendiensten technische und organisatorische Anforderungen erfüllen und die entsprechenden Voraussetzungen hierfür schaffen. Zudem werden geschäftsmäßige Telemediendienste ab 100.000 Kunden zur Einrichtung einer Schnittstelle verpflichtet. Die Fragen der konkreten Ausgestaltung, technischen Vorgaben sowie die zu beachtenden Anforderungen und datenschutzrechtlichen Maßgaben können aufgrund des vorliegenden Entwurfs noch nicht abschließend beantwortet werden. Auf dieser Grundlage kann die Anzahl der betroffenen Telemediendienste und die zu erwartenden Kosten nur vorläufig beziffert werden. Dementsprechend handelt es sich um eine erste Einschätzung.

I. Zusammenfassung

1. Betroffene Anbieter von Telemediendiensten (gesetzliche Definition in § 1 und § 2 TMG):
- **a) Unternehmen: Mindestens 2,3 Millionen**
- **b) Wirtschaftlich tätige Vereine rund 200.000 (Email, Foren, Nutzungsdaten Netzzugang)**
- **c) Kommunen rund 11.000 (Foren, Nutzungsdaten Netzzugang)**
- **d) Öffentliche Einrichtungen rund 16.000 wie beispielsweise**
  - **650 Verkehrsbetriebe ÖPNV (Email, Foren, Nutzungsdaten Netzzugang, Nutzungsdaten Verkehrsmittel)**
  - **7.000 Bäder (Nutzungsdaten Netzzugang)**

- 3.000 Krankenhäuser und Reha-Einrichtungen (Email, Foren, Nutzungsdaten Netzzugang)
- 425 Universitäten (Email, Foren, Nutzungsdaten Netzzugang)

e) Einzelpersonen, u.a. Freiberufler ca. 3.000.000 (die geschäftsmäßig Telemediendienste bereitstellen)

Anmerkung: Die Anzahl der Einzelpersonen und wirtschaftlich tätigen Vereine wurde auf Basis der Anzahl DE-Domains geschätzt:
16.3 Millionen registriert,
15.0 Millionen Inländische Unternehmen und Personen
1.3 Millionen Ausländische Inhaber
9.8 Millionen aktive DE-Domains

2. Technische Realisierbarkeit: Überwiegend ja

- signifikanter Aufwand für Rechtsberatung und Konzepterstellung bei KMU, Vereinen und Einzelpersonen
- Nutzungsdaten bisher zumeist nicht erfasst

3. Erfüllungsaufwand der Wirtschaft:

a) Investitionskosten:
- standardisiert nur mittlere und große Unternehmen (über 100.000 Kunden), ca. 74.000: 18 - 20 Milliarden Euro
- manuell für alle Unternehmen: 3,8 Milliarden Euro

b) Laufende Kosten:
- manuelles Verfahren, Kleinst- und Kleinunternehmen, ca. 2,2 Millionen: 79,15 Millionen Euro
- automatisiertes Verfahren, nur mittlere und große Unternehmen, ca. 74.000: 250 Millionen Euro

4. Erfüllungsaufwand Vereine, Kommunen, Öffentliche Einrichtungen, Einzelpersonen

Belastbare Erkenntnisse zu den eingesetzten Systemen dieser Betroffenen liegen nicht vor. Diese unterliegen jedoch regelmäßig einem besonderen Schutz (z.B. Krankenhäuser), welche den Investitionsbedarf je Einrichtung signifikant erhöhen.

Große Vereine werden regelmäßig in der Form großer Wirtschaftsbetriebe geführt (Beispiel: ADAC, Schufa), gleiches gilt für Verkehrsbetriebe oder

ähnliche kommunale Einrichtungen. Diese Gruppe von Einrichtungen wird in der Regel auch die Schwelle von 100.000 Kunden (bzw. Teilnehmern / Mitgliedern) überschreiten und damit gegebenenfalls unter die Regelungen der automatisierten Schnittstellen fallen.

Insgesamt ist auch für diese Kategorien mit weiteren Investitions- und Betriebskosten in Milliardenhöhe zu rechnen, welche in weiten Teilen auf Landes- oder kommunaler Ebene zu tragen sein werden.

II. Die Ergebnisse unserer Recherche im Einzelnen

1. Anzahl Betroffene

Telemediendienste im Sinne des Gesetzes sind alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht bereits als Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind. Darunter fallen zumindest alle Internetseiten von Unternehmen, aber auch solche weiteren Betreiber wie Vereine mit wirtschaftlichem Teil, Angebote privater Betreiber mit Werbeschaltungen sowie öffentliche und kommunale Betriebe mit kommerziellen Betriebsteilen.

a) Unternehmen
Es gibt Stand 30.09.2018 rund 3,5 Millionen Unternehmen in Deutschland, unabhängig von deren Größenklasse. Von diesen betreiben zumindest 2,3 Millionen bekanntermaßen eine Webseite und unterhalten somit ein Angebot von Telemediendiensten, wobei der überwiegende Teil der Angebote von Kleinst- und Kleinunternehmen unterhalten wird.

Bisher fallen nur nach § 6 TKG gemeldete Unternehmen gemäß § 112 TKG unter eine Verpflichtung zur Bestandsdatenauskunft. Von den derzeit rund 3100 gemeldeten Unternehmen fallen nach Abzug der rund 220 internationalen sowie der alleine mit der Verarbeitung von Rundfunksignalen beschäftigten Unternehmen heute theoretisch ca. 2500 Unternehmen, in der Praxis jedoch nur rund 750 "aktive" Unternehmen unter die bisherige Verpflichtung (Teilnahme Auskunftsverfahren, Teilnahme SINA-VPN, Erstellung Sicherheitskonzept, etc.).

Plakativ betrachtet wäre zukünftig faktisch die gesamte deutsche Wirtschaft zur Bestandsdatenauskunft über Ihre Kunden verpflichtet.

Ergänzend ist darauf hinzuweisen, dass darüber hinaus Millionen von Unternehmen aus Europa ebenfalls zur Erfüllung der Vorgaben verpflichtet wären, sofern sie einen Kundenstamm in Deutschland unterhalten und Sach- oder Dienstleistungen an Kunden in Deutschland über ein Portal erbringen (z.B. Plattformen).

Diese Kosten wurden bisher nicht berechnet.

b) Vereine

Es gibt rund 600.000 Vereine in Deutschland (Stand: 31.12.2017), unabhängig von deren Vereinszweck. Von diesen betreiben zumindest 500.000 ein Webangebot, zumeist mit einem Angebot für Mitglieder. Rund 200.000 unterhalten ein Angebot, welches einem geschäftsmäßig erbrachten Angebot von Telemediendiensten entspricht und den Regelungen des TMG unterliegt.

c) Kommunen

Alle 11.000 Kommunen in Deutschland sind gehalten, ein Angebot an die Öffentlichkeit zu unterhalten, dies umfasst in der Regel auch Foren und ein Angebot zum Netzzugang in öffentlichen Einrichtungen (Rathäuser, Bürgerhäuser, etc.)

d) Öffentliche Einrichtungen

Faktisch alle öffentlichen Einrichtungen unterhalten ein Informationsangebot für die Öffentlichkeit, viele Einrichtungen wie Universitäten, Bibliotheken etc. bieten neben Diskussionsforen auch Emailadressen an. Fast ausnahmslos werden TMG-Angebote wie Netzzugänge über WLAN angeboten, dies gilt auch für den ÖPNV und Einrichtungen wie Bäder, Krankenhäuser oder andere vergleichbare öffentliche Einrichtungen.

e) Einzelpersonen

Eine Vielzahl von Einzelpersonen, betreiben oder bieten Dienste (Foren, Webseiten, EMail) an, die als Telemediendienste im Sinne des TMG anzusehen sind. Hierbei ist zu berücksichtigen, dass diese auch als

geschäftsmäßige erbrachte Telemediendienste zu qualifizieren sind, beispielsweise wenn sich diese über Werbung finanzieren.

2. Technische Realisierbarkeit

Ob Auskunftspflichten für geschäftsmäßige Erbringer zu Bestandsdaten und zu einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse (§ 113 Absatz 1 Satz 3 TKG) technisch realisierbar sind, ist pauschal nur bedingt zu beantworten. Überwiegend ist dies wohl zu bejahen, allerdings dürfte es bei vielen Betroffenen die Anschaffung von Daten-speichersystemen analog der Vorgaben zur Vorratsdatenspeicherung nach §§ 113 ff. TKG erfordern. Derartige Systeme sind äußerst aufwändig und schlugen bereits bei Ihrer Anschaffung bei den TK-Anbietern (d.h. 3100 Unternehmen) mit Investitionskosten von rund 600 Millionen Euro zu Buche.

3. Erfüllungsaufwand für die Wirtschaft

a) Investitionskosten
- Automatisiertes Verfahren
Der Erfüllungsaufwand für die Anbieter von Telemediendiensten bei einem automatisierten Verfahren ist nur bedingt einzuschätzen, da im Gegensatz zu den Telekommunikationsunternehmen der Umfang von "Bestandsdaten" für den überwiegenden Teil der betroffenen Unternehmen noch zwingend weiter abgegrenzt werden muss und die Systeme eines Großteils der Anbieter nicht auf die zusammenhängende Beauskunftung von Bestands-daten ausgelegt sein dürfte.

Elementar ist daher im Vorfeld grundsätzlich die Frage zu klären, ob unter einer "Bestandsdatenauskunft" nur eine Beauskunftung von aus eigenen wirtschaftlichen Interessen der Unternehmen erhobenen und für den erforderlichen und zulässigen Zeitraum gespeicherten Daten zu verstehen ist (d.h. echte "Bestandsdaten"), oder vielmehr analog der Regelung des § 113 TKG oder beispielsweise auch der Speicherung von Daten im Bereich des Flugverkehrs eine Erhebung eines im Vorfeld fest definierten Datenumfangs und einer festgelegten Datenspeicherdauer, welche für das Unternehmen weder erforderlich ist noch im Einklang mit den sonstigen gesetzlichen Regelungen der DSGVO steht ("mandatierte Bestandsdaten"), gemeint ist.

Im Extremfall der mandatierten Bestandsdaten ist technisch eine zwar mögliche, aber ansonsten nicht erforderliche Erhebung und Zuordnung der Rohdaten zu den Anfragen erforderlich, so z.B. bei einem möglichen Eingangsdatum "IP-Adresse und Uhrzeit" statt einer eindeutigen Nutzerkennung oder Kundenummer, auf deren Verarbeitung die Systeme der Anbieter typischerweise ausgelegt sind.

Hierzu wird bei vielen betroffenen Unternehmen erstmalig die Anschaffung von geeigneten Datenspeichersystemen analog der Anforderungen an zulässige Speichersysteme für die Vorratsdatenspeicherung nach den §§ 113 ff. TKG als initiale Investition neben der Investition in die Zuleitung der erforderlichen Daten aus den eigenen Systemen erforderlich werden.

Alleine bei den betroffenen TK-Anbietern waren Investition in Höhe von rund 600 Millionen EUR zur Erfüllung dieser Anforderungen notwendig. Für bisher nicht mit derartigen Anfragenkonfrontierten Unternehmen ist im Rahmen der Anschaffung und Organisation der IT-Systeme zur Ausleitung der notwendigen Daten an das Speichersystem mit überproportional hohen Aufwendungen zu rechnen.

Zudem wären für einen Unterhalt und Betrieb der Systeme laufende Aufwendungen in signifikanter Höher erforderlich.

Unter Annahme einer Aufnahmegrenze von 100.000 Kunden wie in Absatz 5 des § 15a-neu TMG derzeit vorgesehen ist davon auszugehen, dass nur Mittlere- und Großunternehmen von einer systematischen Ausleitung betroffen sein werden, d.h. es wären ca. 74.000 Unternehmen statt der bisher betroffenen 2.500 Unternehmen verpflichtet (Faktor 30).

Im TK-Bereich waren Investitionen von rund 600 Millionen Euro zur Erfüllung der Verpflichtungen aus § 113 TKG erforderlich, bei einem angenommenen Faktor 30 für die Gesamtwirtschaft (d.h. Mittlere und Großunternehmen) wären es somit ca. 18-20 Milliarden Euro oder rund 10% der jährlichen Sachinvestitionen der Gesamtwirtschaft.

Sämtliche Unternehmen auf eine derartige Zuordnung zu verpflichten dürfte auch gesamtwirtschaftlich kaum darstellbar sein (ca. 500 Milliarden Euro) und müsste analog der Regelungen zur Vorratsdatenspeicherung zwingend mit einer Härtefallregelung und einem Kostenersatz verbunden werden. Wir verweisen diesbezüglich eindringlich auf die durchschnittlichen jährlichen Investitionsbudgets der Unternehmen als Relationsmaßstab

anhand derer die Kostenbelastung für die geplanten Verpflichtungen offensichtlich wird.

Als Fazit zeigt sich, das eine Verpflichtung auf Daten außerhalb der aus eigenen Geschäftszwecken bereits erhobenen Daten und die damit verbundene Anschaffung von gesicherten Speichersystemen in jedem Fall zu vermeiden sein dürfte.

- Manuelles Verfahren
Die Investitionsaufwendungen für rein manuelle Auskünfte alleine bezogen auf in den Systemen der Unternehmen bereits gespeicherten Daten sind geringer, hier fallen neben den laufenden Kosten (siehe unter b) primär Kosten für Systeme zur Dokumentation und gesicherten Übertragung sowie organisatorische Kosten an, welche auch für kleine und kleinste Unternehmen tragbar sein dürften. Wir gehen hierbei von Investitionskosten von rund 1.000 Euro für kleinste, 2.000 Euro für kleine, 10.000 Euro für mittlere und 50.000 Euro für große Unternehmen aus (total ca. 3,8 Milliarden Euro).

b) Laufende Kosten
Die laufenden Kosten sind ebenfalls stark von der rechtlichen Auskunftskonstellation und der Anzahl der betroffenen Unternehmen abhängig, hier gilt es primär zwei Fälle zu unterscheiden:

- Manuelle Beauskunftung
Der günstigste Fall stellt sich bei einer reinen Beauskunftung von echten Bestandsdaten im ausschließlich manuellen Verfahren ein, dies erneut unter der Annahme sehr geringer praktischer Anfragezahlen pro Unternehmen und einer Aufnahmegrenze von ca. 100.000 Kunden zur automatischen Beauskunftung.

Beispielrechnung:
Wir legen Stundensätze nach Komplexität der unten genannten einzelnen Tätigkeiten pro Auskunftsersuchen zu Grunde.

Enthalten sind Personal- und Sachaufwand für die Beantwortung eines Auskunftsersuchens. Konkretisiert:

- Verteilung des Ersuchens im Unternehmen an Zuständigen (einfache Tätigkeit 30 €/h); 10 Minuten = 5 Euro;

- erste Bearbeitung mit Prüfung der Berechtigung bzw. Verifizierung des

ersuchenden Dienstes (anspruchsvolle Tätigkeit 50 €/h); 20 Minuten = 16,6 Euro

- Sachverhaltsermittlung im Unternehmen, bspw. Prüfung eigener Kunde / Vorliegen von Datensätzen, (einfache Tätigkeit 30 €/h); 10 Minuten = 5 Euro;

- etwaige Rückfragen, (Mittlere Tätigkeit 40 €/h; 5 Minuten = 2,5 Euro;

- Erstellung der Auskunft mit Formatierung Datensatz, bspw. maschinenlesbar, (mittlere Tätigkeit 40 €/h); 10 Minuten = 6,70 Euro;

In diesem Beispiel kämen wir bei 55 Minuten Bearbeitungszeit auf 35,80 Euro je Fall.

Nach Abzug der Mittleren und Großunternehmen (hier gehen wir von einer automatischen Beantwortung aus) verbleiben 2,211 Millionen kleine und kleinste Unternehmen, rechnerisch ist daher von einem Betrag in Höhe von ca. 79,15 Millionen Euro je Jahr auszugehen, sofern kleine und kleinste Unternehmen zu einem rein manuellen Auskunftsverfahren alleine für bereits regulär erhobene Daten verpflichtet werden.

Zu prüfen bliebe, ob diese Kosten evtl. durch Fallpauschalen analog der Aufwandsregelungen des TKG aufgefangen werden können bzw. sollten.

- Automatisiertes Verfahren
Bei einem automatisierten Verfahren liegt der Aufwand für den Betrieb eines geeigneten Systems derzeit bei mindestens 2400 €/Jahr je Unternehmen für eine gehostete SaaS-Lösung (vgl. § 112 TKG). Diese Summe macht das automatisierte Verfahren unwirtschaftlich für kleine und kleinste Unternehmen.

In diesem unteren Mindestbetrag von 2.400 Euro/Jahr sind enthalten die Personal- und Sachaufwand für die Beantwortung von Auskunftsersuchen, konkret:
- Speichersystem bei einen Hostserver-Anbieter 150 €/Monat

Kosten pauschaliert 50 €/Monat für nachfolgende Positionen:
- Verteilung des Ersuchens im Unternehmen
- erste Bearbeitung mit Prüfung der Berechtigung bzw. Verifizierung des ersuchenden Dienstes
- Sachverhaltsermittlung im Unternehmen (Eigener Kunde/Vorliegen von Datensätzen)

- etwaige Rückfragen
- Kontrolle der Auskünfte wie Formatierung der Datensätze, Übertragungen, Fehlerprotokolle etc.

Entsprechend höhere Kosten entstehen bei Entwicklung und Betrieb eines eigenen Systems oder einer komplexen Integration in die Bestandssysteme des Unternehmens, beispielsweise ist für Großunternehmen mit dediziertem Personaleinsatz ein Mehrfaches dieses Satzes anzunehmen.

Davon ausgehend, dass primär Mittlere und Großunternehmen unter die Regelung fallen werden und die vorgeschlagene Aufnahmeschwelle des Absatz 5 in § 15a-neu TMG von 100.000 Kunden aufrechterhalten wird, werden wie bereits im Investitionsbereich ausgeführt ca. 74.000 Unternehmen von einer derartigen Regelung betroffen.

Im Schnitt erfolgen heute im TK-Bereich ca. 14 Millionen. Anfragen/Jahr, im automatisierten Verfahren, d.h. rund 19.000 Anfragen pro am KDAV Verfahren Teilnehmenden Unternehmen. Auf die Gesamtwirtschaft gerechnet werden diesseits folglich ca. 1,4 Milliarden Anfragen je Jahr erwartet.

Der Verfassungsschutz alleine ist beispielsweise mit 750.000 Anfragen im KDAV-Verfahren vertreten, d.h. rund 1.000 Anfragen pro Jahr/Unternehmen.

In analoger Anwendung wird insofern ein Volumen von rund 75 Millionen Anfragen/Jahr alleine aus dem Bereich des Verfassungsschutzes im automatisierten Verfahren für die Gesamtwirtschaft (mittlere und große Unternehmen) erwartet.

Werden als untere Grenzkosten 2.400 €/Jahr für einen Betrieb im automatisierten Verfahren angenommen entstehen Kosten von mindesten 180 Millionen EUR/Jahr, diese werden in der Praxis jedoch deutlich überschritten und dürften konservativ geschätzt bei rund 250 Millionen Euro liegen.

Auch dies gilt allerdings nur, wenn man zu Grunde legt, dass es sich um Daten handelt, die zu Unternehmenszwecken grundsätzlich bereits gespeichert werden.

Im Falle der Verpflichtung zur Anschaffung von Systemen analog der Vorratsdatenspeicherung werden die Kosten für den laufenden Betrieb der Speicher- und Erfassungssysteme, welche neben den Kosten der

Auskunftssysteme anfallen und diese bei weitem übersteigen, auf die Gesamtwirtschaft gerechnet im unteren zweistelligen Milliardenbereich je Jahr anzusiedeln sein.