Eckpunkte zum „Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität“

Berlin, 20.12.2019

Die Einführung des Netzwerkdurchsetzungsgesetzes (NetzDG) im Jahr 2017 zielte auf die Eindämmung von Hass und Hetze im Internet – auch als Hate Speech bezeichnet – ab. An dem Gesetz ist bereits damals Kritik geübt worden, die seit seinem Inkrafttreten fortbesteht. Die Kritik hat das NetzDG vor allem wegen seiner negativen Auswirkungen und nicht intendierten Nebeneffekte erfahren. Befürchtet wurden unter anderem potentiell negative Auswirkungen auf die Informations- und eine Einschränkung der Meinungsfreiheit gemäß Artikel 5 des Grundgesetzes (GG).

Infolge der Ereignisse im Sommer und Herbst 2019 haben verschiedene politische Entscheidungsträger der Bundesregierung, der Innen- und Justizminister/-senatoren aus Bund und Ländern zahlreiche Maßnahmen zur Bekämpfung von Rechtsextremismus und Hass im digitalen Raum beschlossen. eco – Verband der Internetwirtschaft e.V. bekennt sich ebenfalls zum Ziel der Bekämpfung von Rechtsextremismus und Hasskriminalität. Er unterstützt den generellen Kurs der Politik, dagegen vorzugehen.

Am 18. Dezember 2019 veröffentlichte das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) den Referentenentwurf für ein "Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität". Das Gesetzesvorhaben zielt inhaltlich entgegen der bisherigen Ankündigungen nicht nur auf die Stärkung des NetzDG ab, sondern enthält darüber hinaus Erweiterungen im Strafgesetzbuch, in der Strafprozessordnung, im Telemediengesetz und im BKA-Gesetz, die zum Teil tiefe Eingriffe in das informationelle Selbstbestimmungsrecht nach Art. 2 Abs. 1 i. V. mit Art. 1 Abs. 1 GG, das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG sowie in das Fernmeldegeheimnis gem. Artikel 10 GG für die Bürgerinnen und Bürger zur Folge hätten.

Nach Ansicht des eco geht der vorliegende Referentenentwurf deutlich über eine Überarbeitung und Verschärfung des NetzDG hinaus und hat tiefgreifendende Auswirkungen auf alle Telemediendienste. Es ist vorgesehen, auch die Strafprozessordnung, das BKA-Gesetz und das Telemediengesetz anzupassen. Neben einer Meldepflicht für soziale Netzwerke sollen spezielle Regelungen für die Datenerhebung und

Weitergabe im Telemediengesetz geschaffen sowie Unternehmen zur Herausgabe von Passwörtern verpflichtet werden. Die Befugnisse der Strafverfolgungs- und Sicherheitsbehörden sollen zudem erheblich erweitert werden. Zentrale Aspekte des Gesetzesvorhabens werfen erhebliche datenschutzrechtliche, verfassungsrechtliche und europarechtliche Fragen auf und müssen daher kritisch beleuchtet werden. Insgesamt ist das Vorhaben in höchstem Maße bedenklich.

eco möchte sich frühzeitig in die Debatte einbringen und auf zentrale Probleme und kritische Aspekte des Gesetzesvorhabens hinweisen. Das vorliegende Eckpunktepapier soll hierfür als eine erste Einschätzung und Debattenbeitrag darstellen. Insbesondere die Überlegungen zu den nachfolgend aufgeführten Punkten sind von besonderer Brisanz und bedürfen der eingehenden Betrachtung und einer Diskussion.

- Auskunftspflicht für alle Telemedienbetreiber
- Herausgabe von Passwörtern
- Erfüllungsaufwand für Telemedienbetreiber
- Einführung einer Meldepflicht für Soziale Netzwerke
- Datenübermittlung und Datenspeicherung beim BKA
- Mangelnde rechtsstaatliche Kontrollmechanismen

1. Auskunftspflichten zu Bestands- und Nutzungsdaten für Telemediendienste

Zentraler Bestandteil des Referentenentwurfs des „Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität“ ist die Neugestaltung und Erweiterung von Auskunftspflichten im Telemediengesetz (TMG). Maßgeblich hierfür soll ein neu zu schaffender §15a-neu TMG sein, der die Vorgaben für die Herausgabe von Bestands- und Nutzungsdaten regeln soll, die die Anbieter von Telemediendiensten auf Grundlage der §§ 14 und 15 TMG erheben dürfen. Der Referentenentwurf sieht hier zukünftig eine Pflicht für alle Telemedienbetreiber vor, unabhängig davon, ob es sich um Onlineshops, Diskussionsforen, Messengerdienste, E-Mail-Dienste oder Medienanbieter handelt, die von ihnen erhobenen Bestands- und Nutzungsdaten herauszugeben. Dabei sollen die Unternehmen alle ihnen zur Verfügung stehenden Datenquellen nutzen, um die angefragten Informationen bereitstellen zu können.

Mit der geplanten Regelung im Telemediengesetz werden die Auskunftsansprüche für die Strafverfolgungs- und Sicherheitsbehörden erheblich ausgeweitet und Regelungen für die Datenerhebung und Weitergabe von Bestands- und Nutzungsdaten für Telemediendienste-anbieter geschaffen. Die geplante Einräumung neuer Befugnisse und Auskunftsansprüche von Sicherheitsbehörden sowie die Verpflichtung in ganz erheblichem Umfang personenbezogene Daten von Nutzern herausgeben zu müssen, ist kritisch zu bewerten. Denn damit sind tiefgreifende Einschnitte in bürgerliche Freiheitsrechte, den Datenschutz und das Fernmeldegeheimnis verbunden.

Eine zentrale Frage ist dabei, inwieweit diese Herausgabepflichten verhältnismäßig sind. Die hier pauschal zur Debatte gestellten für die Herausgabe bereitzuhaltenden Bestands- und Nutzungsdaten ermöglichen erhebliche Eingriffe in die Dienste und können dabei auch den Kernbereich der privaten Lebensgestaltung nicht nur der unmittelbar adressierten Nutzer betreffen, bspw. bei Datingportalen oder bei Messengerdiensten. Inwieweit solch tiefgreifende Eingriffe in den einzelnen Fällen sinnvoll und überhaupt gerechtfertigt sein können, bleibt weiteren gesetzlichen Regelungen vorbehalten.

Der Referentenentwurf sieht zudem einen sehr weit gefassten Kreis berechtigter Stellen vor, die entsprechende Auskunftsrechte gegenüber Anbietern von Telemediendiensten geltend machen können. Er erstreckt sich auf alle zuständigen Behörden für die Verfolgung von Straftaten oder Ordnungswidrigkeiten und die Gefahrenabwehr, sämtliche Geheimdienste von Bund und Ländern sowie auf die Zollverwaltung und Ämter, die u.a. auch für die Schwarzarbeitsbekämpfung zuständig sind. Bestands- und Nutzungsdaten dürfen dabei auch für die Verfolgung einfacher Delikte und Ordnungswidrigkeiten herausgegeben werden. Inwieweit zudem durch die Nutzung der Datenquellen bei den Unternehmen eine Mitwirkungspflicht für die Erstellung von Nutzerprofilen entsteht, löst die Bestimmung nicht auf. Die hier getroffenen Regelungen höhlen die bestehenden datenschutzrechtlichen Maßgaben aus, indem sie umfassende Zugriffsrechte für Behörden ermöglichen und Unternehmen dazu verpflichten, die Daten ihrer Nutzer zusammenzuführen.

Dies unterstreicht, dass das BMJV sowohl die qualitative als auch die quantitative Dimension der Neuregelungen des Telemediengesetzes verkannt hat und die damit verbundenen Auswirkungen auf Telemedien-dienste nicht hinreichend bedacht hat. Die Regelungen betreffen nicht nur Anbieter sozialer Medien, sondern alle Dienste die unter das Telemedien-

gesetz fallen und damit alle geschäftsmäßig erbrachten Telemediendienste: Seien es E-Mail-Anbieter, Webseiten- und Forenbetreiber, Online-Shoppingdienste, Chat- und Messengerdienste, Clouddienste.

2. Herausgabe von Passwörtern

Ein sehr problematischer Punkt des § 15a-neu TMG ist, dass sich die Verpflichtung zur Herausgabe von Bestands- und Nutzungsdaten auch auf solche Daten erstrecken soll, mit deren Hilfe ein Zugriff auf Speicher und Endgeräte möglich ist. Damit sind Passwörter oder andere Sicherheits-mechanismen gemeint, mit denen Nutzer ihre Accounts absichern.

Die Verhältnismäßigkeit zur Herausgabe einer solchen Information ist grundsätzlich fragwürdig. Die Herausgabe von Passwörtern ermöglicht den Zugriff auf Online-Konten und damit die Online-Identität eines Nutzers. So wird eine umfassende Onlinedurchsuchung möglich, einschließlich des Zugriffs auf Kommunikationsinhalte wie E-Mails, in der Cloud hinterlegte Fotos, Dokumente, Chat- und Messengernachrichten. Dadurch wird in den Kernbereich der privaten Lebensgestaltung von Nutzerinnen und Nutzern eingegriffen und eingeschränkt. Dies betrifft nicht nur den angefragten Nutzer, sondern bei mehrseitiger Kommunikation auch außenstehende Personen, die in aller Regel keinen Anlass für den behördlichen Datenabruf gegeben haben.

Problematisch ist zudem, dass die jeweils anfragenden Behörden mit den entsprechenden Zugangsdaten nicht nur die Möglichkeit der Ausleitung und Sichtung von Informationen hätten, sondern zusätzlich auch selbst den Account "übernehmen" könnten. Das Vertrauen von Nutzerinnen und Nutzern in digitale Dienste würde durch eine solche Ermächtigung massiv erschüttert und ist daher abzulehnen.

Aus Sicht der Dienstebetreiber ist die Herausgabe von Informationen, mit deren Hilfe auf Speicher und Endgeräte zugegriffen werden kann, ein sicherheitskritisches Problem. Passwörter sollten aus Sicherheitsgründen nur verschlüsselt gespeichert werden, so dass sie nicht unmittelbar einsehbar sind. Offen bleibt, inwieweit aus dem Referentenentwurf eine Verpflichtung für die Betreiber aller Telemediendienste wie Messenger, E-Mailprovider, Social Media Plattformen und Internetforen abgeleitet werden kann, entweder alle Passwörter im Klartext zu speichern oder das Verschlüsselungsverfahren für die Passwörter gegenüber den anfragenden

Behörden zu offenbaren. Aus Gründen der IT-Sicherheit und des Datenschutzes wäre beides fatal.

Zudem stellt sich die Frage, inwieweit die Anbieter von Telemediendiensten überhaupt imstande wären, entsprechende Auflagen zur Offenbarung von Verfahren und Passwörtern zu erfüllen. Insbesondere bei kleinen Anbietern, die nicht mit eigenen technischen Entwicklungen arbeiten, dürfte dies nicht der Fall sein. Eine Mitwirkungspflicht von Betreibern von Telemediendiensten bei der Entschlüsselung von Passwörtern bzw. der Bereitstellung von Informationen zum Entschlüsseln oder zurücksetzen von Passwörtern ist in jedem Fall abzulehnen.

3. Erfüllungsaufwand für Anbieter von Telemediendiensten

Die im Referentenentwurf aufgeführten Auskunfts- und Informationspflichten über Bestands- und Nutzungsdaten stellen auch ohne mögliche Mitwirkungspflichten bspw. bei der Identifizierung und Zusammenführung von Daten für die Betreiber von Telemediendiensten einen enormen Aufwand dar. Besonders schwer wiegt hier, dass der § 15a-neu TMG vorsieht, dass die Prüfung der Rechtmäßigkeit einer Anfrage beim jeweiligen Betreiber des Telemediendienstes durch eine entsprechende Fachkraft zu erfolgen hat. Gerade für kleine und mittelständische Anbieter von Telemediendiensten ist der damit verbundene technische, organisatorische und personelle Erfüllungsaufwand eine enorme finanzielle Belastung. Zusätzlich sieht § 15a-neu vor, dass Telemediendienste, die mehr als 100.000 Kunden haben, zur Einrichtung einer elektronischen Schnittstelle verpflichtet werden, um Auskunftsverlangen der berechtigten Stellen entgegenzunehmen und beantworten zu können.

Die technische Umsetzung und Maßgaben für den Einsatz einer solchen Schnittstelle sind dabei noch vollständig unklar. Das Angebot an Telemediendiensten in Deutschland ist sehr divers, so dass sich die Frage stellt, inwieweit die Daten in Abweichung von den bekannten Abfrageformen des Telekommunikationsgesetz (TKG) für die Bereitstellung aufbereitet und standardisiert sein müssen. Die Anforderungen sowie die individuellen Kosten der Bereitstellung werden sich daher je nach Dienst und genutzten Technologien sowie durch möglicherweise unterschiedliche Anforderungen an die Dienste im Rahmen der unterschiedlichen Auskunftspflichten erheblich unterscheiden. Das erschwert zum jetzigen Zeitpunkt eine konkrete Bezifferung des Erfüllungsaufwandes. Die dafür zu erwartenden Kosten werden jedoch bedingt durch die äußerst hohe Zahl der betroffenen

Unternehmen, die Telemediendienste anbieten, auch bei einfachster Ausgestaltung im Bereich mehrerer Milliarden Euro anzusiedeln sein. Unter Berücksichtigung der bestehenden Datenschutzvorschriften und einer angenommenen Komplexität der technischen Maßgaben analog zu den Verfahren nach §110 TKG werden voraussichtlich Investitionskosten in einem mittleren zweistelligen Milliardenbereich 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 nicht nur die Anbieter von Telemediendiensten vor enorme organisatorische und finanzielle Herausforderungen, sondern auch die berechtigten Stellen.

Zudem ist die Bemessungsgrundlage von 100.000 Kunden sehr problematisch und kein taugliches Kriterium für eine Aufgreifschwelle, da selbst kleinere Online-Dienste und Plattformen bereits eine große Reichweite und damit Nutzerzahlen erreichen, welche regelmäßig die Zahl von 100.000 deutlich übersteigen. Aufgrund der unterschiedlichen Form der Dienste kann das Abstellen auf die Kunden/Nutzerzahl eines Dienstes keine vernünftige Bemessungsgrundlage darstellen.

Das vorliegende Gesetzesvorhaben würde bedeuten, dass aus den Anforderungen des TKG (§113 Abs. 5 TKG iVm §110 TKG) abgeleitet, im Gegensatz zu den bisher knapp 300 Teilnehmern des automatisierten Auskunftsverfahrens über eine Schnittstelle nunmehr geschätzt zumindest rund 25.000 Unternehmen zu einer Teilnahme sowie rund 2.3 Millionen Unternehmen anstatt der bisherigen aus dem TKG abgeleiteten 6.500 Unternehmen zu einer Auskunft im manuellen Auskunftsverfahren verpflichtet wären.

4. Einführung einer Meldepflicht im NetzDG

Durch die Einführung einer Meldepflicht bestimmter rechtswidriger Inhalte in das NetzDG soll die Verbreitung von rechtsextremistischen und hasserfüllten Inhalten im Internet eingeschränkt und Täter verfolgt werden. Die Meldepflicht obliegt den Betreibern sozialer Netzwerke und soll an mehrere Voraussetzungen geknüpft werden. So muss ein Nutzer auf den zu meldenden Inhalt hingewiesen haben, das Netzwerk muss einen rechtswidrigen Inhalt gem. § 1 Abs. 3 NetzDG bejahen und den entsprechenden Inhalt gelöscht oder gesperrt haben. Die Meldungen sollen beim BKA bei einer neu zu schaffenden zentralen Stelle zusammenlaufen.

In der aktuellen Ausgestaltung ist die Meldepflicht aus Sicht der Internetwirtschaft kritisch einzustufen, da diese in vielen Bereichen zu erhöhter Rechtsunsicherheit für die Betreiber sozialer Netzwerke führt. So lässt der Entwurf offen, ob und inwieweit die bisher durchgeführte Überprüfung und Bewertung von Inhalten gem. NetzDG durch die Betreiber sozialer Netzwerke einer Dokumentation bedarf. Es ist fraglich, ob das Prüfverfahren für sich bzw. das Prüfergebnis ein Teil der Meldung sein soll. In diesem Kontext sehen sich die Betreiber sozialer Netzwerke auch mit Fragen zu möglichen "Falschmeldungen" konfrontiert.

Demgegenüber stellt der Entwurf klar, dass eine Meldung die IP-Adresse und die Portnummer des veröffentlichenden Nutzers umfassen muss, sofern sie beim Anbieter vorliegen. Dass die Meldung an das BKA die vorstehenden Informationen enthalten soll, ist zu kritisieren, da die Herausgabe und Übermittlung dieser sensiblen Daten normalerweise an einen Richtervorbehalt geknüpft ist. Mit Blick auf die Umsetzung des Meldeverfahrens ist zu berücksichtigen, dass die Betreiber sozialer Netzwerke seit der Einführung des NetzDG bereits nennenswerte Anstrengungen und Investitionen zur Einrichtung des Beschwerdemanagements und dessen Optimierung aufgewendet haben.

Aus der organisatorischen und technischen Umsetzung der Meldepflicht werden den Unternehmen weitere Kosten erwachsen. Damit der Meldeprozess innerhalb der gesetzlich vorgesehenen Frist umgesetzt werden kann, müssen weitere personelle Kapazitäten aufgebaut werden. Zur technischen Umsetzung muss eine durch das BKA definierte Schnittstelle eingerichtet werden, die mit weiteren Kosten für die Betreiber sozialer Netzwerke einhergehen.

Abschließend bleibt festzustellen, dass eine Meldepflicht für sich allein, nicht zur Eindämmung rechtsextremistischer und hasserfüllter Tendenzen im Internet führen wird. Vielmehr müssen die Behörden zur Täterermittlung und Strafverfolgung mit den notwendigen personellen und technischen Kapenazitäten und Kompetenzen ausgestattet sein, um effektiv gegen die Täter von Rechtsextremismus und Hasskriminalität im Internet vorgehen zu können.

5. Massenhafte Datenspeicherung beim BKA

Auf Basis der Meldepflicht werden binnen kürzester Zeit umfangreiche Datenbestände über die gemeldeten Inhalte und als tatverdächtig

identifizierte Nutzer sozialer Netzwerke beim Bundeskriminalamt (BKA) entstehen.

Der vorliegende Gesetzentwurf lässt jedoch keine Rückschlüsse zum weiteren Umgang mit den von den sozialen Netzwerken übermittelten Daten in Bezug auf deren Verarbeitung, Speicherung und Löschung durch das BKA zu. Es ist zwingend erforderlich, dass der Datenumgang durch das BKA vor Einführung der Meldepflicht in das NetzDG angemessen und rechtssicher normiert wird. Aus der aktuell unklaren Rechtslage entsteht ein enormes Risiko über den Umgang mit den massenhaft auflaufenden Datenmengen und darüber hinaus über die Befugnisse der Ermittlungsbehörde. Auch ist unklar, wie die aus der Meldepflicht erlangten Datensätze für weitere Ermittlungen verwendet und andere Delikte herangezogen werden dürfen.

Deshalb ist es zwingend notwendig, dass die Anforderungen an den Datenumgang und insbesondere an das Löschen der Datensätze umfassend und abschließend gesetzlich geregelt werden.

6. Rechtsstaatliche Sicherungs- und Kontrollmechanismen

Die mit dem Gesetzesentwurf vorgesehenen Maßnahmen zur Herausgabe von personenbezogenen und besonders sensiblen Daten wie z.B. Passwörter, Bestands- und Nutzungsdaten sind höchst fragwürdig.

Rechtsstaatlich gebotene Sicherungsmechanismen und Kontrollen – wie etwa ein Richtervorbehalt – sind im vorliegenden Entwurf nur unzureichend vorgesehen. Die mit der Herausgabe von Bestands- und Nutzungsdaten, Passwörtern, IP-Adressen und Portnummern verbundenen tiefgreifenden Eingriffe in die Grundrechte der Bürgerinnen und Bürger wie dem Fernmeldegeheimnis und dem allgemeinen Persönlichkeitsrecht, werden keiner ausreichenden rechtsstaatlichen Kontrolle unterworfen. Insbesondere im Bereich der Telemediendienste handelt es sich häufig um besonders sensible Daten. Derartige Informationen über die Nutzer von Telemediendienste können weitreichende Rückschlüsse auf politische, sexuelle, finanzielle oder sonstige persönliche Interessen ermöglichen. Das stellt einen massiven Eingriff dar. Die simple Übertragung ähnlich gelagerter Regelungen aus dem Telekommunikationsgesetz wird dem nicht gerecht, da mit einem Zugriff auf Telemediendienste wesentlich tiefere Eingriffe in die Privatsphäre erfolgen werden.

Die Hürden für solche Eingriffe müssen zwingend rechtsstaatlichen Sicherungs- und Kontrollmechanismen unterworfen werden, um den hohen Anforderungen des Datenschutzrechts und des Schutzes der Privatsphäre Rechnung zu tragen.

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.

Über eco
eco - Verband der Internetwirtschaft e.V. ist Interessenvertreter und Förderer aller Unternehmen, die mit oder im Internet wirtschaftliche Wertschöpfung betreiben. Der Verband vertritt derzeit mehr als 1.100 Mitgliedsunternehmen. Hierzu zählen unter anderem ISP (Internet Service Provider), Carrier, Hard- und Softwarelieferanten, Content- und Service-Anbieter sowie Kommunikationsunter-nehmen. eco ist der größte nationale Internet-Service-Provider-Verband Europas.