Anmerkungen zum RefE TKMoG (Stand 9. Dezember) als Ergänzung der Stellungnahme vom 20.11.2020 zum Diskussionsentwurf TKMoG[1] (Stand 6. November)

Berlin, 11. Dezember 2020

Am 9.12.2020 veröffentlichten das BMVI und BMWi einen gemeinsamen Referenten-Entwurf zur Modernisierung des Telekommunikationsgesetzes zur Beteiligung der Verbände und der Länder nach § 47 GGO der Bundesministerien. Damit soll auch der Europäische Kodex für elektronische Kommunikation umgesetzt werden. Das TKG-Gesetzgebungsverfahren wird daher den Rechtsrahmen für etwa ein Jahrzehnt vorgeben und ist daher von zentraler Bedeutung. Der Referenten-Entwurf ist weiterhin nicht final ressortabgestimmt. Die Frist zur Kommentierung beträgt etwas mehr als 48h – und dies bei einem Entwurfstext der 465 Seiten umfasst - und bei dem zahlreiche Änderungen und Ergänzungen gegenüber dem Diskussionsentwurf vom 6. November vorgenommen wurden. Vordringliches Ziel ist ein Kabinettsbeschluss des Referenten-Entwurfs (RefE) am 16.12.2020.

eco hat zu Kenntnis genommen, dass die federführenden Ministerien sich mit dem nunmehr vorliegenden Referenten-Entwurf bemüht haben, einen teilweise brauchbaren und soliden gemeinsamen Entwurf zu erstellen. Nichtsdestotrotz bestehen aber weiterhin zahlreiche Kritikpunkte. Bedauerlicherweise wurde der bisherige DiskE für IT-Sicherheitsgesetzes 2.0 überabeitet und zwischenzeitlich auch ein RefE vorgelegt (vom 09.12.2020). Dieser wurde im Rahmen einer eintägigen Verbändebeteiligung zur Konsultation gestellt wurde. Beide Entwürfe sollen zwar teilweise geplant zusammenwirken und ineinandergreifen, allerdings enthalten die Entwürfe dennoch unterschiedliche Vorschläge für denselben Regelungs-gegenstand. Dies trifft insbesondere auf den Bereich Öffentliche Sicherheit und Sicherheit der Netze zu. Für beide Gesetzesvorhaben muss daher konstatiert werden, dass die konkreten Verfahrensabläufe eine sach- und interessengerechte Beteiligung mit entsprechender Würdigung und Abwägung nahezu unmöglich machen.

eco kann in der Kürze der gewährten Frist für die Verbändebeteiligung daher ausschließlich ergänzend zu seiner Stellungnahme zum DiskE ausführen. Vor diesem Hintergrund wird sich eco in seiner Kommentierung im Wesentlichen auf die umfangreichen Änderungen durch den RefE im Bereich Öffentliche Sicherheit und Resilienz der Netze fokussieren. Die bereits geäußerte Kritik in der Stellungnahme erhalten wir aufrecht, u. a. hinsichtlich der unions-rechtswidrigen Regelung zum Messtool der BNetzA nach § 55 Abs. 4, welche die Exkulpa-tionsmöglichkeit der Anbieter nach zwingendem EU-Recht nicht enthält. Das gilt auch für die

[1] Im Folgenden sind Normen ohne Gesetzesangabe solche des Artikel 1 des RefE TKMoG. Der Diskussionsentwurf TKMoG vom 06.11.2020 wird als DiskE abgekürzt.

Vorschrift nach § 140 Abs. 3 S. 2 Nr. 4 (DigiNetzG), für dessen Änderung mangels Zeit seit In-Kraft-Treten keine Erforderlichkeit nachgewiesen worden sein kann und die dem Absatz 3 insgesamt den Zweck nimmt.

Öffentliche Sicherheit und Resilienz der Netze

Zu § 162 bzw. § 109 TKG-E in Artikel 2 des IT-SiG 2.0

Nach Ansicht des eco ist nicht nachvollziehbar, dass es innerhalb der Bundesregierung über einen Zeitraum von zwei Jahren nicht gelungen ist, sich zu verständigen und auf eine gemeinsame Fassung dieser Norm zu einigen. Der Hinweis des BMWi, dass hier nur Änderungen des IT-SiG 2.0 im Auftrag des BMI vollzogen würden, ist unzutreffend. Die Norm im Artikel 2 Nr. 1 des Entwurfs des IT-SiG 2.0, dort noch § 109, ist anders aufgebaut. Inhaltliche Änderungen lassen sich in der gewährten Zeit aufgrund der Komplexität des Regelungsgefüges nicht ausreichend nachvollziehen, da solche Änderungen auch aus der Systematik des gesamten Regelwerkes folgen können.

eco weist daraufhin, dass in Schweden eine 5G-Auktion verschoben wurde, da ein Hersteller im einstweiligen Rechtschutz vor dem Verwaltungsgericht Stockholm die Bedingungen, die eine Verwendung seiner Komponenten verboten hätten, vorläufig außer Vollzug setzen konnte, da dieses Verbot rechtswidrig ist. Die Auktion selbst hätte wegen dieser Gerichtsentscheidung nicht verschoben werden müssen. Die schwedische Regulierungsbehörde zog diese Verschiebung jedoch einer Auktion ohne Herstellerausschluss vor. Mit diesem Beispiel möchte eco deutlich machen, dass in Deutschland eine Verlagerung bestimmter Entscheidungen auf eine politische Ebene weiterhin die Erfüllung gewisser Tatbestandsmerkmale voraussetzt. So müssen bspw. sicherheitspolitische Belange betroffen sein. Das ist Ausfluss des Rechtstaatsprinzips. Die Frage, ob sicherheitspolitische Belange seitens der Ressorts belegt werden können, ist auch gerichtlich überprüfbar.

Zu § 162 Abs. 2 S. 3 – Schutzmaßnahmen und Stand der Technik

Nach der aktuellen Fassung von Satz 3 des § 162 Abs. 2 müssen nun alle nach Absatz 2 insgesamt zu ergreifenden Maßnahmen seitens der Unternehmen dem Stand der Technik entsprechen. Im Vergleich zum DiskE ist das neu hinsichtlich der Maßnahmen zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen (auch sofern diese Störungen durch äußere Angriffe und Einwirkungen von Katastrophen bedingt sein können), und bzgl. Maßnahmen zur Beherrschung der Risiken für die Sicherheit von Telekommunikationsnetzen und -diensten.

Normadressaten von Absatz 2 sind alle Betreiber öffentlicher TK-Netze und alle Anbieter öffentlich zugänglicher Telekommunikationsdienste. Hierzu zählen im Rahmen der mit dem Gesetzentwurf vorgesehenen einhergehenden deutlichen Ausweitung des Begriffs der Anbieter öffentlich zugänglicher Telekommunikationsdienste nun allerdings eine erheblich größere Anzahl von Unternehmen. Hierzu gehören insbesondere viele kleine und

mittelständische Unternehmen mit einem eingeschränkten Kundenkreis, welcher derartige Schutzmaßnahmen nicht ohne weiteres umsetzen können. Diese Ausweitung ist ohne geeignete, verhältnismäßigkeitswahrende Bagatellgrenzen rechtswidrig. eco spricht sich daher für geeignete und sachgerechte Bagatellgrenzen aus.

Zu § 162 Abs. 3 i. V. m. § 162 Abs. 2 – Angriffserkennungssysteme

Im Vergleich zum DiskE wurde folgender Satz gestrichen: „*Hierzu gehört auch der Einsatz von Systemen zur Angriffserkennung*." Stattdessen wurde für die Konkretisierung der darin enthaltenen Pflicht nun ein eigenständiger, mehrzeiliger neuer Absatz 3 in § 162 geschaffen. § 162 Abs. 3 S. 1 legt zunächst fest, dass als angemessene Maßnahme im Sinne des Absatzes 2 von § 162 Systeme zur Angriffserkennung eingesetzt werden können und es wird auf eine entsprechende Legaldefinition nach § 2 Abs. 9b BSIG-E (RefE IT-SiG 2.0, 9.12, 10.15Uhr) verwiesen. Danach sind „*Systeme zur Angriffserkennung im Sinne dieses Gesetzes durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten.*" In Satz 2 werden Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste mit erhöhtem Gefährdungspotential in jedem Fall verpflichtet Systeme nach Satz 1 einzusetzen. Im vorliegenden RefE wird damit erstmalig wird von Diensteanbietern mit einem erhöhtem Gefährdungspotential gesprochen. S. 3 stellt Anforderungen an die Angriffserkennungssysteme auf. S. 4 gibt den Unternehmen die Verpflichtung auf, relevante, nicht personenbezogene Daten für 4 Jahre zu speichern. Nach Satz 5 kann die BNetzA im Sicherheitskatalog weitere Einzelheiten festlegen.

Nach Ansicht des eco ist die Schaffung der neuen Kategorie von Dienste-Anbietern mit erhöhtem Gefährdungspotential in Satz 2 nicht akzeptabel und wird daher abgelehnt. Bisher war angedacht, dass im Bereich der Telekommunikation nur 5G-Mobilfiunknetzbetreiber als Unternehmen mit erhöhtem Gefährdungspotential gelten. Dieser Fokus war Gegenstand der bisherigen Diskussion. Mit dem nunmehr vorliegenden RefE bestätigen sich die Befürchtungen des eco, dass mittels der Allgemeinverfügung zum Sicherheitskatalog alle Unternehmen ohne Ansehung der tatsächlichen Gegebenheiten und ohne Differenzierungen sehr strengen Sicherheitsanforderungen unterworfen werden sollen. Letztlich wird es wohl auch verwaltungsgerichtliche Streitigkeiten erfordern, um klarzustellen, dass Normtexte, u. a. zur Wahrung des Verhältnismäßigkeitsprinzips, die realen Umstände erfassen müssen. Nach Einschätzung des eco wird sich eine nicht unerhebliche Anzahl an Unternehmen diese gerichtlichen Verfahren nicht leisten können. Nach Ansicht des eco wäre es äußerst bedauerlich, wenn es aufgrund einer verfassungswidrigen Regelung zu einer gesetzlich herbeigeführten Marktbereinigung käme.

Die Regelung des Satzes 3 i. V. m. S. 1 ist zu unbestimmt. Nach jetzigem Wortlaut ist nicht ausgeschlossen, dass auch der Datenverkehr der Kunden mittels der Angriffserkennungssysteme zu prüfen wäre. Dies würde eine Deep Packet Inspection dieser Daten darstellen und wäre datenschutzrechtlich nicht vertretbar. Die Gesetzesbegründung enthält hierzu keine Ausführungen. eco fordert daher eine ausdrückliche Präzisierung der gesetzlichen Regelung in Absatz 3 und ausdrückliche Klarstellung, dass die Angriffserkennungssysteme nur die nicht-öffentlichen Systeme der Verpflichteten prüfen.

Die Vorgabe in Satz 4, dass die Systeme automatisch erkannte Gefahren oder Bedrohungen abwenden und für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen, sind sowohl in der Anschaffung und Implementierung um ein Vielfaches teurer als solche zur Angriffserkennung und Warnung. Die Kosten der Implementierung steigen immens, da tief in die Netzwerkarchitektur eingegriffen werden müsste. Darüber hinaus entsteht doppelter Aktualisierungsbedarf, einmal hinsichtlich der Gefahrerkennung als auch hinsichtlich deren Beseitigung. Das erhöht die laufenden Kosten der Verpflichteten erheblich und dauerhaft. Nach Ansicht des eco ist hier eine tatbestandliche Begrenzung vorzunehmen, die als Voraussetzung für automatische Gefahrenbeseitigung an das tatsächliche Risiko, an das Ausmaß hinsichtlich Anzahl der Betroffenen und an die Auswirkungen des Angriffs anknüpft. Darüber hinaus muss im Tatbestand klargestellt werden, dass Kundensysteme bei automatischer Gefahr- und Bedrohungsabwendung oder Störungsbeseitigung nicht einbezogen sind. Dies kann für Kundensysteme technisch nicht geleistet werden, da in der Regel hier nur eine Sperrung/Filterung von Verkehren erfolgen kann und keine Beseitigungsmaßnahme vorgenommen werden kann. Darüber hinaus wäre ein solcher Eingriff in die Kundensysteme weder zulässig noch wird eine derartige Befugnis von den Unternehmen als sinnvoll erachtet.

Die Regelung in Satz 5 entspricht nicht dem Bestimmtheitsgebot, da unklar bleibt, was ist unter Daten, die für die Angriffserkennung und -Nachverfolgung relevant, aber keinen Personenbezug haben, zu verstehen. Auch die Begründung des Gesetzes enthält hierzu keine zielführenden Erläuterungen. Dies ist nachzuholen.

eco sieht Klarstellungsbedarf in Satz 2. Der Satz kann bisher so verstanden werden, dass auch Netzbetreiber ohne erhöhtes Gefährdungspotential grundsätzlich zum Einsatz von Angriffserkennungssystemen verpflichtet werden sollen. Sollte diese grundsätzliche Verpflichtung beabsichtigt gewesen sein, erachtet eco sie als unverhältnismäßig. eco schlägt daher zur Klarstellung als neuen Satz 2 vor: „*Verpflichtete nach Satz 1 mit erhöhtem Gefährdungspotential haben in jedem Fall entsprechende Systeme zur Angriffserkennung einzusetzen*.“

eco erkennt damit keineswegs die Erforderlichkeit der neuen Kategorie von Dienste-Anbietern mit erhöhtem Gefährdungspotential an.

eco erachtet die Vorgaben nach den Sätzen 1, 2, 3 und 4 auch insoweit für unangemessen, da auch mit der Ausweitung des Begriffs der Diensteanbieter ein viel größerer Kreis von Unternehmen erstmalig verpflichtet werden soll. Für alle Unternehmen werden die Angriffserkennungssysteme hohe Investitions-, Implementierungs- und Wartungskosten nach sich ziehen. Gleiches gilt hinsichtlich der Speicherverpflichtung für eine Dauer von vier Jahren.

Zu § 162 Abs. 4 – Kritische Komponenten und Zertifizierungspflicht

Deutlich zu kritisieren ist der Zirkelschluss, welcher der Regelung nach § 162 Abs. 4 i. V. m. § 2 Abs. 13 BSIG-E (RefE IT-SIG 2.0, 9.12, 10.15Uhr) innewohnt. Nach § 162 Abs. 4 dürfen kritische Komponenten im Sinne § 2 Abs. 13 BSIG-E nur eingesetzt werden, wenn sie von einer anerkannten Prüfstelle überprüft und von einer anerkannten Zertifizierungsstelle zertifiziert wurden. In § 2 Abs. 13 BSIG-E heißt es nun im Wesentlichen, kritische Komponenten im Sinne des BSI-Gesetzes seien solche, die entweder auf Grund Gesetzes als solche bestimmt werden oder auf Grund eines Gesetzes als kritische Funktionen realisierend bestimmt werden, aus denen nach dem Gesetz kritische Komponenten abgeleitet werden können. Das bedeutet schlicht, kritische Komponenten werden in Rechtsverordnungen, Allgemeinverfügungen oder anderen Verwaltungsakten festgelegt. Zugeschnitten ist insbesondere die zweite Variante mit den kritischen Funktionen auf den Listen-Entwurf der Bundesnetzagentur (veröffentlicht am 11.08.2020). Kurz ausgedrückt, TKG verweist auf BSIG, letzteres verweist auf die geplante Ermächtigung im TKG zur Bestimmung kritischen Funktionen nach § 164 Abs. 1 S. 1 Nr. 2 zurück im Sicherheitskatalog. Dieses Verweisungswerk ohne gesetzliche, einhegende Tatbestandsmerkmale entspricht nicht dem Bestimmtheitsgebot. Vor allem verletzt die Regelung die Wesentlichkeitstheorie massiv. Denn damit sind viele, intensive Eingriffe verbunden, wie die Meldepflicht einzelner Komponenten vor Einbau, der Untersagungsvorbehalt, die Rückbaupflicht oder die Auditierungspflicht im Zwei-Jahres-Intervall zusätzlich zu Überprüfungen durch BNetzA.

Daher obliegt die Festlegung, was als kritische Komponenten und kritische Funktionen gelten soll, auch im Bereich Telekommunikation allein dem parlamentarischen Gesetzgeber.

eco ist bewusst, dass es dem Gesetzgeber hier gerade darauf ankommt, bzgl. der absehbaren Dauer des Verfahrens der Exekutive die Entscheidungsbefugnis zuzuweisen. Das steht dem Gesetzgeber indes nicht frei, wenn er plant, derart tief in die Grundrechte der betroffenen Unternehmen einzugreifen:

- in das Recht auf Berufsausübung nach Art. 12 Abs. 1 GG i. V. m. Art. 19 Abs. 4 GG,
- in das Recht am eingerichteten und ausgeübten Gewerbebetrieb nach Art. 14 Abs. 1 i. V. m. Art. 19 Abs. 4 GG,
- in das Recht auf Eigentum nach Art. 14 Abs. 1 i. V. m. Art. 19 Abs. 4 GG,
- sowie in das Recht der unternehmerischen Freiheit gem. Art 16 EU-Grundrechte-Charta.

Als Ausgleich für diese Eingriffsintensität gebietet die Wesentlichkeitstheorie und der Gesetzesvorbehalt die Entscheidung durch das Parlament, unter Abwägung der widerstreitenden Interessen. Eine solche Abwägung im Rahmen einer parlamentarischen Debatte braucht auch eine angemessene Zeit.

Nach Auffassung des eco ist zudem dringend geboten, dass die Kriterien erhöhtes Gefährdungspotential und kritische Komponente kumulativ vorliegen müssen, damit eine Zertifizierungspflicht entsteht. Unternehmen, die kein erhöhtes Gefährdungspotential aufweisen, dürfen keiner Zertifizierungspflichten unterworfen werden. Dies wäre unverhältnismäßig.

Der Vollständigkeit halber weisen wir darauf hin, dass auch der o. g. Listen-Entwurf der BNetzA seitens eco kommentiert wurde. Darin unsere Einschätzung ausführlich dargelegt und festgestellt, dass es unter anderem für diese Liste derzeit im TKG keine Rechtsgrundlage gibt. Die Formulierung in § 164 Abs. 1 stellt nun eine passende Grundlage bereit, ist aber noch de lege ferenda. Bis zum 09.12.2020 ist diese Liste weder im Amtsblatt noch auf den Webseiten der BNetzA veröffentlicht worden.

Zu § 167 Abs. 2 – Umsetzung von Überwachungsmaßnahmen, Erteilung von Auskünften sowie Art. 39 – Änderungen der Telekommunikations-Überwachungsverordnung (TKÜV)

In § 167 Abs. 2 Nr. 2 lit. b) wird der vormals verwendete Begriff des "Teilnehmers" durch den Begriff des "Nutzers" ersetzt. Nach der Gesetzesbegründung soll es sich insoweit lediglich um redaktionelle Änderungen handeln. Bei den ebenfalls geplanten Änderungen der TKÜV soll es sich ausweislich der Entwurfsbegründung um Folgeänderungen zu den geplanten Änderungen der sicherheitsrechtlichen Vorschriften des TKG handeln.

Nach Ansicht des eco sind die damit verbundenen Auswirkungen und Konsequenzen nicht hinreichend bedacht worden. Denn die Ersetzung des Begriffs "Teilnehmer" durch "Nutzer" u.a. in der Ausnahmevorschrift des § 3 Abs. 2 Nr. 5 TKÜV, kann jedoch zu einer erheblichen Ausweitung der Verpflichtung zur Implementierung technischer und organisatorischer Umsetzung von Maßnahmen zur Überwachung der Telekommunikation führen. Würde im Rahmen der Ausnahmevorschrift nicht mehr auf die Anzahl der Teilnehmer (d. h. der Kunden, mit denen der Anbieter unmittelbar einen Vertrag über die Bereitstellung von Telekommunikationsdiensten unterhält), sondern auf den "Nutzer" abgestellt, so kommt es im Hinblick auf Anwendbarkeit der Ausnahmeregelung des § 3 Abs. 2 Nr. 5 TKÜV im Ergebnis darauf an, wie vielen weiteren Personen der Vertragspartner die entsprechenden Dienste letztendlich zugänglich macht. Hierauf hat der Anbieter in den meisten Fällen jedoch keinen Einfluss und daher keine ausreichend gesicherte Kenntnis von der Nutzerzahl. Denn dies hängt davon ab, in welchem Umfang Teilnehmer die bereitgestellten Dienste anderen Personen zur Nutzung überlassen. Die Anbieterverpflichtungen würden daher von

Umständen anhängig gemacht werden, die nicht aus der Sphäre des Anbieters resultieren. Nach Ansicht des eco ist es daher sachgerecht, die Formulierungen "Teilnehmer" bzw. "Teilnehmer oder anderer Endnutzer" beizubehalten und nicht durch den Begriff "Nutzer" zu ersetzen.

Zu § 170 – Automatisiertes Auskunftsverfahren

eco hält es für erforderlich und geboten, dass der Gesetzgeber im Rahmen des Gesetzgebungsverfahrens den Beschluss des Bundesverfassungsgerichts zur manuellen Bestandsdatenauskunft (1 BVR 1873/13) auch zum Anlass nimmt, die Norm zum automatisierten Auskunftsverfahren gem. §170 auf deren Verfassungskonformität zu überprüfen. Nach Ansicht des eco betrifft dies die Norm des § 170 TKG insgesamt, insbesondere auch dessen Absatz 2. Nach dem Beschluss des BVerfG muss der Gesetzgeber bei den Übermittlungsregelungen für Bestandsdaten von Telekommunikations-diensteanbietern die Verwendungszwecke der Daten hinreichend begrenzen. Die Datenverwendung muss durch den Gesetzgeber an bestimmte Zwecke, tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz gebunden werden. Bereits dem Gesetzgeber der Übermittlungsregelung hat die normenklare Begrenzung der Zwecke der möglichen Datenverwendung gesetzlich zu regeln. Diese Vorgaben des BVerfG treffen nach Ansicht des eco erst recht auf das automatisierte Auskunftsverfahren zu.

In der praktischen Relevanz hat das AAV nach § 112 TKG in den vergangenen Jahren zunehmend an Bedeutung für die Beauskunftung gewonnen, und es stellt das quantitativ am häufigsten genutzte Instrument von Datenabfragen dar. Zudem stehen seit der letzten Aktualisierung der Technischen Richtlinie, welche das AAV nach § 112 TKG in seinen technischen Einzelheiten ausgestaltet, mehr Datenkategorien für den automatisierten Abruf zur Verfügung. Daneben wurden die Suchmöglichkeiten für die Behörden anhand verschiedener Parameter, etwa unter Verwendung sogenannter Wildcards oder verkürzten Suchangaben, erweitert.

Schließlich werden nach § 112 Abs. 5 S. 3 TKG den verpflichteten Unternehmen keine Entschädigungen oder Vergütungen für erteilte Auskunft gewährt, was moderierend auf die bereits heute ausufernde Anzahl der Auskunftsersuchen wirken könnte.

Diese Regelung soll jedoch unverändert beibehalten werden.

In der Praxis ist bereits zu beobachten, dass das manuelle Auskunftsverfahren nur noch bei Unklarheiten zum Einsatz kommt, oder wenn es um spezielle Datenarten wie beispielsweise eine Zuordnung von IP-Adressen zu Kundendaten geht, die im AAV nicht beauskunftet werden.

Im Gesetzentwurf zur Anpassung der Bestandsdatenauskunft hat das BMI zumindest die Abrufregelungen für die 19 deutschen Nachrichtendienste in dem Sinne qualifiziert, als das „tatsächliche Anhaltspunkte im Einzelfall“ vorliegen müssen. Offen bleibt aber, warum der Gesetzgeber bei den Regelungen für die deutschen Nachrichtendienste dem Erfordernis der

Doppeltür Rechnung trägt, nicht aber in den übrigen Abrufregelungen oder wie im Rahmen des RefE bei dem automatisierten Verfahren.

Somit bleibt unklar, unter welchen konkreten Voraussetzungen Daten im Bereich der Strafverfolgung und polizeilichen Gefahrenabwehr automatisiert abgerufen werden dürfen. Angesichts der mittlerweile hohen Praxisrelevanz des AAV erachtet eco diesen Zustand für äußerst bedenklich.

eco fordert deshalb eine gleichlaufende Anpassung der Verfahrensarten, in welcher auch Abrufe im automatisierten Auskunftsverfahren hinsichtlich Strafverfolgung und allgemeiner Gefahrenabwehr konkreten und ausdrücklich formulierten Voraussetzungen unterworfen werden, wie sie für den Bereich der manuellen Bestandsdatenauskunft bereits durch die Entscheidung des Bundesverfassungsgerichts vorgegeben werden.

Zu § 171 Abs. 7 S. 2 – Manuelles Auskunftsverfahren

Die grundsätzliche Ausweitung der Verpflichtung der Vorhaltung einer elektronischen Schnittstelle auf Unternehmen, die mit dem RefE in der Vorschrift zukünftig verwendeten Begriff Nutzer (anstatt wie bisher Kunden, also die direkten Vertragspartner) ab einer Anzahl von 100.000 ist nicht sachgerecht und führt gerade im Geschäftskundenbereich zu praktischen Umsetzungsschwierigkeiten. Hier besteht nach Ansicht des eco Anpassungsbedarf und es sollte zur ursprünglichen Regelung, die auf die Kunden abstellt, zurückgekehrt werden.

Zu §182 - Telekommunikationssicherstellungspflicht

Die aus dem PTSG übernommenen Regelungen entstanden vor dem Jahr 2000 und treffen auf die aktuelle Sachlage nicht mehr zu. Die Normen sind deswegen sowohl hinsichtlich des Anwendungsbereiches, der Adressaten sowie dem Stand der Technik anzupassen. Der zugrunde gelegte Schwellenwert von 100.000 ist deutlich zu niedrig. Die Anzahl der Anschlüsse (oft mehrere pro Person) hat sich seitdem vervielfacht, der durchschnittliche Umsatz pro Kunden bei den einzelnen Anbietern dagegen erheblich gesunken ist. Der Marktanteil ist mit 100.000 Kunden heute sehr klein. Der Wegfall eines Anschlusses oder eines Dienstes ist für den Einzelnen sehr leicht kompensierbar. Die Belastungen, die mit den Pflichten der §§ 181 ff TKG einhergehen, überfordern kleinere Anbieter. Die Grenze müsste nach heutigen Maßstäben über 3.000.000 Nutzern liegen.

Zu § 183 – Telekommunikationsbevorrechtigung

Die neue Regelung in Abs. 1 Nr. 2 hinsichtlich Bandbreiten von Übertragungswegen ist abzulehnen, denn diese Forderung ist gerade im Sicherstellungsfall in der Krise überhaupt nicht zu leisten. Denn eine Steigerung der Bandbreite ist technisch unmöglich, wenn der Anschluss diese Bandbreite nicht von Anfang an erbringen kann. Zudem bedeutet eine

höhere Bandbreite regelmäßig eine andere Technik, auf die im Krisenfall nicht einfach umgerüstet werden kann. Eine solche Umrüstung ist ein Aliud gegenüber einer Erweiterung, von der aber die Gesetzesbegründung ausgeht: "Absatz 1 wird um die Verpflichtung zur unverzüglichen und vorrangigen Erweiterung der Datenübertragungsraten von bestehenden Anschlüssen erweitert. Dadurch wird die Arbeitsfähigkeit Telekommunikationsbevorrechtigten im Krisenfall geschützt." Tatsächlich handelt es sich dabei in der praktischen Umsetzung nicht um eine Sicherstellung oder Bevorrechtigung der bestehenden Anschlüsse. Vielmehr würde es sich dabei faktisch um eine Neuschaltung auf Zuruf handeln.

Erhöhung von Zwangs- und Bußgeldern

eco hält eine regelmäßig stattfindende Evaluierung der Wirksamkeit der Zwangsmittel und Sanktionsmöglichkeiten, welche der Bundesnetzagentur zur Verfügung stehen, für sinnvoll. Dies wäre eine geeignete Tatsachengrundlage, um überhaupt eine Erforderlichkeit für die vorgesehene Erhöhung der Zwangs- und Bußgelder zu belegen. Dies fehlt im Gesetzesentwurf. So kann nicht festgestellt werden, ob Zwangs- und Bußgelder ihren Zweck nicht bereits erfüllen. Vor diesem Hintergrund ist die geplante Erhöhung der Zwangs- und Bußgelder gegenwärtig unangemessen.

Umsetzungsfristen

eco fordert die Bundesregierung auf, sich bei der EU-Kommission, im Rat der EU und dem Europäischen Parlament für längere Umsetzungsfristen hinsichtlich der vom EECC vorgegebenen Normen, die Umstellungs- und Implementierungsprozesse nach sich ziehen, von mindestens 18 Monaten nach In-Kraft-Treten des TKMoG einzusetzen. Dies ist erforderlich und verfassungsrechtlich geboten, vgl. BVerfG, Urteil v. 4. Mai 2012, Az. 1 BvR 367/12.

Zusammenfassung

eco sieht erheblichen Nachbesserungsbedarf an dem vorliegenden Referenten-Entwurf.

Die geplante Verschränkung von TKG, BSI-Gesetz und jeweils darauf beruhenden Allgemeinverfügungen (Sicherheitskatalog, Liste kritischer Funktionen, technische Richtlinie des BSI zur Zertifizierung kritischer Komponenten, Allgemeinverfügung des BMI zu Einzelheiten der Garantie-Erklärung) regelt diesen Themenbereich überkomplex und ist für die betroffenen Unternehmen nicht mehr nachvollziehbar.

Durch das Fehlen relevanter Regelungsbereiche fehlt den betroffenen Unternehmen zudem die erforderliche Rechts- und Planungssicherheit, was Investitionen hemmt und den Ausbau verzögert.

eco sieht sich durch § 162 Abs. 3 darin bestätigt, dass zu besorgen ist, dass die besonders strengen Sicherheitsanforderungen welche derzeit nur für 5G- Mobilfunkanbieter gelten sollen, im Wege der Änderung der bestehenden und zukünftigen Allgemeinverfügungen auf einen deutlich größeren Adressatenkreisausgedehnt werden sollen.

Dies wird von eco äußerst kritisch beurteilt und daher abgelehnt. Diese Herangehensweise verletzt den Parlamentsvorbehalt, und ist weder interessen- noch sachgerecht. Zudem wäre eine solche Ausdehnung des Adressatenkreises unverhältnismäßig.

Im Bereich Öffentliche Sicherheit muss zur Wahrung der Angemessenheit der Kreis der Verpflichteten tatbestandlich eingegrenzt werden. Die in dem Entwurf enthaltene undifferenzierte Herangehensweise ist nicht nachvollziehbar. Es werden wesentlich ungleiche Diensteanbieter gleich behandelt, ohne Vorliegen einer sachlichen Rechtfertigung.

Weiterhin ist es nach Ansicht des eco zwingend erforderlich an mehreren Stellen angemessene und praktikable Bagatellgrenzen vorzusehen.
