Deutscher Bundestag
19. Wahlperiode
Ausschuss für Wirtschaft und Energie

Ausschussdrucksache 19(9)980(neu)
26. Februar 2021

An den
Ausschuss für Wirtschaft und Energie
des Deutschen Bundestages

Stellungnahme zum GE des TKModG-E zum 1. März 2020

Sehr geehrte Damen und Herren,

seit nunmehr über 30 Jahren sind wir mit unserer Hosting-Sparte und unseren eigenen E-Mail-Anbietern „jpberlin.de“ und „mailbox.org“ am Markt.

In unserem Geschäftsbereich IT-Consulting haben wir uns auf Aufbau und Betrieb von E-Mail-Anbietern aller Größenordnungen spezialisiert und betreuen Provider, Unternehmen, Universitäten und natürlich auch die öffentlich-rechtliche Hand in allen Fachfragen rund um den sicheren Mailbetrieb.

Wir freuen und bedanken uns, wenn wir mit unserem langjährigen Erfahrungsschatz und mit dieser Stellungnahme zum Diskussionsprozess rund um das TKModG beitragen können.

Mit freundlichen Grüßen und Dank für Ihre Aufmerksamkeit

[redacted]
Peer Heinlein
Geschäftsführung

mailbox.org

https://mailbox.org
presse@mailbox.org

eine Marke der
Heinlein Support GmbH
Schwedter Str. 8/9b
10119 Berlin

[redacted]
Geschäftsführung: Peer Heinlein
Amtsgericht Berlin-Charlottenburg
HRB 93818 B

[redacted]

1) Allgemein zur Erweiterung vom „Teilnehmer“ zum „Nutzer“-Begriff

Das bisherige TKG kennt an verschiedenen Stellen wie beispielsweise §113 (5) TKG die Grenze 100.000 „Kunden“ (woanders auch: „Teilnehmern“), was in den vergangenen Jahren im Sinne von „Vertragspartner“ verstanden wurde. So wurde ein Geschäftskunde auch dann als „ein Kunde/Teilnehmer“ gewertet, wenn er für mehrere Tausend Mitarbeiter E-Mail-Konten einrichtete.

Im TKModG-E wurde dieser Begriff überraschenderweise durchgehend durch den Begriff des „Nutzers“ ersetzt, was nun bedeutet, dass jede E-Mail-Adresse einzeln gezählt werden würde im Sinne von „schlagende Herzen“.

In der Praxis sorgt dies auch für erhebliche (Rechts-)Unsicherheit:

- Wenn ein Nutzer A des Providers 1 einem Nutzer B bei einem anderen Provider 2 eine E-Mail schreibt, so „nutzen“ zwar defacto zwei Personen die Leistungen des Providers A, doch wird dies dem Provider A sicherlich noch als „ein Nutzer“ zugerechnet werden.

- Anders könnte es sein, wenn Nutzer A@provider1 dem Nutzer B@provider2 eine verschlüsselte E-Mail zusendet. Dies kann nativ als PGP-verschlüsselte E-Mail erfolgen, doch existieren auch Systeme, wo Provider1 die fragliche E-Mail nicht versendet, sondern lokal speichert und stattdessen einen https-Link zum Login in ein für Nutzer B angelegtes Gastpostfach versendet. B loggt sich dann für den Mailabruf als Gast in die Systeme von Provider1 ein und ist den Systemen von Provider 1 gegenüber auch über eine (Gast-)Nutzerkennung identifiziert. Im Folgenden kann ein Mailwechsel zwischen A und B stattfinden, der sich gänzlich innerhalb des Providers 1 abspielt. In diesem Fall müsste konsequenterweise auch B als Nutzer des Providers1 zugerechnet werden. Da am Ende nicht kalkuliert werden kann, wie viele Kontakte in welchen Nutzungsarten ein Nutzer A entwickeln wird, hätten Provider 1 und auch die Bundesnetzagentur gar keine saubere Grundlage zu entscheiden, ob Provider 1 die Grenze von 100.000 Nutzern erreicht hat, oder nicht.

- Mailinglisten sind nicht nur reine Adressbuch-Mailverteiler, sondern können von allen Nutzern einer Mailingliste auch aktiv angeschrieben werden, damit diese E-Mails an alle Teilnehmer der Liste verteilt werden. Bislang war es Nutzer A, der mit seinem Account als Teilnehmer juristisch hinter einer Mailingliste mit vielen Zehntausend Empfängern stand. Sollen nach dem neuen Nutzer-Begriff nun mehrere Zehntausend Nutzer anderer Provider dem Mailinglistenprovider als Nutzer zugerechnet werden?

- Manche Mailinglisten umfassen mehrere Hunderttausend Teilnehmer – schon mit einer einzigen solchen Liste würde der Provider den neuen Nutzer-Begriff des neuen TKModG-E erfüllen. Und woher soll der Provider bei Vertragsschluss wissen, ob ein Nutzer über Nacht Verteiler mit mehreren Zehn- oder Hunderttausend Nutzern anlegt? Für die Provider entstehen auch hier völlig intransparente, nicht berechenbare und kaum vorhersehbare Situationen.

2) Zu den politisch, gesellschaftlich und wirtschaftlichen Auswirkungen der Überwachungsmaßnahmen und der Bedeutung der „digitalen Souveränität“

Insbesonders die im TKModG-E vorgesehenen Regelungen zur Telekommunikationsüberwachung (TKÜ) und Auskunftsverfahren (§§169,171 TKModG-E), die Regelungen zur Notfallvorsorge (§§ 183ff. TKModG-E) und auch die Regelungen zur Bestandsdatenerhebung wirken sich in sehr vielschichtiger Weise aus.

2.1) Wettbewerblich/wirtschaftlich:

Verglichen mit anderen europäischen Ländern zeichnet sich der deutsche Internet-Markt als erfreulich dezentral aus und kann eine Vielzahl auch kleiner und mittlerer Provider aufweisen. Gerade im E-Mail-Sektor konzentrieren sich –anders als in anderen Ländern – die Postfächer der Bürger nicht nur auf wenige oligopole beherrschende Anbieter.

Dabei haben sich gerade im Bereich der sicheren, datenschützenden E-Mail-Kommunikation in Deutschland eine Vielzahl innovativer Startups und kleinerer Unternehmen wie beispielsweise Tutanota, mail.de oder mailbox.org hervorgetan. Diese sind unter dem Motto „sichere Kommunikation und Datenschutz aus Deutschland“ auch international erfolgreich und verzeichnen eine hohe Bekanntheit und überdurchschnittliche Wachstumsraten. Der hohe deutsche Datenschutzstandard ist hier ein ausdrücklicher Wettbewerbsvorteil.

Innenpolitisch bewirkt diese dezentrale Kommunikationsstruktur durch Resilienz, Unabhängigkeit und Innovation die auch von der Bundesregierung ausdrücklich und immer wieder erwünschte „digitale Souveränität“, mit der sich Deutschland selbst von Oligopolen und ausländischen (i.d.R. US-basierten) Anbietern durch eigene Lösungsanbieter unabhängig macht.

Doch: Die vorliegende Regelung des TKModG-E verpflichtet lediglich deutsche Provider zu Umsetzungen von Maßnahmen wie in den §§169,171,172 TKModG-E. Dies ist ein eklatanter Nachteil im europäischen wie auch weltweiten Wettbewerb:

- Im Bereich Marketing und Martkpositionierung, denn Datenschutz und Datensparsamkeit ist heutzutage ein ganz wesentliches wettbewerbliches Unterscheidungsmerkmal.

- Und auch in wirtschaftlicher Hinsicht, denn die Kosten der daraus entstehenden Maßnahmen sind vom Anbieter selbst zu tragen und sind defacto gerade für kleine Anbieter so hoch, dass eine konkrete Ungleichbehandlung gegenüber ausländischen Mitbewerbern entsteht.

Dies gilt insbesondere unter dem Gesichtspunkt, dass alle anderen Anbieter aus dem Ausland heraus beliebig in Deutschland anbieten können und wirtschaftlich tätig sein können.

2.2) Politisch:

Mit dem Verlust des Vertrauens in die Sicherheit der Kommunikation bei deutschen Anbietern, werden Nutzer aller Bereiche zu Anbietern im EU- oder gar weltweiten Ausland gedrängt, wenn diese sich der Eingriffe in ihre Gedanken- und Meinungsfreiheit durch Auskunfts- und Überwachungsmaßnahmen erwehren wollen und kein ausreichendes Vertrauen, in die Rechtsstaatlichkeit der Auskunfts- und Überwachungsmaßnahmen entwickeln.

- Selbst wenn ein Teil dieser Nutzer zu ebenso mittelständischen Anbietern im Ausland abwandert, unterliegen diese Daten dort nicht mehr dem hohen Datenschutzstandard wie in Deutschland, mit dem sie der Staat eigentlich schützen wollte.

- Es ist ebenso zu befürchten, dass ein relevanter anderer Teil der Nutzer getreu dem Motto „wenn das so ist, dann kann ich auch gleich bei Google bleiben" ebenso im Ausland bleiben oder dorthin abwandern wird – dann jedoch zu den bekannten oligopolen US-basierten Global Playern, was ebenfalls kaum im Sinne einer digitalen Souveränität Deutschlands sein kann.

Der Gesetzesentwurf verspielt die Wettbewerbsfähigkeit Deutschlands und torpediert die IT-Strategie der „digitalen Souveränität" der Bundesregierung.

2.3) Gesellschaftlich:

Vorweg ist festzuhalten, das auch ich das Internet keinesfalls als rechtsfreien Raum verstehe oder gar verstehen möchte und strafrechtliche Ermittlungen bei gegebenem Anlaß ausdrücklich zu begrüßen sind.

Präventiv vorzuhaltende Maßnahmen wie die des §169 TKModG-E bedeuten in der Wahrnehmung der Bürger immer zugleich einen schweren Eingriff in die Gedanken- und Meinungsfreiheit und die Vertraulichkeit der Kommunikation. Und gerade die deutsche Geschichte zeigt deutlich, dass dabei schon das Wissen um die Existenz solche Maßnahmen und Möglichkeiten als Bedrohung und Einschränkung wahrgenommen werden kann, die per se zu Verhaltensänderungen und damit Einschränkungen führen kann.

Dies zeigt sich beispielhaft auch in der Wahrnehmung der sogenannten „Kryptobox" („SINA-Box") aus der TR TKÜV, die zwar sicherlich nur als VPN-Gateway dient, in der Wahrnehmung der Bürger jedoch großflächig als „Überwachungsinfrastruktur" verstanden wird. Dies ist gegenüber der SINA-Box so in dieser Härte sicherlich falsch und wird der technischen Funktion nicht gerecht, ändert jedoch nichts an der über Jahre so entstandenen Wahrnehmung.

Es kommt im Einzelfall also gar nicht unbedingt auf den tatsächlichen Einsatz an. Das öffentliche Bewußtsein um diese Sachverhalte ist bereits geeignet, das Vertrauen der Bürger in „ihren" Rechtsstaat zu erschüttern. Dies ist für uns als Provider durch regelmäßige Anfragen von Nutzern, Diskussionen im Userforum oder anderen öffentlichen Diskussionen deutlich spürbar und wirkt sich real aus.

Die im TKModG-E vorgesehen massiven Aufweichungen u.a. in den §173 (7) TKModG-E sind sicherlich geeignet, hier weiter Öl ins Feuer zu gießen.

2.4) Historisch:

Es sollte stets bedacht werden, dass auch gut gemeinte Kontroll- und Überwachungsschnittstellen langfristig missbraucht werden könnten. Was einmal technisch implementiert und in der Fläche ausgerollt ist, ist so schnell nicht wieder abzuschaffen.

Im Rahmen einer Kosten-Nutzen-Rechnung muss berücksichtigt werden, wohin sich diese Technik und Schnittstellen entwickeln könnten, wenn demokratiefeindliche Kräfte in die Regierungsverantwortung kommen könnten. Was einmal etabliert ist, ist dauerhaft vorhanden und leicht per zukünftiger Gesetzgebung zu missbrauchen.

Umso mehr ein Argument, als dass sich die Bundesregierung zur Sicherstellung der Rechte und Werte unserer Verfassung um eine möglichst dezentrale, nicht staatlich kontrollierbare robuste Kommunikationsinfrastruktur bemühen und diese ausdrücklich fördern sollte, statt sie zu belasten oder gar zu riskieren.

Dies gilt umso mehr wenn man feststellen muss, dass öffentliches Recht, Ordnung und Strafverfolgung auch im Internet (auch) auf anderem Wege (mindestens) ebenso erfolgreich zu erreichen ist.

Die dazu notwendigen Evaluierungen sind überfällig und meines Erachtens nach notwendige Grundlage für die Entscheidung, derart einschneidende und ggf. langfristig auch politisch-gesellschaftlich unerwünschte Maßnahmen vorzunehmen.

mailbox.org

https://mailbox.org
presse@mailbox.org

eine Marke der
Heinlein Support GmbH
Schwedter Str. 8/9b
10119 Berlin

[redacted]
Geschäftsführung: Peer Heinlein
Amtsgericht Berlin-Charlottenburg
HRB 93818 B

[redacted]

3) Zum Nutzen der Auskunftsverfahren und TKÜs

Auch in dem jüngsten vom Anbieter mailbox.org vorgestellten Transparenzbericht zu Zahl und Verteilung der Auskunftsersuchen im Jahr 2020 mussten wir wieder feststellen: 43 von 85 Auskunftsersuchen (also über 50%) erfolgten fehlerhaft und mussten von uns als rechtswidrig zurückgewiesen werden.

Spannend dabei: Von den 43 zurückgewiesenen Abfragen wurden nur 20 erneut in einer korrekten Art und Weise gestellt.

Im Umkehrschluss heißt das: Bei 23 Anfragen (also rund 25%) war die Auskunftsanfrage der anfragenden Stelle nicht wichtig genug, als dass sie sich der Mühe gemacht hätte, ein korrektes erneutes Auskunftsersuchen zu stellen. Es drängt sich der Eindruck auf, dass die Anfragen nicht mit dem notwendigen Maß an Zurückhaltung erfolgten, sondern im Zweifel zu leichtfertig und damit ggf. auch ohne tatsächliche Notwendigkeit gestellt wurden.

Gleichzeitig zeigen diese Zahlen, wie wichtig eine Kontrolle durch die Rechtsabteilung des Providers ist und wie wenig man hier auf die Rechtmäßigkeit der Ermittlungsbehörden vertrauen kann.

Nach konkreter Einschätzung aller uns vorliegenden Anfragen der letzten Jahre müssen wir zu dem Schluß kommen, dass vermutlich in kaum einen – oder gar keinem? – Fall ein sinnvoller Beitrag zum Ermittlungsverfahren erzielt werden konnte. Dies ergibt sich u.a. aus der erkennbaren Sinnlosigkeit der gefundenen und übermittelten Daten, soweit wir diese (unfreiwillig) durch Ausdruck und Faxübersendung an die anfragende Stelle zur Kenntnis nehmen mussten bzw. soweit ich als Gutachter vor Gericht mit diesen Daten in Berührung gekommen bin.

- Sofern es sich um „geplante schwerer Kriminalität“ handelte (Betrug, Phishing, Einsatz von Erpressungs-Trojanern, Waffenhandel), konnten zudem in keinem mir präsenten Fall sinnvolle Nutzer- oder Verkehrsdaten ermittelt werden. Professionelle Täter setzten in jedem einzelnen Fall auf gefälschte Nutzerangaben und verschleierten ihre eigenen IP-Adressen, beispielsweise durch den Einsatz von Anonymisierungsnetzwerken wie TOR.

- Allenfalls bei einer jährlich einstelligen Anzahl von „privaten Delikten“ (Beleidigung) konnten vermutlich in seltenen Fällen sinnvoll erscheinende Nutzerdaten übermittelt werden.

Dies heißt unserer Ansicht nach vor allem, dass diese Methoden zur Ermittlung im Bereich geplanter schwerer Kriminalität kaum geeignet sind.

Demgegenüber steht jedoch der permanente Eingriff in die geschützte Kommunikation der Bürger, die sich schon alleine durch die Möglichkeit eines solchen Eingriffs äußert und darum bereits durch ihre abstrakte Existenz einen Eingriff darstellt, selbst dann, wenn er nicht tatsächlich ausgeübt wird.

4) Automatisierte Auskunfts-/Überwachungsverfahren (§§169ff. TKModG-E, TR TKÜV)

§§169ff TKModG-E verpflichtet die Telekommunikationsanbieter zur Vorhaltung einer durch eine technische Richtlinie TR TKÜV der Bundesnetzagentur präventiv installierten Überwachungsschnittstelle.

- *Anmerkung: Die TR TKÜV kennt in §3 Nr. 6 eine eigene Definition von „100.000 Teilnehmern". Die folgenden Ausführungen unterstellen, dass in der Folge der Aufweichung des Teilnehmerbegriffs hin zu einem Nutzerbegriff, auch eine analoge Anpassung des §3 TR Nr. 6 TR TKÜV zu befürchten ist.*

4.1) Anhebung der Voraussetzungen des §173 (7) TKModG-E

Auch wenn die Lizenz- und Gerätepreise in den letzten Jahren deutlich gefallen sind, rechnen wir für Lizenzierung, Inbetriebnahme, Schulung, Wartung, Personalkosten, Netzwerkanbindung, Dokumentation und Schulung mit einem initialen betriebswirtschaftlichen Aufwand von rund 75.000 bis 100.000 € im ersten Jahr.

Die Kosten dieser technischen Maßnahmen sind dabei ausdrücklich vom Telekommunikationsanbieter zu tragen, was zweifelhaft anmutet, wenn es sich um die öffentliche Aufgabe des Staates handelt und diese Vorrichtungen alleine als Ermittlungswerkzeug für Polizei und andere befugte Stellen dienen sollen.

Schon mit der bisherigen Definition der „100.000 Teilnehmer" nach §113 (5) TKG stellten die initialen Kosten und personellen Aufwände einer solchen Vorrichtung ein erhebliches marktbeschränkendes Instrument für kleine und mittlere Unternehmen dar – zumal gerade im Bereich „E-Mail-Services" nur mit sehr geringen Umsätzen und Gewinnmargen gewirtschaftet wird und viele Anbieter mit kostenlosen, werbefinanzierten Angeboten auf dem Markt sind.

Wird mit der neuen Formulierung von „100.000 Nutzern" nach §173 (7) TKModG-E die Grenze erneut quasi beliebig nach unten abgesenkt, wird sich dies als spürbare Marktzugangsbeschränkung auswirken, Innovationen und Startups verhindern und damit die digitale Souveränität, aber auch Wettbewerbsfähigkeit Deutschlands schädigen.

Setzt man

- den Kosten und Aufwand der Umsetzung
- die anscheinend nur sehr beschränkte Wirksamkeit
- und die geringen Umsätze und Gewinne in diesem Marktsegment

in Relation, so bleibt nur der Schluß, dass die Grenze des §173 (7) TKModG-E ganz gegenteilig zum vorliegenden Entwurf deutlich nach oben anzuheben ist.

Aus diesem Grunde ist die vom ECO e.V. geforderte Größenordnung von „3 Millionen" Teilnehmern deutlich plausibler, marktverträglicher und angemessener. Erst in diesen Bereichen befinden wir uns in Größenordnungen, in der die Kosten nicht mehr außerhalb jeder Relation über Gebühr belastend und defacto marktzutrittsverhindernd sind. Wir möchten uns der Forderung des ECO e.V. darum ausdrücklich anschließen.

4.2) Restriktive Anwendung des §173 TKModG-E

Nachdem der Beschluss „Bestandsdaten II“ des Bundesverfassungsgerichts ein deutliches Urteil bezüglich der viel zu offenen gestalteten Zugriffs- und Verwertungsmöglichkeiten auf Nutzerdaten fällte, sind folgerichtig in §173 III TKModG-E klar definierte Hürden für manuelle Auskunftsverfahren bezüglich Nutzerdaten geregelt worden. Jedoch nur für das manuelle Verfahren.

Diese müssen jedoch logischerweise in §172 TKModG-E für automatisierte Auskunftsverfahren absolut identisch geregelt werden. Es kann nicht sein, dass die bloße Technik des Verfahrens über gänzlich unterschiedliche Zugriffs- und Verwertungsvoraussetzungen bestimmt.

Auch §172 TKModG-E muss darum ausdrücklich formulierte Voraussetzungen analog zu §173 III Nr. 2 TKModG-E fordern.

4.3) Qualifizierte Evaluierung notwendig

Angesichts der Tatsache, wie präventiv (verhaltensändernd) und damit defacto breitflächig (grund-)rechtseingreifend derartige Maßnahmen gegenüber

a) Endnutzern und auch
b) wirtschaftlichen Anbietern

sind, stellt sich auch die Frage, auf welcher fachlichen Grundlage diese Grenzwerte überhaupt bestimmt worden sind und ob es diesbezüglich überhaupt belastbare Untersuchungen zu den positiven wie negativen Auswirkungen am Markt gegeben hat.

Uns ist nicht bekannt, dass es dazu jemals Untersuchungen und belastbare Kosten-Nutzen-Untersuchungen gegeben hat.

Angesichts der wirtschaftlichen Auswirkungen und der Schwere der Eingriffe in die kommunikativen Grundrechte der Bürger und angesichts der Tatsache, dass das Bundesverfassungsgericht hier wiederholt einen deutlich zu laxen Umgang und verfassungswidrige Gesetze festgestellt hat, ist eine zeitnahe qualifizierte Evaluierung dieser Schwellen und Eingriffe deutlich geboten. Bis dahin müssen diese Schwellenwerte so restriktiv wie möglich angesetzt werden.

5) Vorratsdatenspeicherung, §175 TKModG-E

In mehreren Fällen und über Jahre hinweg ist die Einführung einer anlasslosen Vorratsdatenspeicherung (VDS) vom Bundesverfassungsgericht als verfassungswidrig bzw. vom EuGH als unionsrechtswidrig erkannt worden. Der aktuelle Gesetzesentwurf lässt nicht erkennen, dass den Bedenken dieser hohen Gerichte auch nur ansatzweise Rechnung getragen wurde.

So finden sich keinerlei Einschränkungen der Verwertungsmöglichkeiten, beispielsweise eine Limitierung auf schwere Straftaten. Gleichzeitig werden von einer VDS qua Definition fast ausnahmslos unbeteiligte Nutzer präventiv erfasst. Es ist nach wie vor nicht davon auszugehen, dass die Regelungen des Gesetzesentwurfs vor Bundesverfassungsgericht oder EuGH Bestand haben könnten.

Schon jetzt sind gegen die bisherigen Regelungen der derzeitigen (immer wieder für rechtswidrig erkannten und derzeit ausgesetzten) Vorratsdatenspeicherung weitere laufende Verfassungsbeschwerden vor dem Bundesverfassungsgericht anhängig – wir selbst sind dort Beschwerdeführer.

Zu Bedenken ist auch, dass sich viele Daten der VDS im alltäglichen Betrieb in den (sehr flüchtigen) Betriebs-Logfiles der Provider einige wenige Tage lang finden würden, wenn die zuständigen Ermittlungsbehörden nur schnell und konsequent vorgehen würden. Der Zugriff auf diese Daten ist ja durchaus möglich. Da die VDS ja nunmehr seit längerer Zeit ausgesetzt ist, muss also davon ausgegangen werden,

- dass kein ausreichender Ermittlungsdruck besteht, der zu einer höheren Ermittlungseffizienz geführt hat

oder

- dass ohne VDS kein relevanter Nachteil entsteht, weil die Ermittlungsbehörden offensichtlich anderweitig ausreichend Ermittlungsergebnisse erzielen.

Andernfalls wäre die vergangenen Jahre ausreichend Zeit und Druck gewesen, hier personell wie organisatorisch nachzusteuern.

Insofern stellt sich die Frage, was angeblich zwingend nur durch eine VDS erreichen werden kann oder soll, was nicht anderweitig wesentlich weniger grundrechtseingreifend erreicht werden kann, könnte oder bereits erreicht wird.

Darum: Angesichts der Tatsache, dass

- bislang kein Versuch zur Einführung einer anlasslosen Vorratsdatenspeicherung rechtlich Bestand hatte

- und angesichts der Tatsache, dass auch im aktuellen Entwurf keine grundlegende Richtungsänderung und Berücksichtigung der wiederholten Rechtssprechung der vergangenen 15 Jahre zu spüren ist

- und angesichts der Tatsache, dass in all diesen Jahren nicht spürbar geworden ist, dass sich eine fehlende anlasslose Vorratsdatenspeicherung tatsächlich negativ ausgewirkt hätte,

sollte der Beschluss eines TKModG-E klarer Anlass sein, aus diesem fortgesetzten und wiederholten Rechtsbruch zu lernen die Regelungen zur Vorratsdatenspeicherung nach §175ff. TKModG-E ersatzlos aus dem Gesetz zu streichen und das Vorhaben einer VDS endgültig politisch zu begraben.

6) Kommunikationssicherstellungspflicht, §184ff. TKModG-E

Auch im §184 (1) TKModG-E wird nunmehr vom Nutzerbegriff gesprochen. Provider mit mehr als 100.000 Nutzern gelten nun als kritische Infrastruktur im Sinne der §§183ff. TKModG-E.

Zwar ist grundsätzlich begrüßenswert, dass der Gesetzgeber hier die Wichtigkeit und Bedeutung der E-Mail-Kommunikation erkannt hat und deren Kontinuität sicherstellen will, doch ist auch hier analog zu obiger Diskussion zu den §173 (7) TKModG-E der Nutzerbegriff viel zu schwammig und vor allem (wie bereits dargelegt) für den Provider nicht ausreichend vorhersehbar oder gar planbar.

Zu welchen abstrusen Ergebnissen dies führen kann, zeigt ein Beispiel aus der aktuelle Corona-Situation. Nicht wenige Gemeinden oder Bundesländer lassen derzeit ihre Lehrer mit E-Mail-Adressen auch über kommerzielle Anbieter versorgen. Verschiedentlich sollen die Anbieter dabei auch jedem Schüler ein Postfach zur sicheren Kommunikation zur Verfügung stellen.

1. Wenn die Senatsschulverwaltung Berlin einen Provider mit dem Betrieb der Schülerpostfächer von Berlin beauftragen würde, wäre dies nach alter Rechtslage „ein Teilnehmer" gewesen, nach neuer Rechtslage wäre mit rund 366.000 Nutzern zu rechnen. Die Installation würde demnach unter die „Notfallvorsorge" der §§183ff. TKModG-E fallen.

2. Anders im Bundesland Bremen, das nur über rund 60.000 Schüler verfügt. Hier ist die Versorgung der Bremer Schüler wohl in keinem Fall eine aufrechtzuerhaltende kritische Infrastruktur. Politisch wie inhaltlich sicherlich schwer zu vermitteln.

3. Schwierig wird es übrigens im Bundesland Saarland, aktuell wohl 90.986 Schüler. Spätestens wenn die derzeit 8.775 Lehrer auf dem gleichen System betrieben werden, wird ein Wert von 99.761 Nutzern erreicht. Am Ende entscheiden die Postfächer der Schulsekretariate das Rennen – oder die Zahl der Corona-Wiederholer als Folge der Pandemie.

Regelungsklarheit und inhaltlich logische gesetzliche Konsequenz sehen sicherlich anders aus.

Im Übrigen gilt auch hier: Selbst wenn 100.000 Teilnehmer zugrunde gelegt werden, ist die Grenze willkürlich, zu undifferenziert und zu gering angesetzt.

Auch aufgrund der (analog an anderer Stelle bereits dargelegten) daraus entstehenden wirtschaftlichen Auswirkungen ist eine deutliche Erhöhung der Grenzwerte in den deutlichen siebenstelligen Bereich notwendig. Andernfalls wäre auch hier §184 TKModG-E geeignet, für kleinere und mittlere Unternehmen und innovative Startups als Marktzutrittsbehinderung zu wirken.

Und: Der reine Begriff des „E-Mail-Dienstes" aus §184 (1) Nr. 4 TKModG-E ist zudem sicherlich zu unspezifiziert; so kann der Betrieb eines werbefinanzierten Gratis-Anbieters, der temporär gültige Wegwerf-Mailadressen zur Umleitung auf das eigene echte Mailpostfach zur Verfügung stellt, selbst bei siebenstelligen Nutzerzahlen kaum als „kritische Infrastruktur" i.S.d. §§ 183 TKModG-E verstanden werden.

7) Fazit

Alles in allem komme ich zu folgendem Fazit:

- Der Begriff „Kunde“ oder „Teilnehmer“ darf sowohl aus Gründen der Regelungsklarheit, als auch aus Gründen der wirtschaftlich-politischen Auswirkungen keinesfalls zum Begriff „Nutzer“ aufgeweicht werden.

- Schon die vorhandenen Regelungen zur Überwachungs- und Auskunftsverfahren sind ein erheblicher wirtschaftlicher wie auch politischer Nachteil und unterlaufen das Ziel der "digitalen Souveränität". Der Gesetzgeber sollte hier Vorgaben lockern, statt neue Vorgaben aufzuerlegen.

- Die vorhandenen Regelungen sorgen schon jetzt für einen Vertrauensverlust der Bevölkerung in den Staat und beeinflussen damit die Gedanken- und Meinungsfreiheit der Bevölkerung.

- Die Aufwände und Kosten automatisierter Auskunfts- und Überwachungsverfahren (§172 TKModG-E) stehen schon bei den jetzigen Grenzen von 100.000 Teilnehmern in keinem Verhältnis zur Zahl der Abfragen oder dem daraus gewonnenen Nutzen.

- Es ist zweifelhaft, ob die unkontrollierte Datenverwendung des automatisierten Auskunftsverfahrens (§173 TKModG-E) einer Überprüfung durch das BVerfG oder dem EuGH standhalten würde.

- Nach 15 Jahren des Scheiterns sollte jeder weitere Versuch einer anlasslosen Vorratsdatenspeicherung (§175ff TKModG-E) im Sinne und aus Respekt unserer Verfassung gegenüber unterbleiben.

- Der Anwendungsbereich der Telekommunikationssicherstellungspflicht (§184 (1) TKModG-E) sind zu unspezifiziert und unklar geregelt und setzt viel zu enge Grenzwerte.