STELLUNGNAHME

ZUM GESETZENTWURF DER BUNDESREGIERUNG FÜR EIN GESETZ ZUR EINFÜHRUNG EINER SPEICHERPFLICHT UND EINER HÖCHSTSPEICHERFRIST FÜR VERKEHRSDATEN

Berlin, 08.06.2015

In ihrer Kabinettssitzung vom 27. Mai hat die Bundesregierung die Neuregelung der sogenannten Vorratsdatenspeicherung beschlossen. Obwohl im Gesetzgebungsverfahren eine Anhörung der betroffenen Verbände nicht vorgesehen ist, möchte eco – Verband der deutschen Internetwirtschaft e.V. im Hinblick auf das bevorstehende, parlamentarische Verfahren auf technische und rechtliche Bedenken hinweisen.

I. Das Gesetz verstößt gegen Grundrechte. Insbesondere wird es durch die geänderten technischen Rahmenbedingungen bei Umsetzung durch die Anbieter zu einem mehr Datenspeicherungen als zu Zeiten der letzten Vorratsdatenspeicherung kommen.

II. Viele der technischen Vorschriften sind für die Praxis nicht handhabbar.

III. Für die Umsetzung der Vorgaben werden den betroffenen Unternehmen enorme Kosten entstehen. Es sind nahezu keine Entschädigungen vorgesehen, das ist in Anbetracht der Tatsache, dass in diesem Fall originär staatliche Aufgaben auf die Privatwirtschaft abgewälzt werden, nicht angemessen.

IV. Viele Vorschriften zu Speicherung und Sicherung der Daten sind nicht hinreichend klar formuliert.

eco fordert deshalb:

- **Den generellen Verzicht auf das Instrument der Vorratsdatenspeicherung.**

Das Ziel des Verbandes der deutschen Internetwirtschaft war und ist, die anlasslose, verdachtsunabhängige Vorratsdatenspeicherung zu verhindern. Es widerspricht dem Wesen einer demokratischen Gesellschaft, ihre Bürger unter Generalverdacht zu stellen und zu überwachen.

- **Ausklammerung der Internetdienste**

Es muss vermieden werden, dass Daten gespeichert werden müssen, die eine Aufzeichnung des kompletten Nutzerverhaltens zur Folge haben. Dafür wäre eine Lö-

sung, jedwede Datenspeicherung der das Internet betreffenden Dienste von der Speicherverpflichtung auszunehmen.

- **Als Minimallösung eine Modifizierung des Entwurfs**

Wenn die Regierung an ihrem Vorhaben, die Datenspeicherung trotz ernsthafter verfassungsrechtlicher Bedenken einzuführen, dennoch festhält, muss der Gesetzentwurf zwingend modifiziert werden: So müssen die technischen Vorgaben zur Speicherung in technisch realistische, für die Praxis handhabbare Anforderungen umgewandelt werden.

- **Die Zahlung von Entschädigungen an die betroffenen Unternehmen**

Die verpflichteten Unternehmen sind zu entschädigen: Mit den neu geschaffenen Normen werden die Anbieter dazu angehalten, originäre Aufgaben des Staates zu erfüllen. Die Investitionen hierfür sollen sie aber selbst tragen. Das ist nicht verhältnismäßig.

- **Rechtssicherheit für Unternehmen**

Eine Haftung der Unternehmen bei technisch und rechtlich nicht hinreichend klaren bzw. umsetzbaren Normen muss definitiv ausgeschlossen werden. Zudem müssen die Verpflichtungen und Sicherheitsbestimmungen hinreichend klar gefasst werden.

I. Verfassungsmäßigkeit des Gesetzentwurfs

Die Bundesregierung geht davon aus, dass der neue Vorschlag verfassungsgemäß ist, da einige vom Bundesverfassungsgericht vor fünf Jahren aufgestellten Eckpunkte miteingeflossen sind und die Neufassung sich an dem Urteil aus dem Jahr 2010 orientiert. Dabei verkennen sie, dass sich die Technik gerade im IT-Bereich in den letzten fünf Jahren erheblich weiterentwickelt hat. Auch schweigt der Entwurf zu der vom Verfassungsgericht aufgeworfenen Problematik der „Überwachungsgesamtschau“.

Aus diesen Gründen wird sich bei Umsetzung des Gesetzentwurfs in seiner derzeitigen Fassung die Frage der Verhältnismäßigkeit neu stellen.

Die Maßnahme der Vorratsdatenspeicherung ist geeignet, das Vertrauen der Bevölkerung in die neuen Technologien nachhaltig zu beschädigen und die Menschen aufgrund eines „diffusen Überwachungsgefühls“ (BVerfG) dazu zu bringen, ihr Verhalten im Hinblick auf ihre Mediennutzung zu ändern.

Die umfassende und anlasslose Speicherung von persönlichen Daten steht damit einer effektiven Strafverfolgung gegenüber. Die Speicherung dieser Daten ist daher mit dem Grundsatz der Unschuldsvermutung, sowie dem Recht auf informelle Selbstbestimmung und dem Fernmeldegeheimnis nur dann vereinbar, wenn es sich um das mildeste Mittel zur Erreichung eines höher einzuschätzenden Zieles handelt. Hier lohnt es sich also genau hinzusehen: Das Gesetz dient nicht dazu, Verbrechen zu

verhindern, sondern soll einer besseren Strafverfolgung dienen ("Aufklärung schwerer Straftaten"). Die in § 100g StPO-E genannten schweren Straftaten sind allerdings allesamt Straftaten, bei denen bereits ohne Vorratsdatenspeicherung eine Aufklärungsquote von etwa 90 % besteht[1]. Den Anspruch auf eine 100%ge Aufklärungsquote zu Lasten der Freiheitsrechte wurde aber weder von der Rechtsprechung noch der Lehre seit Bestehen der Bundesrepublik je gefordert. Hinzu kommt, dass ein Nutzen auch deshalb fraglich ist, da die Datenspeicherung nur die Dienste betreffen wird, die im Telekommunikationsgesetz geregelt sind. Andere Dienste – die unter das Telemediengesetz fallen – sind nicht betroffen.

Das heißt beispielsweise: Die Verbindungsdaten einer SMS werden gespeichert, die einer WhatsApp-Nachricht nicht. Das ist insofern bemerkenswert, als internetbasierte, alternative Chat-Dienste immer beliebter werden: Verschickten die Deutschen im Jahr 2012 noch fast 60 Milliarden SMS, waren es im Jahr 2014 nur noch 22,5 Milliarden. Es ist auch zu erwarten, dass diese Entwicklung ebenso rasant weitergehen wird, wenn man bedenkt, dass Dienste über das Internet häufig kostenfrei (bzw. in der Internetflat eines Smartphones enthalten) sind.

1. *Ausmaß der geplanten Speicherung nach §113 b Absatz 3 TKG-E*

Die Dimension der Datenspeicherung wird heute durch die veränderten technischen Gegebenheiten – entgegen der Verlautbarungen aus den zuständigen Ministerien – eine ganz andere als noch bei Erlass der ersten Regelung vor knapp zehn Jahren sein.

Dies liegt vor allem an der Zuordnung von IP-Adressen: Diese sollen nach §113 b Absatz 3 TKG-E vom Anbieter gespeichert werden. Konnten IP-Adressen zu Zeiten des ersten Gesetzes zur Vorratsdatenspeicherung aber noch einem einzigen Anschluss zugeordnet werden, werden sie mittlerweile mehrfach und nur temporär vergeben. Grund hierfür ist eine wachsende IPv4-Adressen-Knappheit, da es immer mehr Anschlüsse gibt. Das führt dazu, dass die IP-Adresse alleine nicht mehr ausreicht, um einen bestimmten Anschluss zu identifizieren, hierzu werden vielmehr weitere Daten benötigt. Dazu müssen die Anbieter eine neue, riesige Datenbank aufbauen. Neben der IP-Adresse gespeichert werden müssen in dieser dann der sogenannte Port, der den genutzten Dienst feststellt; darüber hinaus bedarf es einen hochgenauen Zeitstempels, der die Nutzung eines Dienstes idealerweise bis auf die Millisekunde genau festhält. Damit ist der Provider gezwungen, das gesamte Nutzerverhalten zu speichern, um den gesetzlichen Verpflichtungen entsprechen zu können. So entsteht eine lückenlose Aufzeichnung des Verhaltens aller Nutzer im Netz. Dies stellt einen weitaus tieferen Eingriff in das Post- und Fernmeldegeheimnis (Art. 10 GG) dar, als es bei der alten Regelung der Fall war. Denn mit den so gespeicherten Daten kann – auch

[1] s. PKS 2014

bei kürzeren Speicherfristen – ein vollständiges Nutzerprofil des Einzelnen erstellt werden.

Im Übrigen widerspricht sich der Entwurf an dieser Stelle selbst. Nach §113 b Absatz 5 TKG-E sollen der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post aufgrund der Vorschrift nicht gespeichert werden dürfen. Die Speicherung von Informationen über den genutzten Port enthält aber gerade auch Auskünfte zu den im Netz genutzten Diensten und kann mithin auch Informationen über besuchte Seiten und Inhalte liefern.

Um dieser Problematik entgegenzuwirken, wäre ein zielführender Ansatz, alle Internetdienste vollumfänglich von den Speicherungsverpflichtungen des Entwurfs auszunehmen.

2. Ausmaß der Speicherpflicht nach §113 a Absatz 1 TKG – E

Ein großes Problem ergibt sich auch bezüglich der Verpflichteten gemäß §113 a Absatz 1 TKG – E. Bleibt es bei dem jetzigen Wortlaut der Norm, wird die Speicherverpflichtung der Telekommunikationsunternehmen und Internetprovider auf ein Niveau ausgeweitet, das nicht beabsichtigt sein kann. Insoweit bedarf es bei diesem Paragraphen dringend einer Klarstellung:

Nach der geplanten Neufassung sollen alle Erbringer öffentlich zugänglicher Telekommunikationsdienste zu den Gewährleistungen der §§113b bis 113g TKG –E verpflichtet werden. §113a Absatz 1 Satz 2 Nummer 1 schreibt dem Erbringer von TK-Dienstleistungen darüber hinaus vor, sicherzustellen, dass die nicht von ihm selbst bei der Erbringung seines Dienstes erzeugten und verarbeiteten Daten ebenfalls gemäß §113b Absatz 1 gespeichert werden. Es ist anzunehmen, dass den Verfassern des Entwurfs die Konstellation vorschwebte, dass ein Netzbetreiber, der zwar einen Telekommunikationsdienst anbietet, selbst aber keine Infrastruktur besitzt und sich deshalb der Übertragungswege eines anderen Betreibers bedient, sicherstellen muss, dass dieser „Reseller“ die erforderlichen Speicherungen ebenfalls vornimmt, auch wenn er nicht Vertragspartner des Kunden ist.

Da – anders als in der alten Fassung des §113 a TKG – das Kriterium der „Endnutzer“ entfallen ist, sind aber auch weitere Konstellationen denkbar: So kann etwa ein Provider, der lediglich den Internetzugang anbietet, nicht wissen, welche Dienste sein Kunde über diesen Zugang sonst noch in Anspruch nimmt. Nutzt dieser bspw. einen Internettelefondienst (wie Skype), müsste der Provider das nach dem jetzigen Wortlaut der Norm speichern, um später nach §113a Absatz 1 Nr. 2 TKG beauskunften zu können, dass der Kunde Skype genutzt hat und alle weiteren Angaben dort zu erfragen sind. Da der Provider jedoch zugleich nach Absatz 5 „Inhalte der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post“ nicht speichern darf, wird ihm zur Unterscheidung der IP-Pakete seines Kunden etwa von diesen „Skype-Paketen“ kaum etwas anderes übrig bleiben, als den gesamten Traffic mit Hilfe von Technik zur Deep Packet Inspection (DPI) zu überwachen und

entsprechend zum Zwecke der angeordneten Speicherung zu filtern. Denn nur, wenn gleichzeitig der Datenteil und der Headerteil des Datenpaketes auf bestimmte Merkmale wie IP-Telefonie untersucht werden, kann er die Speicherpflicht des §113a Abs. 1 Nr. 1 erfüllen, ohne gegen die in § 113 b Abs. 5 bestimmte Inhaltliche Schranken zu verstoßen. Im Unterschied zu klassischen Paketfiltern reicht die Überprüfung des Headerteils nicht für eine Regulierung und Unterscheidung dieser Datenströme. Ein derart weite Speicherungsverpflichtung steht aber in einem eklatanten Widerspruch zu den Regelungen des §88 TKG und Artikel 10 GG, dem Post- und Fernmeldegeheimnis. Mittels dieser Anforderung würde faktisch eine „Totalüberwachung" des Datenverkehrs angeordnet, die gerade dem erklärten Willen des Gesetzentwurfs widerspricht.

3. Regelungen für Berufsgeheimnisträger

Der EuGH hat in seinem Urteil klargestellt, dass die Verkehrsdaten von Berufsgeheimnisträgern nicht gespeichert werden dürfen.

Es gibt aber kein Verzeichnis von Berufsgeheimnisträgern, es dürfte im Einzelfall nicht einmal sicher sein, welche Personen unter diese Bezeichnung fallen (z.B.: wer ist eigentlich Journalist und wer nicht?). Selbst wenn dies aber abschließend geklärt werden könnte, wäre die Anlage einer Datenbank mit allen Personen, die von der Speicherung ausgenommen werden müssen, technisch nicht möglich. Denn auch wenn ein Telekommunikationsanbieter tatsächlich wissen sollte, dass einer seiner Kunden Geheimnisträger ist und etwa bei diesem eingehende Anrufe deshalb nicht speichert, würden die Anrufe trotzdem durch die Anbieter der Anrufer aufgezeichnet, die nicht wissen können, dass ihr Kunde gerade einen Berufsgeheimnisträger kontaktiert.

Die Erhebung der Daten von Berufsgeheimnisträgern soll gemäß §100 g Absatz 4 StPO – E unzulässig sein, obwohl das also technisch unmöglich zu gewährleisten ist. Dennoch erlangte Erkenntnisse sollen nicht verwendet werden dürfen, werden also einem Verwertungsverbot unterstellt. Dieses Verwertungsverbot wird in der Praxis die Regel sein. Es darf bezweifelt werden, dass diese Konstruktion den verfassungsrechtlichen Anforderungen der Obergerichte entspricht.

Verfassungsrechtlich sehr fraglich dürfte daneben die Tatsache sein, dass die sogenannte „Bestandsdatenabfrage" des §100 g Absatz 1 i.V.m. §96 TKG auch für Berufsgeheimnisträger gelten soll. Der Regierungsentwurf bleibt hierbei sogar noch hinter dem Referentenentwurf zurück: War ursprünglich vorgesehen, Datenerhebungen gegen eine der in §53 Absatz 1 Satz 1 Nummer 1 bis 5 StPO genannten Personen ganz zu verbieten, sollen nun Erhebungen nur für Fälle des §100 g Absatz 2 StPO unzulässig sein. Das heißt, dass der notwendige Schutz zeugnisverweigerungsberechtigter Personen bei leichterer Kriminalität – bei der auch der strenge Richtervorbehalt nicht gilt – ganz entfällt.

4. Benachrichtigungspflicht, §101 a Absatz 6 StPO – E

§101 a Absatz 6 StPO – E des Entwurf sieht eine Benachrichtigungspflicht des Betroffenen vor Abruf seiner Daten vor. Eine heimliche Verwendung soll nach gerichtlicher Prüfung nur ausnahmsweise zulässig sein, dann soll es aber einer Benachrichtigung bedürfen, von der wiederum aber mit richterlicher Bestätigung abgesehen werden kann.

Faktisch wird eine Benachrichtigung aber nur im Ausnahmefall erfolgen. In der Praxis wird der Richter eine heimliche Verwendung (zu Recht) immer dann für erforderlich halten, wenn durch die Benachrichtigung des Betroffenen die polizeilichen Ermittlungen gefährdet würden. Das dürfte – gerade in Fällen, in denen sonst keine Ermittlungsansätze vorhanden sind – so gut wie immer der Fall sein. Ein Fall, in dem die vorherige Benachrichtigung des Betroffenen keine Gefährdung darstellt, ist nur dann vorstellbar, wenn der Betroffene ohnehin schon von Maßnahmen gegen sich weiß und andere Beweise schon vorliegen. Dann aber bedürfte es zu einer effektiven Strafverfolgung nicht der Vorratsdatenspeicherung. Diese Vorschrift läuft also ins Leere und kann als Rechtfertigung für einen schweren Grundrechtseingriff kaum herangezogen werden.

5. „Überwachungsgesamtrechnung“

Nicht ausreichend Rechnung getragen wird in dem Entwurf dem vom Bundesverfassungsgericht aufgebrachten Merkmal der „Überwachungsgesamtrechnung“. Die Richter schrieben in ihrem Urteil von 2010 (1 BvR 256/08 Rn. 218): *„Umgekehrt darf die Speicherung der Telekommunikationsverkehrsdaten nicht als Schritt hin zu einer Gesetzgebung verstanden werden, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielte. Eine solche Gesetzgebung wäre, unabhängig von der Gestaltung der Verwendungsregelungen, von vornherein mit der Verfassung unvereinbar. Die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten setzt vielmehr voraus, dass diese eine Ausnahme bleibt. Sie darf auch nicht im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen. (…) Die Einführung der Telekommunikationsverkehrsdatenspeicherung kann damit nicht als Vorbild für die Schaffung weiterer vorsorglich anlassloser Datensammlungen dienen, sondern zwingt den Gesetzgeber bei der Erwägung neuer Speicherungspflichten oder -berechtigungen in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen zu größerer Zurückhaltung.“*

Diese Voraussetzungen sind bei Umsetzung des Vorhabens nicht gewährleistet. In den letzten Jahren hat es eine Reihe von Maßnahmen gegeben, die die „Überwachung“ der Bürger weiter ausbauen. Dies betrifft insbesondere die Änderungen des

TKG, namentlich die Neuregelung der Bestandsdatenauskunft und die geplante Neuregelung des Verfassungsschutzgesetzes. Auch in anderen Bereichen wie der anstehenden Einführung der PKW-Maut oder der enorm ausgeweiteten Befugnisse der Finanzbehörden werden immer mehr private Bereiche einer verstärkten Kontrolle des Staates unterzogen. Betrachtet man diese Entwicklung vor dem Hintergrund der ständig fortschreitenden technischen Entwicklung, steht zu befürchten, dass die Behörden bald in der Lage sein werden, umfassende Informationen über das Verhalten der Bürger für sich nutzbar zu machen.

II. Technische Umsetzbarkeit des Regierungsentwurfs

1. *Einsatz eines besonders sicheren Verschlüsselungsverfahrens, §113 b Satz 1 Nummer 1 TKG – E*

In seinem Urteil aus dem Jahr 2010 hat das Bundesverfassungsgericht eine asymmetrische Verschlüsselung als Möglichkeit einer verfassungsmäßigen Speicherung der Daten genannt. Hierauf bezieht sich die Gesetzesbegründung zu §113 b Satz 1 Nummer 1 TKG – E, der ein besonders sicheres Verschlüsselungsverfahren fordert. Asymmetrische Verschlüsselung bedeutet, dass der Provider verpflichtet ist, jeden Datensatz einzeln zu verschlüsseln. Dies heißt aber für die Praxis, dass auch die Personen, die eine Behördenanfrage bearbeiten sollen, nur auf verschlüsselte Daten zugreifen können. Deshalb müsste ein exakter Suchindex geschaffen werden, um die Datensätze für eine Abfrage auffindbar zu machen. Jeder Index stellt aber selbst wieder eine Metadatensammlung dar. Vollkommen unklar ist, wie ein spezieller Suchindex für Massenabfragen, wie etwa die Funkzellenabfrage, technisch realisiert werden soll.

2. *Speicherung der Daten auf vom Internet entkoppelten Verarbeitungssystemen, §113 d Satz 1 Nummer 3 TKG – E*

Probleme wirft des Weiteren die Vorgabe auf, die Daten auf vom Internet entkoppelten Datenverarbeitungssystemen zu speichern. Die zu speichernden Daten werden in vernetzten und dezentralen Systemen erhoben, transportiert und wieder in vernetzten Systemen verarbeitet. Auch die Schnittstelle zu den Bedarfsträgern für die Beantwortung von Auskunftsersuchen durch die Anbieter ist ein vernetztes und dezentrales System und muss mit dem Auskunftssystem zwangsläufig verbunden werden.

Eine physikalische Trennung, wie sie der Gesetzentwurf vorsieht, ist demnach logisch nicht denkbar. Die Daten müssen irgendwie auf ein zentrales Speichermedium gelangen. Fraglich ist, ob hier die Vorstellung zugrunde liegt, dass ein Techniker alle paar Minuten neue Daten auf einen USB-Stick kopiert, um sie dann ständig per Hand in einen anderen Rechner einzuspeisen? Das ist bei den enormen Datenmengen, die durch die Provider zu speichern sind, und bei den Betriebsabläufen in der Praxis schlicht nicht vorstellbar.

3. Vier- Augen- Prinzip, §113 d Satz 1 Nummer 5 TKG – E

Die in §113 d Satz 1 Nummer 5 TKG – E vorgeschriebene Mitwirkung von mindestens zwei Personen beim Zugriff auf die Daten, die dazu durch den Verpflichteten besonders ermächtigt worden sind (Vier-Augen-Prinzip), ist für mittlere und kleine Provider ebenfalls kaum umzusetzen. Die weit überwiegende Anzahl der von der Neuregelung betroffenen Betriebe sind solche mit relativ wenigen Mitarbeitern (s. u. zum Punkt Kosten). Häufig gibt es im ganzen Unternehmen nur zwei oder drei Administratoren, die eine Datenabfrage beantworten könnten. Diese müssten also immer und gleichzeitig anwesend sein, um die gesetzlichen Voraussetzungen zu erfüllen. Das ist ebenso praxisfern wie die Vorstellung, kleine Unternehmen könnten sich eine Vervielfachung ihrer Mitarbeiter leisten, um sicherzustellen, dass eventuell eingehende Abfragen nach dem Vier-Augen-Prinzip zeitnah beantwortet werden können. Selbst für größere Anbieter dürfte sich die Frage nach Aufwand und Nutzen stellen, sodass diese Leistung grundsätzlich kompensiert werden muss.

III. Wirtschaftliche Faktoren

Diesem Punkt voranzustellen ist die grundsätzliche Überlegung, dass eine Schwächung des Wirtschaftsstandortes Deutschland unbedingt verhindert werden muss. Schon jetzt sind Unternehmen im Internet- und Telekommunikationssektor verpflichtet, viel weitergehende Vorgaben zu erfüllen als europäische oder internationale Mitbewerber; das verhindert hierzulande heute schon Innovationen und Investitionen. Das kann in einem Wirtschaftsbereich, der in den letzten Jahren so stark gewachsen ist wie kein anderer in der Bundesrepublik, nicht das Ziel vorausschauender und chancenorientierter Politik sein.

1. Kosten der Regelungen für die betroffenen Unternehmen

Schon jetzt ist absehbar, dass den Anbietern von Telekommunikations- und Internetdiensten enorme Kosten für Anschaffung und Implementierung der für die Speicherung notwendigen Infrastruktur, sowie für die laufenden Betriebskosten entstehen werden. Durch die in §113 b TKG geplante Differenzierung der Speicherdauer sowie die gestiegenen Sicherheitsstandards (z. B. Vier-Augen-Prinzip) wird bei den verpflichteten Unternehmen ein noch größerer Aufwand entstehen als nach der ersten Regelung im Jahr 2007: Damals mussten nach Hochrechnungen der Branchenverbände ca. 300 Millionen investiert werden, um die gesetzlichen Vorgaben zu erfüllen.

Eine genaue Schadensabschätzung für die Internetbranche ist aufgrund der noch ungenauen gesetzlichen Anforderungen aktuell schwer zu beziffern. eco geht nach ersten Hochrechnungen von einer Verdopplung der Summe von 2007 aus, mithin von Ausgaben in Höhe von ca. 600 Millionen Euro.

Diese Schätzung basiert auf der folgenden Hochrechnung angenommener Kosten für die verschiedenen Unternehmens-Größenklassen:

Unternehmensgröße	**Anzahl der Unternehmen**	**Geschätzte Kosten pro Unternehmen**	**Gesamtkosten für diese Größenklasse**
Top Anbieter mit über einer Million Kunden	5	30 Mio. Euro	150 Mio. Euro
Unternehmen mit über 100.000 Kunden	15	8 Mio. Euro	120 Mio. Euro
Unternehmen mit mehr als 10.000 Kunden	300	500.000 Euro	150 Mio. Euro
Unternehmen mit mehr als 1.000 Kunden	2.200	80.000 Euro	176 Mio. Euro
		Gesamtkosten	**596 Mio. Euro**

Anders als der Entwurf – der aus nicht nachvollziehbaren Gründen von lediglich 1000 betroffenen Unternehmen ausgeht – geht eco von mindestens 2.500 Unternehmen aus, die die Regelungen werden umsetzen müssen.

Eine genaue Berechnung der zu erwartenden Kosten wird allerdings erst möglich sein, sobald alle technischen, gesetzlichen und personellen Anforderungen im Detail bekannt sind.

Anders als in der Begründung des Gesetzentwurfs angenommen, können die Unternehmen nicht auf die für den letzten Durchgang der Vorratsdatenspeicherung angeschaffte Infrastruktur zurückgreifen, da sich die Technik zum einen in den letzten fünf Jahren beständig weiterentwickelt hat, zum anderen aber ganz andere Verpflichtungen für die Speicherung gelten sollen.

Auch die Vorgabe des §113 b Absatz 1 TKG – E, die Daten ausschließlich im Inland zu speichern, widerspricht der Praxis vieler Anbieter. Unternehmen, die ihre Dienste im europäischen oder gar im internationalen Raum anbieten, haben hierfür zentrale Server, die nicht notwendigerweise in Deutschland stehen. Diese Anbieter werden durch das neue Gesetz gezwungen, auch im Inland Infrastruktur für die Speicherung der geforderten Daten zu schaffen. Dies ist ein erheblicher Aufwand, der mit dem

Nutzen in keinem Verhältnis steht. Zudem ist sehr fraglich, ob eine solche Vorgabe nicht gegen Europarecht verstößt. Zwar geht auch die Begründung des Entwurfs davon aus, dass hier in die Dienstleistungsfreiheit gemäß Artikel 56 AEUV eingegriffen wird. Gerechtfertigt sein soll das aber mit zwingenden Gründen des Allgemeininteresses, hier um die „gespeicherten Vorratsdaten wirksam vor Missbrauch sowie vor jedem unberechtigten Zugang und jeder unberechtigten Nutzung zu schützen und das durch eine unabhängige Stelle zeitnah und effizient überwachen zu können." Das soll nur in Deutschland zu gewährleisten sein. Dass das der EGMR im Falle seiner Befassung genauso sieht, darf bezweifelt werden.

2. Entschädigungsleistungen, §113 a Absatz 2 TKG – E

Eine Entschädigung ist nach dem Entwurf des §113 a Absatz 2 TKG nur dann vorgesehen, „soweit dies zur Abwendung oder zum Ausgleich unbilliger Härte geboten erscheint". Das soll nach der Begründung dann der Fall sein, wenn die Anbieter darlegen können, dass die Auswirkungen der Speicherpflicht für ihr Unternehmen erdrosselnde Wirkung haben könnten. Lediglich für die Kosten, die durch den Abruf der Daten für die Bedarfsträger im Einzelfall entstehen, ist die Zahlung pauschalierter Beträge vorgesehen.

Das ist paradox: Die Vorratsdatenspeicherung soll ausschließlich für originäre staatliche Aufgaben, namentlich die Strafverfolgung, eingeführt werden. Für die Kosten aufkommen soll aber alleine die Privatwirtschaft. Gleichzeitig verzichtet die Bundesregierung auf die Ergreifung alternativer Maßnahmen, wie etwa die flächendeckende Ausstattung der Strafverfolgungsbehörden mit qualifiziertem IT- Personal und moderner Technik. Dabei wäre dies dringend geboten und dürfte auch eine effizientere Verfolgung möglich machen, allein durch das Instrument der Vorratsdatenspeicherung zu erwarten ist.

Dies gilt umso mehr, als durch die Vorratsdatenspeicherung Vorbehalte gegen die speichernden Unternehmen geschürt werden, sie haben mit Imageverlusten zu rechnen. Es steht zu befürchten, dass mit Einführung dieser in der Bevölkerung als Überwachungsinstrument wahrgenommenen Maßnahme ein Vertrauensverlust in die gesamte Branche einhergeht.

Deshalb ist die verpflichtende Zahlung von Entschädigungen an alle Unternehmen erforderlich.

Es ist unverhältnismäßig, dass eine Entschädigung hingegen nur bei Nachweis einer „erdrosselnden" Wirkung gezahlt werden soll. Ein solcher Nachweis wird im Einzelnen nur sehr schwer und mit großem Aufwand zu führen sein. Dies umso mehr, als auch nach der Begründung des Gesetzentwurfs nicht klar ist, ab welcher Belastung von dieser Wirkung ausgegangen werden soll.

Besonders für kleine oder mittlere Betriebe – die mit 2.200 von 2.500 Anbietern die mit Abstand größte Gruppe darstellen – sowie Geschäftskundenanbieter wird die Umsetzung der Normen und die Auferlegung der Kosten der Vorratsdatenspeicherung eine enorme Belastung darstellen, die in keinem Verhältnis zum zu erwartenden Nutzen steht. Diese Betriebe werden erfahrungsgemäß kaum mit Behördenanfragen konfrontiert; aber sie würden von den finanziellen und logistischen Anforderungen überdimensional hart getroffen.

Deshalb müssen zumindest kleine Unternehmen und Geschäftskundenanbieter vollständig aus dem Anwendungsbereich des neuen Gesetzes ausgenommen werden.

IV. Rechts- und Planungssicherheit für betroffene Anbieter

1. Verlässlichkeit der Investitionen

Bezüglich der finanziellen Belastungen stellt sich außerdem die Frage, wie verlässlich neue Investitionen durch die Unternehmen getätigt werden können. Nach Verabschiedung des §113a TKG a.F. haben deutsche Telekommunikationsanbieter mehrstellige Millionenbeträge für die Umsetzung der gesetzlichen Anforderungen aufgewendet. Nur zwei Jahre später wurde das Gesetz für verfassungswidrig erklärt, die Kosten für die Anbieter stellten sich als von Anfang an sinnlos heraus.

Bei Verabschiedung eines neuen Gesetzes ist absehbar, dass dieses wiederum vor das Bundesverfassungsgericht (eventuell auch vor den EGMR) gebracht werden wird. Erst dann wird sich herausstellen, ob es Bestand hat. Also wird sich auch erst dann erweisen, ob erneute finanzielle Aufwendungen seitens der Anbieter überhaupt notwendig waren. Bei dieser unklaren Ausgangslage ist es – auch nach dem oben Dargelegten – kaum zu rechtfertigen, die Anbieter zu verpflichten, große Summen vor der gerichtlichen Klärung zu investieren – auch vor dem Hintergrund der Erfahrung mit dem ersten Gesetz zur Vorratsdatenspeicherung.

2. Umsetzung der Sicherheitsanforderungen

Der neue §113 d TKG –E regelt die grundsätzlichen Sicherheitsvorgaben, die die Unternehmen umsetzen müssen. Wie bereits oben dargelegt, sind einige von ihnen gar nicht technisch praktikabel oder kaum handhabbar. Der Anbieter soll aber nach §149 Absatz 1 Nr. 40 i.V.m. §149 Absatz 2 Nr.1 TKG – E mit einer Geldbuße bis zu 500.000€ belegt werden können, wenn er entgegen des §113 d Satz 1 TKG – E nicht sicherstellt, dass Daten gegen unbefugte Kenntnisnahme und Verwendung geschützt werden.

Das bedeutet, dass die Unternehmen einen Katalog technisch teilweise undurchführbarer Maßnahmen umsetzen müssen, um sicherzugehen, dass sie bei etwaigem Missbrauch der Daten durch Dritte nicht haftbar gemacht werden können. Das ist für die Anbieter offensichtlich nicht zu leisten.

Dazu kommt die Vorschrift des §113 f TKG, die die Anbieter zusätzlich verpflichtet, bei der Umsetzung der §§113 b bis 113 e TKG einen besonders hohen Standard der Datensicherheit und Datenqualität zu gewährleisten. Eine konkrete Ausgestaltung der jeweiligen Anforderungen wird in demselben Paragraphen der Bundesnetzagentur übertragen. Die Einhaltung dieses hohen Standards soll nur dann vermutet werden, wenn der Verpflichtete alle Anforderungen dieses – von der Bundesnetzagentur aufgestellten – Katalogs erfüllt. Das heißt, dass sich ein Unternehmen auch nur in diesem Fall exkulpieren kann.

Was es dafür konkret tun muss, ergibt sich aus dem Gesetz aber nicht. Die Unternehmen müssen vielmehr darauf warten, dass die Bundesnetzagentur gemäß §150 Absatz 13 TKG – E hinreichend konkrete und umsetzbare Kriterien erstellt, mit denen die Anbieter arbeiten können: Nach dieser Vorschrift sind die Unternehmen eineinhalb Jahre nach Inkrafttreten des Gesetzes verpflichtet, die Speicherungen unter Einhaltung der entsprechenden Sicherheitsvorgaben zu erfüllen. Davon ist jedoch die meiste Zeit für die Bundesnetzagentur vorgesehen, der ein ganzes Jahr zugestanden wird, die Sicherheitsanforderungen für die Praxis zu konkretisieren. Das heißt, dass den Anbietern lediglich ein halbes Jahr bleiben wird, um alle gesetzlichen Anforderungen zu erfüllen, die technischen und organisatorischen Prozesse aufzusetzen und die finanziellen Ressourcen bereitzustellen. In Anbetracht der komplizierten Regelungsmaterie ist das absolut unrealistisch.

Der Gesetzgeber sollte den Anbietern eine ausreichende Frist von mindestens 18 Monaten nach der konkreten Festlegung aller Anforderungen durch die Bundesnetzagentur zur Umsetzung gewähren, die erst dann zu laufen beginnt, wenn über die Verfassungsmäßigkeit der geplanten Regelungen höchstrichterlich entschieden ist.