



INITIATIVE
EUROPÄISCHER
NETZBETREIBER

IEN · Dorotheenstrasse 54 · 10117 Berlin

Stellungnahme zum Gesetzentwurf für ein Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten

Berlin, den

12.06.2015

In ihrer Kabinettsitzung am 27. Mai hat die Bundesregierung den Entwurf für ein „Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten“ (Vorratsdatenspeicherung) beschlossen. Nach den Plänen der Bundesregierung soll das parlamentarische Verfahren noch vor der Sommerpause abgeschlossen und das Gesetz verabschiedet werden. Woraus sich die sachliche Begründung für die angebliche Eilbedürftigkeit ergeben soll, ist aus Sicht der IEN allerdings nicht ersichtlich, eine hinreichende parlamentarische Beratung wäre angesichts der Schwächen dieses Gesetzentwurfes dringend geboten. Insofern würde es die IEN sehr begrüßen, wenn das Parlament für die Beratung dieses Entwurfs hinreichend Zeit einplanen würde.

Die IEN bewertet den aktuellen Entwurf aus einer Vielzahl von Gründen als kritisch, da – ungeachtet der Frage einer generellen Befürwortung oder Ablehnung der Vorratsdatenspeicherung – sowohl im Ansatz der Regelungen, als auch im Detail ihrer Formulierung ein erheblicher Nachbesserungsbedarf besteht.

I. Allgemeine Anmerkungen

Einleitend möchte die IEN auf ihre erheblichen Bedenken hinsichtlich des Verfahrens zur Verabschiedung des gegenständlichen Gesetzentwurfes hinweisen.

Die Durchführung in einem gesetzgeberischen Eilverfahren ohne eine Einbeziehung oder Anhörung der betroffenen Verbände und betroffenen Telekommunikations- und Internetunternehmen ist weder sinnvoll noch angemessen.

Die Branche der deutschen Telekommunikations- und Internetunternehmen hat bereits infolge des letzten Gesetzes über die Vorratsdatenspeicherung, welches im Jahr 2010 vom Bundesverfassungsgericht für nichtig erklärt wurde, Ausgaben in mehrstelliger Millionenhöhe tätigen müssen, ohne da-

MITGLIEDER

Colt
Orange Business
Verizon
Vodafone

SITZ UND BÜRO

Dorotheenstrasse 54
10117 Berlin

GESCHÄFTSFÜHRUNG

RAin Malini Nanda

VORSTAND

Sabine Hennig
Dr. Jutta Merkt
Dr. Andreas Peya

KONTAKTE

Telefon +49 30 3253 8066
Telefax +49 30 3253 8067
info@ien-berlin.com
www.ien-berlin.com

für nach Feststellung der Verfassungswidrigkeit der Vorgaben entschädigt worden zu sein. Bei der Implementierung neuer gesetzlicher Speichervorgaben, die von den betroffenen Unternehmen erneut erhebliche – und aus Sicht der IEN in den meisten Fällen unverhältnismäßigen – Neuinvestitionen fordern, muss eine hinreichende Rechts- und Planungsunsicherheit geschaffen und das drohende unkalkulierbare finanzielle Risiko ausgeschlossen werden. Dies gewinnt insbesondere vor dem Hintergrund Bedeutung, dass bereits gegenwärtig absehbar ist, dass einige der Vorgaben des Entwurfs weder zielführend im Sinne des angestrebten Zwecks des Gesetzes, noch technisch praktikabel sind.

Die IEN kritisiert insbesondere den erheblichen Verstoß gegen das Gebot der Datensparsamkeit nach § 3a BDSG, da nach dem gegenständlichen Gesetzentwurf unter erheblichem Aufwand Daten gesondert in Deutschland zu speichern sind, obgleich sie bereits zu Abrechnungszwecken vorgehalten und gegenüber den Strafverfolgungsbehörden entsprechend beauskunftet werden. Dies gilt vor allem in Bezug auf diejenigen Anbieter von TK-Diensten, die Angebote für große und international agierende Geschäftskunden oder Behörden erbringen und für diese lediglich statische IP-Adressen vergeben.

Die IEN verweist in diesem Zusammenhang auch auf die Vorgaben des § 4b BDSG, welcher Regelungen über die Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen trifft. In Absatz 3 der Vorschrift werden Vorgaben über die Angemessenheit des Schutzniveaus bei der Übermittlung und Verarbeitung von Daten ins Ausland gemacht, welche durch die hier gegenständlichen Vorgaben letztlich ausgehebelt würden.

Darüber hinaus wurde im gegenständlichen Entwurf das Kriterium der Endkundenbeziehung gestrichen, so dass es gerade auch im Bereich von Wholesale-Angeboten zu Doppelspeicherungen kommt, die entsprechend zu speichernden Daten über den Teilnehmer jedoch gar nicht vorhanden sind.

Schließlich ist der Adressatenkreis der Regelung unverhältnismäßig weit gefasst. Die Einleitung zum Gesetzentwurf räumt selbst ein, dass eine, im Verhältnis zu ihren geringen Marktanteilen erhebliche Anzahl von Unternehmen unbillig hart betroffen sein könnte – ergreift jedoch keine wirksamen Maßnahmen, wie etwa die Einführung einer Bagatellgrenze oder der Möglichkeit von Ausnahmekriterien, um eine entsprechende Verhältnismäßigkeit wieder herzustellen.

Die erheblichen Anforderungen an die Speicherung nach dem gegenständlichen Gesetzentwurf stehen – gerade sofern Daten bereits aus anderen Zwecken gespeichert werden – in keinem Verhältnis. Dies gilt besonders

bezüglich einer zusätzlichen Speicherverpflichtung im Inland, was nach Auffassung der IEN auch europarechtlich bedenklich ist.

II. Im Einzelnen

1. § 113a TKG-E: Zum Kreis der Verpflichteten

Der neue § 113a Abs. 1 TKG-E verpflichtet zur Speicherung ausnahmslos alle „Erbringer öffentlich zugänglicher Telekommunikationsdienste“. Nicht ersichtlich ist zunächst, warum der Entwurf ein neues Merkmal des „Erbringers von Telekommunikationsdiensten“ schafft und worin der Unterschied zur sonst üblichen Definition des „Anbieters von Telekommunikationsdiensten“ liegen soll. Der Begriff des „Erbringers“ ist den Definitionen des TKG fremd.

Im Hinblick auf den Kreis der Verpflichteten ist zudem die gebotene Verhältnismäßigkeit nicht gegeben. So wird in der Einleitung des Gesetzentwurfs zutreffend bereits die Unverhältnismäßigkeit festgestellt: *„Von den vorhandenen ca. 1.000 Erbringern öffentlich zugänglicher Telekommunikationsdienste sind 20 so groß, dass sie 98 Prozent des Marktes abdecken, die übrigen sind kleine bis mittlere Unternehmen, die sich voraussichtlich häufig auf eine unbillige Härte berufen werden.“* (S.4) Dennoch sollen 980 Unternehmen unterschiedslos verpflichtet und damit unverhältnismäßig hart betroffen werden. Die lediglich theoretisch bestehende Möglichkeit einer Entschädigung nach § 113 a Abs. 2 TKG-E ändert an dieser Unbilligkeit nichts – zumal diese Regelung auch ungenau gefasst ist.

Ferner ist nicht ersichtlich, weshalb lediglich 1.000 Unternehmen betrachtet werden: Die Liste der BNetzA mit den vom Gesetz betroffenen Unternehmen, auf welche in der Begründung des Gesetzes auch Bezug genommen wird, ist deutlich länger.

Der gegenständliche Entwurf ist jedenfalls bereits vor dem Hintergrund der Entscheidung des BVerfG (Urteil vom 02.03.2010 AZ 1 BvR 256/08) grundsätzlich problematisch: Festgestellt wurde in dem der Entscheidung des BVerfG zugrundeliegenden Fall bezüglich eines einzelnen Unternehmens insbesondere, dass die Speicherpflicht im Hinblick auf die finanziellen Lasten der Unternehmen nicht von vornherein unverhältnismäßig sei. Das BVerfG hat aber im Rahmen der Begründung folgende Ausführungen gemacht: So wie die Telekommunikationsunternehmen die neuen Chancen der Telekommunikationstechnik zur Gewinnerzielung nutzen könnten, müssten sie auch die Kosten für die Einhegung der neuen Sicherheitsrisiken, die mit der Telekommunikation verbunden sind, übernehmen und in ihren Preisen verarbeiten. Ein Gesetz, das die Berufsausübung in der Weise regelt, dass es Privaten bei der Ausübung ihres Berufs Pflichten auferlegt und dabei regelmäßig eine Vielzahl von Personen betreffe, sei nicht bereits dann unverhältnismäßig, wenn es einzelne Betroffene unzumutbar

belaste, sondern erst dann, wenn es bei einer größeren Betroffenenengruppe das Übermaßverbot verletze.

Seite 4 | 14
12.06.2015

Unter Berücksichtigung der Ausführungen des BVerfG ist zunächst festzuhalten, dass bereits ausweislich der Ausführungen im gegenständlichen Gesetzentwurf selbst nicht nur einzelne Betroffene übermäßig belastet werden, sondern vielmehr mehr als 980 Unternehmen, die gemeinsam gerade einmal 2% des relevanten Datenbestandes unterhalten. Hinzu kommt, dass unter diesen Betroffenen eine erhebliche Anzahl von Anbietern existiert, die überwiegend *Geschäftskunden und Behörden* mit Telekommunikationsdienstleistungen versorgen und infolge dieser Kundenstruktur darüber hinaus noch in weit unverhältnismäßiger Weise von den Verpflichtungen zur Vorratsdatenspeicherung betroffen sind: Für den Kundenkreis der Geschäftskundenanbieter wie den IEN-Mitgliedsunternehmen gehören meist große Banken, börsennotierte Industriekonzerne sowie zahlreiche Behörden. Bei dieser Kundenstruktur steht – belegt durch die praktischen Erfahrungen der letzten Jahre – in der Praxis nicht zu erwarten, dass jemals in nennenswertem Umfang auf Vorrat gespeicherte Daten abgefragt würden.

Darüber hinaus besteht bei dieser Kundengruppe auch nicht die Problematik der Zuordnung dynamischer IP-Adressen, deren Speicherung die Bundesregierung gerade mit dem gegenständlichen Gesetzentwurf zu erreichen versucht. Große Geschäftskunden und Behörden verwenden ausschließlich statische IP-Adressen, deren Beauskunftung auch bereits auf Basis der Abrechnungsdaten, welche heute und auch in Zukunft nach § 97 TKG parallel zu speichern sind, möglich ist.

a. Einführung einer Bagatellgrenze

Die IEN fordert daher im Hinblick im Einklang mit den Überwachungsvorgaben der Telekommunikations-Überwachungsverordnung (TKÜV) die Einfügung einer Bagatellregelung. In der TKÜV ist eine Bagatellgrenze von 10.000 Teilnehmern oder sonstige Nutzungsberechtigte in § 3 Abs. 2 Nr. 5 vorgesehen um kleine und mittlere Unternehmen (KMU) im Bereich der Informations- und Telekommunikationsindustrie nicht übermäßig zu belasten. Zudem soll diese Bagatellgrenze sicherstellen, dass die berechtigten Interessen an der Strafverfolgung kein Innovations- und Gründungshemmnis darstellen.

In diesem Zusammenhang verweist die IEN insbesondere auf die Rede der Bundeskanzlerin Merkel auf der diesjährigen CeBit, nach welcher die Bundesregierung Start-Up Unternehmen ausdrücklich fördern will¹.

¹ Rede von Dr. Angela Merkel am 16.03.2015, auszugsweise abrufbar etwa unter: <http://www.gruenderszene.de/allgemein/merkel-cebit-2015>

Eine Übertragung der genannten Grenze aus § 3 Abs. 2 Nr. 5 TKÜV in den gegenständlichen Gesetzentwurf erscheint vor dem Hintergrund des vorstehenden daher nicht nur sinnvoll, sondern auch erforderlich und geeignet, um die bestehende Unverhältnismäßigkeit der Verpflichtungen zu verringern.

Die Unverhältnismäßigkeit schlägt sich im Übrigen nicht nur hinsichtlich der Investitionskosten zur gesonderten Speicherung nieder, sondern auch hinsichtlich der Verpflichtung der Beschäftigung von mindestens zwei Personen zur Gewährleistung des Vier-Augen-Prinzips nach § 113 d TKG-E. Gerade für kleine Unternehmen bedeutet dies nicht zu rechtfertigende, laufende Kosten, ohne dass die parallel aufzubauende Struktur - gerade bei ohnehin vorhandenen Daten – irgendeinen Nutzen haben könnte. Für die bereits vorhandenen Daten entfaltet die gegenständliche Regelung keine Wirkung, denn es bleibt der bestehende Auskunftsanspruch der Behörde nach §§ 113 TKG neben dem neuen Anspruch auf die Vorratsdaten bestehen.

Da die für diese Tätigkeit hinreichend qualifizierten Administratoren für kleinere Unternehmen und insbesondere Start-Ups überhaupt in ausreichender Zahl auf dem Arbeitsmarkt verfügbar wären, um diesen Verpflichtungen nachzukommen, ist zudem ebenfalls fraglich.

b. Ausnahmeregelungen

aa. Britisches Modell

Soweit die Einführung einer Marginalgrenze der Teilnehmer im Hinblick auf die Vorratsdatenspeicherung als nicht zulässig angesehen wird, wäre dennoch eine Bagatellregelung dergestalt denkbar, dass zwar alle Unternehmen abstrakt-generell zur Speicherung verpflichtet werden, jedoch im Hinblick auf die Anbieter von Geschäftskundenprodukten für große Unternehmen und Behörden, welche nicht zu den 20 Unternehmen gehören, die 98% der relevanten Daten vorhalten, Ausnahmeregelungen vorgesehen werden.

So wäre eine Regelung in Anlehnung an die in Großbritannien getroffene Lösung denkbar. In Großbritannien hat der Gesetzgeber die Verpflichtung zur Vorratsdatenspeicherung mit größerer Flexibilität ausgestaltet. Die abstrakt-generelle Verpflichtung zur Vorratsdatenspeicherung erstreckt sich richtlinienkonform ausnahmslos auf alle TK-Unternehmen. Jedoch wählt das zuständige Ministerium dann konkret die Unternehmen aus, bei denen die VDS in kriminalistischer Hinsicht am meisten Sinn macht und eine nicht nur unerhebliche Anzahl von Abfragen in der Praxis zu erwarten sein wird.

Statt einer pauschalen und unterschiedslosen Verpflichtung aller Anbieter werden in Großbritannien lediglich die vier bis sechs größten TK-Anbieter, bei denen die größte Anzahl der Abfragen zu erwarten ist, angesprochen und dann mit diesen Unternehmen eine Lösung zur Speicherung abge-

stimmt. Dies ist zugleich auch in kriminalistischer Hinsicht effizient, denn diese großen Unternehmen wirken in aller Regel mindestens auf einer Seite der Kommunikation mit, entweder auf der des Anrufers oder des Angerufenen, und sind somit in der Praxis in der Lage, annähernd 99% der gewünschten Informationen im Rahmen der VDS zu speichern und zu beauskunften.

Weiterhin gewährt das Britische Modell den wenigen, konkret angesprochenen Unternehmen eine Erstattung der Anschaffungskosten der Speicherlösung. Obwohl hierdurch zwar auf den ersten Blick zusätzliche Kosten entstehen, schafft diese Regelung jedoch einen gerechten Ausgleich zwischen den Anbietern und reduziert die zusätzlichen Kosten auf ein Mindestmaß. Hierdurch wird zugleich eine Verteuerung von Telekommunikationsdiensten – und damit ein Standortnachteil für in Großbritannien ansässige Nachfrager von Telekommunikationsdiensten – vermieden.

bb. Australisches Modell

Auch Australien hat bei der Implementierung von gesetzlichen Vorgaben für die Vorratsdatenspeicherung in diesem Jahr von dieser Möglichkeit Gebrauch gemacht. Im März 2015 hat das australische Parlament dem Entwurf für ein sehr weitreichendes Gesetz zur Vorratsdatenspeicherung (VDS) zugestimmt. Das Gesetz: TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) AMENDMENT (DATA RETENTION) BILL 2014 bringt eine deutlich weitergehende Pflicht zur Speicherung von Benutzerdaten, als die im gegenständlichen Entwurf diskutierte Vorratsdatenspeicherung. Dennoch enthält das Gesetz einen Aspekt, dessen Übernahme – bei aller grundsätzlichen Kritik – auch unserem Gesetzgeber in der parlamentarischen Beratung zu raten wäre:

In der australischen Fassung einer VDS wird der ACMA, der “Australia Media and Communications Authority”, als Regulierungsbehörde die Möglichkeit eröffnet, bestimmte Services bzw. Anbietergruppen von der Überwachungspflicht zu befreien, um dem Gebot der Verhältnismäßigkeit und Datensparsamkeit individuell angemessen Rechnung tragen zu können. Ein Communications Access Coordinator (CAC) der beim Generalstaatsanwalt angesiedelt ist, ist zudem als koordinierendes Bindeglied zwischen Ermittlungsbehörden und verpflichteten Unternehmen u.a. dafür zuständig, die konkreten Ausnahmen näher zu definieren (Hervorhebungen nur hier):

Division 3 of Part 5-1A—Exemptions

Section 187K—The Communications Access Co-ordinator may grant exemptions or variations

7. *Section 187K provides that the CAC may exempt a service provider from the mandatory data retention and information security obligations imposed on the service provider under Part 5-1A of the TIA*

Act, or vary the obligations that the service provider is subject to. The CAC may grant this exemption or variation on his or her own volition or on application by a service provider.

8. *This exemption and variation scheme is intended to permit exemptions or variations to be granted in a range of circumstances, including where imposing data retention obligations for a particular relevant service would be of limited utility for law enforcement and national security purposes.*
9. *The scheme provided by this section is modelled on existing sections 192 and 193 of the TIA Act, which provide that the CAC or the ACMA may grant exemptions in relation to the interception capability obligations of service providers.*

(...)

6. *The decision of the CAC may be expressed broadly. In making a determination, the CAC may specify service providers in any way, for example by reference to a class of service providers, and is not required to refer specifically to individual service providers. For example, the CAC may specify that any service provider that provides Internet Protocol television (IPTV) services is not required to retain any data in relation to its IPTV service. Similarly, an exemption or variation may be expressed to apply to a class of obligations.*

7. (...)

8. *The data retention obligations under Part 5-1A may cover services that are of limited or no relevance to law enforcement or national security. These could include services relating to IPTV, content on demand, the leasing of dark fibre and machine-to-machine communications. Subsection 187K(1) recognises that, in certain instances, a service provider may not achieve complete technical compliance in relation to a particular service or some aspect of that service, or that the non-compliance has limited implications for law enforcement or national security agencies.*

(....)

19. *Subsection 187K(8) enables the CAC to take into account any other relevant matter when deciding whether or not to grant an exemption or variation, which might include relevant technological or industry factors such as:*
 - *the size, market share and national security and law enforcement risk profile of the service provider*

- the degree to which an exemption would effectively mitigate costs and minimise impacts on the service provider's cash flow, and
- the pre-existing business plans of the service provider.

Section 187KA– Review of exemption or variation decisions by the ACMA

CAC exemption regime

22. Division 3, Part 5-1A of the TIA Act provides a mechanism for the CAC to grant an exemption to a service provider from some or all of the mandatory data retention obligations. The scheme operates in a similar way to the existing exemption regime for interception capability under section 192 of the TIA Act.
23. Under the data retention exemption scheme, a service provider may apply to the CAC for an exemption and the CAC is required to make a decision on the application within a specified period. The exemption may also stipulate expiration dates or circumstances whereby the service provider must reapply for an exemption.
24. The CAC exemption facility indirectly strengthens the right to privacy of individual customers in that it provides a method of reducing data retention obligations, for example, in circumstances where the volume of data to be retained is disproportionate to the interests of law enforcement and national security.

2. § 113 a Abs. 1 TKG-E: Unbegründete Ausweitung des Adressatenkreises

Die bisherige Regelung im TKG bezieht sich auf die Anbieter von TK-diensten für Endnutzer. Diese Beschränkung wurde nunmehr aufgegeben. Stattdessen sollen alle Anbieter, wie insbesondere auch Wholesale- oder Zwischenhändler, virtuelle Netzbetreiber (VNB), von der BNetzA angeordnete Angebote von Terminierungsleistungen für andere Netzbetreiber, betroffen sein.

Die IEN erachtet die Doppelverpflichtung zur Speicherung, welche gegen das Gebot der Datensparsamkeit verstößt (dazu unter II. 3.) besonders im Bezug auf Wholesale-Angebote als problematisch. Da § 113a und b Abs. 2 TKG-E die „Erbringer öffentlich zugänglicher Telefondienste“ pauschal verpflichtet und im Gegensatz zur bisherigen Formulierung des § 113a TKG das Kriterium der „Endnutzer“ entfallen ist, werden sowohl diejenigen zur Speicherung verpflichtet, die über die jeweilige Beziehung zum Endkunden verfügen als auch zusätzlich diejenigen Anbieter, die z.B. lediglich Transitleistungen für dieselben Daten erbringen.

Auch die Vorgaben des § 113a Abs. 1 Satz 2 TKG-E sehen lediglich gesonderte Verpflichtungen für diejenigen Diensteanbieter vor, die die zu speichernden Daten nicht alle selbst erzeugen oder verarbeiten. Diese Regelung zielt auf die andernfalls mögliche Umgehung der Speicherverpflichtung für bei Resale-Nachfragern ab und nicht auf die Anbieter von Vorleistungsprodukten. Wesentlich ist jedoch stets das Vorliegen einer Endkundenbeziehung, wenn für staatliche Zwecke Auskünfte über die an einer Kommunikation Beteiligten gewünscht sind. Darüber hinaus ergibt sich aus dieser Regelung auch kein Mehrwert, da die jeweiligen „Großhändler“ regelmäßig den Ermittlungsbehörde unbekannt sind und daher auch keine Anfragen zur Beauskunftung erhalten werden.

Um entsprechend überflüssige und somit unverhältnismäßige Doppelspeicherungen zu vermeiden, sollte in den § 113 a und ggf. b TKG-E eingefügt werden: „Erbringer öffentlich zugänglicher Telefondienste für Endnutzer“ (§ 3 Nr. 8 TKG).

3. § 113 b Abs. 1 TKG-E: Doppelverpflichtung zur Speicherung

Die nunmehr geschaffene Pflicht nach § 113b TKG-E zur Speicherung von Verkehrsdaten samt Fristen zur Löschung nach 10 Wochen soll parallel zu der Speichermöglichkeit für Abrechnungszwecke nach § 97 TKG bestehen. Dies bedeutet, dass die ohnehin gespeicherten Daten in den Billing-Systemen der Unternehmen nun separat nochmal zu speichern wären. Diese Verpflichtung zur Speicherung von Daten, die bereits existieren, begründet einen klaren Verstoß gegen das Gebot der Datensparsamkeit nach § 3a BDSG.

Die IEN weist nochmals ausdrücklich darauf hin, dass gerade im Bereich der Angebote für große Geschäftskunden lediglich statische IP-Adressen verwendet werden, so dass kein Mehrwert durch die gesonderte, parallele Speicherung von Daten nach dem gegenständlichen Gesetzentwurf entsteht.

Zudem ist die Speicherverpflichtung nach § 113d 2 TKG-E gerade der ohnehin vorhandenen Daten „in gesonderten, von den für die üblichen betrieblichen Aufgaben getrennten Speichereinrichtungen“ unverhältnismäßig. Sie steht zudem im Widerspruch zur Annahme, dass „Unternehmen teilweise auf die bereits getätigten Investitionen zurückgreifen können“ (S. 3 des Gesetzentwurfs). Etwaige Rückgriffsmöglichkeiten auf bestehende Investitionen sind in der Realität insbesondere wegen der Verpflichtung zur Speicherung im Inland (dazu unter II. 4.) marginal, zudem erfordert die Erfüllung des vier-Augen-Prinzips nach § 113d 5 TKG-E weiteren Personalaufwand. Die automatisierte Übermittlung der Daten an die berechtigten Stellen ist in „getrennten“ Systemen auch nicht in der zugleich vom Gesetz geforderten leichten Abrufbarkeit realisierbar.

4. Verpflichtung zur Datenspeicherung im Inland

Nach § 113b Abs. 1 TKG-E werden die betroffenen Anbieter verpflichtet, die Daten im Inland zu speichern. Eine Begründung findet sich auf S. 41 des Gesetzentwurfs: „Abweichend von § 113a TKG a. F. sind die Daten ausschließlich im Inland zu speichern; eine Erfüllung der Speicherpflicht durch die Speicherung in einem anderen Mitgliedstaat der Europäischen Union ist nicht mehr vorgesehen. Die Beschränkung der Speicherung der Vorratsdaten auf das Inland ist eine Beschränkung der Dienstleistungsfreiheit im Sinne von Artikel 56 AEUV. Eine solche lässt sich rechtfertigen, wenn sie notwendig ist, um zwingenden Gründen des Allgemeininteresses gerecht zu werden und wenn sie zudem verhältnismäßig ist.[...] Bei einer Speicherung im europäischen Ausland könnte nicht ausgeschlossen werden, dass entgegen der strengen Verwendungsbeschränkung in § 113c TKG-E der ausländische Staat nach Maßgabe seines (innerstaatlichen) Rechts Zugriff auf die auf seinem Hoheitsgebiet gespeicherten Daten nimmt, was angesichts jüngerer Erfahrungen nicht als nur theoretische Gefahr erscheint.“

Die IEN weist darauf hin, dass eine derartige Herleitung der Verhältnismäßigkeit bei grenzüberschreitenden Diensten besonders für ein und denselben grenzüberschreitend aus dem Ausland agierenden Kunden nicht zu überzeugen vermag. Multinationale Anbieter von Telekommunikationsdienstleistungen, die international tätige Kundenkreise versorgen, bedienen sich zentraler Strukturen in einem Mitgliedsstaat der EU, da dieses gerade dem Kundenwunsch entspricht. Diese werden erheblich in der Ausübung ihrer unternehmerischen Tätigkeit beschränkt und damit entgegen der Regelungen zum Binnenmarkt der EU Nachteile gegenüber Unternehmen mit Hauptsitz in Deutschland erleiden.

Gerade im Hinblick auf Geschäftskunden der IEN-Mitgliedsunternehmen, die selbst europaweit agieren und ihre Telekommunikationsdienstleistungen von einem einzigen TK-Anbieter einkaufen, erfolgt vielfach eine zentrale Organisation der TK-Dienstleistungen. Unterschiedliche Speichervorgaben hinsichtlich der Daten ein und desselben Unternehmens führen zu unnötigem Mehraufwand, erhöhen damit die Kosten und bedeuten für betreffenden TK-Anbieter somit erhebliche Hürden für die Zurverfügungstellung marktgerechter Angebote - ohne dass es dafür jedoch eine sachlich tragfähige Begründung gäbe.

Insoweit stehen die Ausführungen in der Begründung aus Sicht der IEN auch im klaren Widerspruch zu den Vorgaben des § 4b BDSG zur Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen, insbesondere zum Absatz 3, welcher die Angemessenheit des Schutzniveaus betrifft. Die in Art 25 Abs. 2 EU-DatenSchRL zur Beurteilung eines angemessenen Datenschutzniveaus beispielhaft vorgegebenen Kriterien wurden in Absatz 3 nahezu wörtlich

übernommen. Sofern ein Unternehmen ein den europäischen und deutschen Schutzanforderungen angemessenes Datenschutzniveau im Ausland nachweisen kann, steht nach § 4b BDSG einer Speicherung/Datenverarbeitung nichts im Wege, da dem Betroffenen keine Einbußen hinsichtlich seiner Datenschutzposition drohen. Es ist kein Grund ersichtlich, weshalb diese Vorgaben nun hinsichtlich des gegenständlichen Speicherungsansatzes keine Geltung mehr erlangen sollen.

Soweit die Bundesregierung hier Bedenken mit Blick auf ein unterschiedliches Datenschutzniveau in den jeweiligen Mitgliedsstaaten hat, werden sich diese nur im Rahmen der Neuregelung einer Datenschutzgrundverordnung politisch und rechtlich lösen lassen. Dies kann nicht im grenzüberschreitenden Fluss von Daten durch die hier offensichtlich vorgesehene Re-Nationalisierung von Speicher-Infrastrukturen gelöst werden.

Schließlich weist die IEN darauf hin, dass die unter Umständen viel umfanglicheren Daten, die zu Abrechnungszwecken nach § 97 TKG richtigerweise auch weiterhin im Ausland gespeichert werden dürfen, bereits beauskunftet werden (müssen). Bereits damit wird die nunmehr vorgesehene Regelung ad absurdum geführt. Die nunmehr zu speichernden Vorratsdaten stellen lediglich eine (begrenzte) Kopie dessen dar, was gegebenenfalls auf Basis des Rechts anderer europäischer Staaten von dem betroffenen Unternehmen im Ausland beauskunftet werden müssen. Dagegen kann sich aber selbst ein rein deutscher TK-Anbieter nicht wehren, soweit er im Ausland irgendwelche Infrastrukturen unterhält.

Die IEN fordert daher die Möglichkeit zur zentralisierten Datenspeicherung im Einklang mit den europäischen Vorgaben beizubehalten.

5. § 113b Abs. 2 und 3 TKG-E: Erhebliche Rechtsunsicherheiten

Der § 113b (2) 5 TKG-E sieht nun auch die Verpflichtung zur Speicherung von IP Adressen bei IP Telefonie vor. Die IEN weist darauf hin, dass gerade hinsichtlich dieser Vorgabe einige technische Missverständnisse vorliegen dürften:

Bei VoIP-Diensten handelt es sich im Datenverkehr nicht von anderen Daten unterscheidbare Datenpakete. Soweit im gegenständlichen Entwurf festgelegt werden soll, dass nur für diese Dienste die IP-Adressen gespeichert werden sollen, handelt es somit um die Analyse von Inhalten der Datenpakete. Diese aber sind nur identifizier- und damit unterscheidbar, wenn der TK-Anbieter automatisiert den Inhalt jedes Paketes untersucht (deep packet inspection).

Darüber hinaus stellt sich die Frage, wie sich diese Regelung konkret auswirkt, wenn diese Daten bei dem jeweiligen Anbieter nicht vorhanden sind –

etwa weil diese Daten aufgrund der konkreten Ausgestaltung des vom Kunden verwendeten Produktes nicht verarbeitet werden. Sollte dies zu einem faktischen Verbot von bestimmten Diensten führen, stellt dies eine erhebliche Beschränkung des Wettbewerbs dar und widerspricht auch dem Gedanken der Neutralität des Datentransporteurs.

Soweit in § 113 b Abs. 3 Nr. 2 TKG-E vorgesehen ist, dass die Erbringer öffentlich zugänglicher Internetzugangsdienste „eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, sowie eine zugewiesene Benutzerkennung“ speichern sollen, führt dies zu erheblichen Rechtsunsicherheiten. In der früheren Fassung des § 113 b TKG war diese weitergehende Formulierung („sowie“) nicht enthalten.

Nach Auffassung der IEN kann daher nicht ausgeschlossen werden, dass nunmehr eine extrem weitgehende Anforderung gestellt wird und neben der IP-Adresse („sowie“) jede andere möglicherweise vorhandene Benutzerkennung zu speichern ist, die eine eindeutige Identifizierung des Teilnehmers erlaubt.

In diesem Zusammenhang stellt sich ebenfalls die Frage, was diese Verpflichtung für Auswirkungen auf Angebote haben soll, bei denen eine solche Eindeutigkeit des Anschlusses oder des Nutzers nicht besteht und ob nicht gar eine Sperrung dieser Dienste erzwungen würde.

6. § 113d TKG-E: Unverhältnismäßigkeit und Zielverfehlung

In § 113 d TKG-E werden Vorgaben getroffen, die die Sicherheit der Daten gewährleisten sollen.

In diesem Zusammenhang verweist die IEN auf die obigen Ausführungen zur Unverhältnismäßigkeit der Verpflichtung, wenn von sämtlichen Unternehmen, ungeachtet von Relevanz der zu speichernden Daten, Kundenstrukturen und Marktanteilen, verlangt würde, gesonderte Speichereinrichtungen vorzuhalten, besonders qualifiziertes Personal aufzustocken und zudem unspezifische Regelungen zu Verschlüsselung („besonders sicher“) nachkommen sollen.

Gerade in diesem Zusammenhang ist darauf hinzuweisen, dass die extrem weitreichenden Vorgaben zur gesonderten Speicherung und die eindeutige Aufforderung zur Personalerweiterung einen erheblichen Eingriff in die betriebliche Ausgestaltung der Unternehmen bedeutet und entsprechend zu kompensieren ist.

Gleichzeitig laufen diese Vorgaben, wie bereits dargestellt, ohnehin ins Leere, da gerade im Bereich der TK-Angebote für große Unternehmenskunden und Behörden sämtliche Daten – inklusive der statischen IP-

Adressen - ohnehin für Abrechnungszwecke nach § 97 TKG gespeichert werden und mithin gleichzeitig - ohne diese erheblichen, kostenintensiven Maßnahmen gesondert vorzuhalten – heute schon entsprechend auch aus den bereits vorhandenen für geschäftszwecke zu speichernden Daten abgerufen und beauskunftet werden können.

7. § 202 d StGB-E – Datenhehlerei streichen

Die neu eingefügten Vorschriften zur Datenhehlerei, die mit diesem Gesetzentwurf verabschiedet werden sollen, haben keinen Bezug zur Vorratsdatenspeicherung und sind aus Sicht der IEN schließlich ebenfalls zu kritisieren.

Abgesehen von allgemein gültigen Kritikpunkten, wie der Frage der Reichweite dieser Regelung vor dem Hintergrund des engen Presseprivilegs und der Zielverfehlung bezüglich des Missbrauchs von Daten durch ehemalige Mitarbeiter, stellt gerade die drohende „Kriminalisierung“ von Mitarbeitern, die wegen der Verpflichtung der Vorratsdatenspeicherung mit Daten umgehen müssen, ein erhebliches Problem für die betroffenen TK-Anbieter dar.

Denn diejenigen Mitarbeiter, welche etwa für die fristgemäße Löschung der Daten zuständig sind, laufen nach den derzeit vorgesehenen Regelungen bereits im Fall der verspäteten Löschung der Daten – auch wenn dies letztlich nicht von ihnen verschuldet ist – Gefahr, wegen § 202 StGB-E belangt zu werden.

Abgesehen von der Frage, ob diese Fälle überhaupt betroffen sein sollen, stellt dies die betroffenen Unternehmen vor die Problematik, dass die Mitarbeiter aufgrund des Risikos der persönlichen Strafbarkeit nicht gewillt sind, diese Aufgabe überhaupt noch zu übernehmen.

8. Verlängerung der Übergangsregelung

Die IEN erachtet schließlich die Umsetzungsfrist als zu kurz bemessen (§ 150 Abs. 13 TKG-E, § 12 StPO, S. 16 und 50 des Gesetzentwurfs). Zwar sollen den TK-Anbietern offiziell 18 Monate zur Verfügung stehen – tatsächlich sind es jedoch lediglich sechs Monate, da erst nach 12 Monaten der Anforderungskatalog der BNetzA zur Verfügung gestellt werden muss, auf dessen Grundlage die Anbieter erst eine Umsetzung vornehmen können. Eine vorherige Umsetzung in Unkenntnis des Anforderungskatalogs und in dem Risiko, die dortigen Vorgaben nicht zu erfüllen, wäre für die Verpflichteten unsinnig.

In diesem Zusammenhang weist die IEN auch noch einmal darauf hin, dass die betroffenen TK-Anbieter bereits auf Basis des früheren, verfassungswidrigen Gesetzes über die Vorratsdatenspeicherung erhebliche vergebli-



INITIATIVE
EUROPÄISCHER
NETZBETREIBER

che Investitionen tätigen mussten und daher jedweder Zwang zu im Nachhinein als unbrauchbar darstellenden Investitionen zu vermeiden ist.

Seite 14 | 14
12.06.2015

Aufgrund des erheblichen Aufwands sollte die Umsetzungsfrist daher entsprechend mindestens auf 18 Monate nach Ergehen des Anforderungskatalogs verlängert werden.

Für Rückfragen stehen die Vertreter der Mitgliedsunternehmen der IEN sowie ich selbst jederzeit gern zur Verfügung. Die Stellungnahme enthält keine Betriebs- und Geschäftsgeheimnisse.