Erläuterungen

Allgemeiner Teil

A. Zwischenstaatliche Verpflichtungen

1. Rechtsakte der EU

a) Richtlinie 2006/24/EG vom 15. März 2006 über die Vorratsspeicherung von Daten

Die „Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG“ war von Österreich gemäß ihrem Art. 15 spätestens bis zum 15. September 2007 mit der Inkraftsetzung der erforderlichen Rechts- und Verwaltungsvorschriften umzusetzen. Österreich hat im Vorfeld auch eine Erklärung gemäß Art. 15 Abs. 3 der Richtlinie abgegeben, wonach deren Anwendung betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail bis 15. März 2009 zurückgestellt wurde. Die Umsetzung der Richtlinie soll nun bei laufendem Vertragsverletzungsverfahren nachgeholt werden.

Die Richtlinie 2006/24/EG verfügt in Art. 3, dass die Mitgliedstaaten durch entsprechende Maßnahmen dafür Sorge zu tragen haben, dass die in Art. 5 der Richtlinie genannten Datenkategorien, soweit sie im Rahmen ihrer Zuständigkeit im Zuge der Bereitstellung der betreffenden Kommunikationsdienste von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, gemäß den Bestimmungen der vorliegenden Richtlinie auf Vorrat gespeichert werden. Im Sinne des Art. 1 Abs. 2 gilt diese Richtlinie für Verkehrs- und Standortdaten sowohl von juristischen als auch von natürlichen Personen sowie für alle damit in Zusammenhang stehende Daten, die zur Feststellung des Teilnehmers oder registrierten Benutzers erforderlich sind. Sie gilt gemäß Art. 5 Abs. 2 nicht für den Inhalt elektronischer Nachrichtenübermittlungen einschließlich solcher Informationen, die mit Hilfe eines elektronischen Kommunikationsnetzes abgerufen werden. Art. 6 der Richtlinie bestimmt, dass die in Art. 5 angegebenen Datenkategorien für einen Zeitraum von mindestens sechs Monaten und höchstens zwei Jahren ab dem Zeitpunkt der Kommunikation auf Vorrat gespeichert werden müssen. Gemäß Art. 8 haben die Mitgliedstaaten sicherzustellen, dass die in Art. 5 genannten Daten gemäß den Bestimmungen dieser Richtlinie so gespeichert werden, dass sie und alle sonstigen damit zusammenhängenden erforderlichen Informationen unverzüglich an die zuständigen Behörden auf deren Anfrage hin weitergeleitet werden können. Mit dieser Richtlinie sollen gemäß deren Art. 1 Abs. 1 die Vorschriften der Mitgliedstaaten über die Pflichten von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes im Zusammenhang mit der Vorratsspeicherung bestimmter Daten, die von ihnen erzeugt oder verarbeitet werden, harmonisiert werden, um sicherzustellen, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen.

Im Detail regelt die Richtlinie:

i. Welche Daten sind auf Vorrat zu speichern?

Nach den Vorgaben der Richtlinie sind jene Daten (im Folgenden als Vorratsdaten bezeichnet, siehe dazu auch Art. 5 der Richtlinie) auf Vorrat zu speichern, die benötigt werden

- zur Rückverfolgung und Identifizierung der Quelle einer Nachricht (wie Rufnummer, Name und Anschrift des Teilnehmers, Benutzerkennung oder die zugewiesene IP-Adresse bei Internetnutzung),
- zur Identifizierung des Adressaten einer Nachricht (wie die angewählte Rufnummer, Name und Anschrift des Teilnehmers und die Benutzerkennung),
- zur Bestimmung von Datum, Uhrzeit und Dauer der Nachrichtenübermittlung,
- zur Bestimmung der Art der Nachrichtenübermittlung benötigte Daten (der in Anspruch genommene Telefon- oder Internetdienst),
- zur Bestimmung der Endeinrichtung von Benutzern benötigte Daten (wie IMSI und IMEI) und
- zur Bestimmung des Standorts mobiler Geräte.

Nicht erfasst werden soll hingegen der Inhalt der Kommunikation. In diesem Sinne normiert Art. 5 Abs. 2 der Richtlinie ausdrücklich, dass keinerlei Daten gespeichert werden dürfen, die Aufschluss über den

Inhalt der Kommunikation geben. Jedoch besteht das Problem, dass häufig eine klare Trennung zwischen Verkehrsdaten (einschließlich Standortdaten) und jenen Daten, die Aufschluss über den Inhalt einer Kommunikation geben, nicht möglich ist.[1] Zwar ist die inhaltliche Aussagekraft von Verkehrsdaten keine einheitliche, sondern variiert je nach Datenkategorie, grundsätzlich können aber „bloße“ Verkehrsdaten über eine inhaltliche Aussagekraft verfügen, mitunter sogar Aufschluss über den Inhalt einer Kommunikation geben.[2]

ii. Wie sind die Daten zu speichern?

Die Richtlinie normiert, dass Vorratsdaten so zu speichern sind, dass

- sie von der gleichen Qualität sind und der gleichen Sicherheit und dem gleichen Schutz unterliegen wie die im Netz vorhandenen Daten (Art. 7 lit. a der Richtlinie);
- geeignete technische und organisatorische Maßnahmen getroffenen werden, um die Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust oder zufällige Änderung, unberechtigte oder unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung oder Verarbeitung zu schützen (Art. 7 lit. b der Richtlinie);
- geeignete technische und organisatorische Maßnahmen getroffen werden, um sicherzustellen, dass der Zugang zu den Daten ausschließlich besonders ermächtigten Personen vorbehalten ist (Art. 7 lit. c der Richtlinie);
- sie auf entsprechende Anfrage hin unverzüglich an die zuständige Behörde weitergeleitet werden können (Art. 8 der Richtlinie).

Die ersten drei dieser Bestimmungen finden sich in der Richtlinie unter der Überschrift „Datenschutz und Datensicherheit“. Wiewohl die Grenzen der Datensicherheit mit jenen des Datenschutzes in Teilbereichen verschwimmen,[3] stand bei der Abfassung dieser Bestimmung offenkundig mehr das Ziel der Datensicherheit und insbesondere der Datenrichtigkeit im Vordergrund als jenes des Datenschutzes. Dennoch weisen Teile dieser Bestimmungen des Art. 7 auch datenschutzrechtliche Teilaspekte auf. So muss der lit. b des Art. 7, der zu Folge der Zugang zu Vorratsdaten „ausschließlich besonders ermächtigten Personen“ vorzubehalten ist, (auch) ein datenschutzrechtlicher Charakter zugebilligt werden.[4]

Obgleich von den zuständigen Ausschüssen des EU-Parlaments zahlreiche Änderungsanträge mit datenschutzrechtlicher Schwerpunktsetzung ausgearbeitet und in den Ausschüssen fraktionsübergreifend

---

1 So kann mitunter aus "bloßen" Verkehrsdaten durchaus auf den Inhalt der Kommunikation rückgeschlossen werden. Beispielsweise sei auf einen Anruf bei der Aidshilfe, Rat auf Draht oder einer ähnlichen Beratungseinrichtung verwiesen. Diese Anrufe werden in aller Regel eine entsprechende Beratung oder Hilfestellung und damit verbundene Inhalte zum Gegenstand haben. Ein Anruf bei einer Anwaltskanzlei wird in aller Regel eine anwaltliche Beratung zum Gegenstand haben, wie Telefonate eines Geistlichen regelmäßig einen seelsorgerischen Hintergrund haben. Nichts anderes gilt für andere Formen der Kommunikation. Insbesondere bei der Korrespondenz via Email tritt das (wahrscheinliche) Gesprächsthema und somit der (wahrscheinliche) Gesprächsinhalt regelmäßig noch unmittelbarer zu Tage als "bloß" bei einer Telefonnummer; dies, da das Tätigkeitsfeld des Emailadresseninhabers oftmals unmittelbar aus der Adresse hervorgeht.

2 Der allfällige Einwand, dass der aus den Verkehrsdaten via Rückschluss indizierte Inhalt des Gesprächs nicht zwingend den tatsächlichen Gegebenheiten entsprechen muss, geht insofern ins Leere, als der Richtliniengeber in Art. 5 Abs. 2 nicht von Inhaltsdaten im engeren Sinn, sondern lediglich von Daten spricht, die "Aufschluss über den Inhalt der Kommunikation geben". Diese Formulierung weist zudem in auffallender Weise Parallelen zu Art. 8 Abs. 1 der Richtlinie 95/46/EG auf. Dieser Bestimmung zu Folge dürfen Daten, "aus denen die rassische und ethnische Herkunft, politische Meinungen (...) hervorgehen sowie (...) Daten über die Gesundheit oder Sexualleben" (so genannte "sensible personenbezogene Daten") grundsätzlich nicht verarbeitet werden. Für die "Sensibilität" eines Datums ist nun keinesfalls erforderlich, dass das sensible Faktum, also etwa die ethnische Herkunft oder die politische Meinung, selbst Gegenstand des Datums ist, sondern es genügt, wenn auf dieses Datum rückgeschlossen werden kann. Als Beispiel sei auf die Mitgliedschaft bei einer Vereinigung, der die Nähe zu einer bestimmten politischen Partei nachgesagt wird, verwiesen. Das Datum "Mitgliedschaft" bei dieser Vereinigung wäre ein sensibles, obgleich die "politische Meinung", also das die Sensibilität begründende Faktum, nicht selbst Gegenstand des Datums ist, sondern aus der Mitgliedschaft auf diese nur geschlossen werden kann. Ähnlich verhält es sich mit dem Datum "Besuch beim Lungenfacharzt". Dieses Datum wird als sensibles angesehen, obwohl es sich ja auch um einen Freundschaftsbesuch handeln könnte.

3 So dienen Maßnahmen, die die Daten vor unberechtigter und unrechtmäßiger Speicherung, Verarbeitung und Zuänglichmachung schützen, sowohl dem Ziel der Datensicherheit wie auch jenem des Datenschutzes.

4 Der datenschutzrechtliche Wert dieser Bedingung ist durch die weite und unbestimmte Textierung allerdings ein nur geringer. Denn "besonders ermächtigt" werden könnte auch ein sehr weit gefasster Personenkreis.

bestätigt worden waren, finden sich in der Richtlinie keine weiteren, über die vorgenannten Regelungen hinausgehenden datenschutzrechtlichen Bestimmungen.

iii. Zugang zu Daten

Hinsichtlich des Zugangs zu den Vorratsdaten sieht die Richtlinie (siehe Art. 4) lediglich vor, dass seitens der Mitgliedstaaten Maßnahmen zu erlassen sind, um sicherzustellen, dass die Daten „nur in bestimmten Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden weitergegeben werden".

Ob es sich hierbei um Gerichte, Sicherheits- oder auch andere Behörden handelt, ist dem Text der Richtlinie mangels ausdrücklicher Regelung nicht unmittelbar zu entnehmen. Dass unter den „zuständigen Behörden" im Sinne der Richtlinie freilich nicht jede nationale Behörde zu verstehen sein kann, ergibt sich schon durch die vom Richtliniengeber vorgenommene Zweckbestimmung der Vorratsspeicherung.

Art. 1 der Richtlinie sieht ausdrücklich vor, dass mit der europaweiten Einführung der Vorratsspeicherung sichergestellt werden soll, „dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten (…) zur Verfügung stehen." Damit ist vorgegeben, dass die Daten nur jenen Behörden zur Verfügung zu stehen haben, die mit der Verfolgung dieser Zwecke betraut sind, also den Strafverfolgungsbehörden.

Soweit Art. 4 also normiert, dass die Vorratsdaten an die „zuständigen Behörden" weiterzugeben sind, ist festzuhalten, dass die Autonomie des nationalen Gesetzgebers bei Bestimmung jener Behörden, die Zugriff auf die Vorratsdaten haben sollen, im vorgenannten Sinne eingeschränkt ist. Diese, schon durch eine systematische Interpretation gebotene Auslegung wird zudem auch durch einen Blick auf die Entstehungsgeschichte bestätigt.

Aus der eben dargelegten Zweckbestimmung, genauer aus der Festlegung des Zwecks der Vorratsspeicherung auf die Ermittlung, Feststellung und Verfolgung von „schweren Straftaten" folgt eine weitere Einschränkung des Zugangs zu den auf Vorrat gespeicherten Daten. Der Entstehungsgeschichte der Richtlinie lassen sich Hinweise entnehmen, wonach der EU-Gesetzgeber ursprünglich an die Bekämpfung des Terrorismus und schwerer organisierter Kriminalität als Zweckbindung der Vorratsdatenspeicherung gedacht hat (siehe die Ausführungen unter Punkt 1/a). Auch in den Erwägungsgründen (7)-(9) der Richtlinie wird der Zusammenhang mit der Bekämpfung von Terrorismus und organisierter Kriminalität mehrfach deutlich. Da aber die Richtlinie zur Festlegung des Begriffs „schwere Straftaten" auf das jeweilige nationale Recht verweist, dürfte deren Definition letztlich im – allerdings vor allem grundrechtlich begrenzten – Ermessen der Mitgliedstaaten liegen.

iv. Speicherdauer

Im Hinblick auf die Speicherdauer normiert die Richtlinie, dass die Vorratsdaten für einen Zeitraum zwischen sechs Monaten und zwei Jahren zu speichern sind (siehe Art. 6).[5] Am Ende der Vorratsspeicherungsfrist sind die Vorratsdaten zu vernichten (mit Ausnahme jener Daten, die abgerufen und gesichtet worden sind).

v. Haftung, Rechtsbehelfe und Sanktionen

Hinsichtlich dieser Themenbereiche wird in der Richtlinie festgehalten, dass die Mitgliedstaaten erforderliche Maßnahmen zu ergreifen haben, um sicherzustellen, dass die in der Datenschutzrichtlinie 95/46/EG normierte Haftung wie auch die dort vorgesehenen Rechtsbehelfe und Sanktionen auf Datenverarbeitungen nach der vorliegenden Richtlinie in vollem Umfang umgesetzt werden (siehe Art. 13).

vi. Kontrollstelle

In jedem Mitgliedstaat ist eine oder sind mehrere unabhängige Kontrollstellen zu benennen, die für die Kontrolle der Anwendung der von den Mitgliedstaaten zur Umsetzung des Art. 7 über Datenschutz und Datensicherheit erlassenen Vorschriften zuständig sind siehe Art. 9).[6]

---

5 In diesem Zusammenhang sei auf Art. 12 hingewiesen, der die Möglichkeit einer über den Zeitraum von zwei Jahren hinausgehenden Höchstspeicherdauer eröffnet, sofern "besondere Umstände die Verlängerung der maximalen Speicherungsfrist" rechtfertigen.

6 Dies dürfte eine der wenigen Bestimmungen sein, die tatsächlich auf eine Initiative des Europäischen Parlaments zurückgehen. Der LIBE-Ausschuss hatte in seinem dem Plenum vorgelegten Bericht zum Richtlinienentwurf den Änderungsantrag aufgenommen, dass jeder Mitgliedstaat "gemäß dem nationalen Recht die Datenschutzbehörde oder eine andere geeignete unabhängige Behörde beauftragt, die rechtmäßige Umsetzung dieser Richtlinie zu beaufsichtigen." Da weder der Rahmenbeschlussentwurf des Jahres 2004 noch der Richtlinienentwurf der

vii. Statistik

Schließlich normiert die Richtlinie, dass die Mitgliedstaaten eine Statistik, die keine personenbezogenen Daten enthalten darf, zu führen und jährlich an die Kommission zu übermitteln hat (siehe Art. 10). Aus dieser hat insbesondere hervorzugehen,

- in welchen Fällen im Einklang mit dem innerstaatlichen Recht Daten an die zuständige Behörde weitergegeben wurden;
- wie viel Zeit zwischen dem Zeitpunkt der Vorratsspeicherung der Daten und dem Zeitpunkt, zu dem sie von der zuständigen Behörde angefordert wurden, verging;
- in welchen Fällen die Anfragen nach Daten ergebnislos blieben.

Eine umfassende Evaluierung der Vorratspeicherung ist offenbar nicht das Ziel dieser Statistik. Eine statistische Auswertung der Anwendung der zur Umsetzung der Richtlinie erlassenen Vorschriften wäre aber als Teil einer größer angelegten Evaluierung der Richtlinie zu begrüßen, insbesondere im Hinblick darauf, ob und inwieweit der vom Richtliniengeber vorgesehene Zweck der Vorratsspeicherung erreicht werden konnte. Eine statistische Erhebung, aus der hervorgeht, inwieweit verarbeitete Daten zur Ermittlung, Feststellung und Verfolgung von schweren Straftaten beigetragen haben, ist aber gerade nicht Gegenstand der in Rede stehenden Bestimmung.

b) Weitere EU-Rechtsakte

Weiters sind noch folgende Richtlinien zu beachten, auf welche die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten auch ausdrücklich verweist, und zwar

- die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzrichtlinie) und
- die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

Während die Richtlinie 95/46/EG den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Gegenstand hat, dient die Richtlinie 2002/58/EG der Harmonisierung der Vorschriften der Mitgliedstaaten , die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft zu gewährleisten.

2. Rechtsakte außerhalb der EU

Neben der Richtlinie sind vom Gesetzgeber auch das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten des Europarates vom 28.1.1981, BGBl. Nr. 317/1988, sowie das Zusatzprotokoll zum Europäischen Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr vom 8. November 2001, BGBl. Nr. 91/2008, zu beachten.

B. Stand der Umsetzung der Richtlinie in den EU-Mitgliedstaaten

Nach derzeitigem Informationsstand haben neben Österreich einige weitere EU-Mitgliedstaaten die Richtlinie noch nicht oder noch nicht vollständig umgesetzt. Es sind dies: Griechenland, Irland, Litauen, Niederlande und Schweden. Gegen diese Staaten laufen daher auch Vertragsverletzungsverfahren vor dem EuGH, die aufgrund von Klagen der Europäischen Kommission gemäß Art. 226 EGV eingeleitet wurden.

Im Hinblick auf die Dauer der Vorratsdatenspeicherung haben sich Deutschland, Rumänien und Tschechien für eine sechsmonatige Speicherung entschieden (geplant auch in Schweden), in England, Frankreich, Finnland und Italien beträgt die Speicherfrist zwölf Monate (geplant auch von Irland) und Belgien überlegt eine Speicherdauer von 12 oder 24 Monaten.

Kommission eine Kontrollstelle iSd Art. 9 vorsah, ist mit gutem Grund anzunehmen, dass der eben angesprochene Änderungsantrag in Art. 9 aufgenommen wurde.

C. Der Begutachtungsentwurf 2007

Im Frühjahr wurde vom BMVIT bereits der Entwurf einer TKG-Novelle zur Umsetzung der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten in Begutachtung gegeben.[7] Der Gesetzentwurf sah die Erfüllung der Verpflichtung im Hinblick auf Daten betreffend Telefonfestnetz und Mobilfunk sowie jene Daten vor, die den Internetzugang, die Internet-Telefonie und Internet-E-Mail betreffen, die zur Identifizierung der Quelle einer Nachricht benötigt werden. Mit dem Entwurf wurden im Wesentlichen folgende Regelungen vorgeschlagen:

- Anpassung der Begriffsbestimmungen an jene der Richtlinie 2006/24/EG,
- Verpflichtung von Diensteanbietern und Netzbetreibern zur Vorratsspeicherung von Daten für sechs Monate,
- taxative Aufzählung der zu speichernden Daten,
- Verpflichtung zur Löschung der Daten nach Fristablauf,
- Verpflichtung von Diensteanbietern und Netzbetreibern zur Auskunftserteilung an Strafverfolgungsbehörden,
- Strafbestimmung für den Fall der Nichteinhaltung der Verpflichtung zur Vorratsspeicherung bzw. der Auskunftserteilung.

Da der Entwurf mehrfach von verschiedensten Seiten auf Kritik stieß und zeitnah eine Regierungsumbildung erfolgte, wurde er nicht mehr weiterverfolgt.

D. Grundrechtskonforme Umsetzung der Richtlinie und Grundzüge des Entwurfes

1. Grundrechtskonformität

Bei der Umsetzung der Richtlinie ist darauf zu achten, dass die gesetzlichen Bestimmungen den Anforderungen der Eingriffsvorbehalte des Art. 8 Abs. 2 EMRK insbesondere im Hinblick auf Datensicherheit und Datenschutz entsprechen . Dies steht auch mit Erwägungsgrund (17) der Richtlinie in Einklang, wonach die Mitgliedstaaten gesetzgeberische Maßnahmen zu ergreifen haben, um sicherzustellen, dass die gemäß dieser Richtlinie auf Vorrat gespeicherten Daten „nur in Übereinstimmung mit den innerstaatlichen Rechtsvorschriften und unter vollständiger Achtung der Grundrechte der betroffenen Personen an die zuständigen nationalen Behörden weitergegeben werden“.[8] Keinesfalls dürfen gemäß Art. 5 der Richtlinie Daten auf Vorrat gespeichert werden, die Aufschluss über den Inhalt einer Kommunikation geben.[9]

Nach Erwägungsgrund (25) der Richtlinie berührt diese nicht das Recht der Mitgliedstaaten, Rechtsvorschriften über den Zugang zu und die Nutzung von Daten durch die von ihnen benannten nationalen Behörden zu erlassen. Dennoch sieht Art. 4 der Richtlinie vor, dass Mitgliedstaaten sicherstellen sollen, dass die gemäß dieser Richtlinie gespeicherten Vorratsdaten nur in bestimmten Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden weitergegeben werden und im innerstaatlichen Recht unter Berücksichtigung insbesondere der EMRK in der Auslegung des EGMR das Verfahren und die Bedingungen festgelegt werden, die für den Zugang zu Vorratsdaten gemäß den Anforderungen der Notwendigkeit und der Verhältnismäßigkeit einzuhalten sind. Aus der Zusammenschau des Wortlautes „zuständigen nationalen Behörden“ mit der Zweckbindung in Art. 1 zur „Ermittlung, Feststellung und Verfolgung von schweren Straftaten“ ergibt sich klar, dass sich die Richtlinie damit eigentlich im Bereich der Dritten Säule, der Polizeilichen und Justiziellen Zusammenarbeit in Strafsachen bewegt. Weiters verpflichtet Art. 13 Abs. 1 der Richtlinie die Mitgliedstaaten sicherzustellen, dass die einzelstaatlichen Maßnahmen zur Umsetzung der in Kapitel III der Richtlinie 95/46/EG[10] niedergelegten Bestimmungen über Rechtsbehelfe, Haftung und Sanktionen im Hinblick auf die Datenverarbeitung gemäß der vorliegenden Richtlinie in vollem Umfang umgesetzt werden.

In seiner jüngeren Rechtsprechung hat der EGMR für den Fall der Sammlung und Verwendung inhaltlicher Informationen, die im Zuge geheimer optischer und akustischer Überwachungsmaßnahmen gewonnen werden und von denen alle Einwohner eines Landes betroffen sein können, bestimmte Anforderungen und Vorrausetzungen entwickelt, die sich an den Gesetzgeber richten.[11] Zwar ist die

---

7 61/ME XXIII. GP - Ministerialentwurf.

8 Siehe auch die Verweise auf Art. 7 und 8 der EU-Grundrechtecharta in Erwägungsgrund (22).

9 Jedoch dürfen bzw. müssen Verkehrsdaten gespeichert werden, selbst wenn aus ihnen gewisse Rückschlüsse auf Kommunikationsinhalte gezogen werden können, etwa zu E-Mail Kommunikationsvorgängen.

10 Siehe Fn 8.

11 Vor allem Urteil des EGMR im Fall Association for European Integration and Human Rights and Ekimdzhiev gegen Bulgarien vom 28. Juni 2007, Z. 71 ff.

Ausgangslage dieses Falles nicht mit der hier gegenständlichen Vorratsdatenspeicherung vergleichbar, doch handelt es sich um eine Form geheimer Überwachung letztlich auch dann, wenn in konkreten Verdachtsmomenten auf Vorrat gespeicherte personenbezogene Daten – noch ohne Information der betroffenen Person – verwendet werden, um eine Straftat zu ermitteln, festzustellen oder zu verfolgen, weswegen die vom EGMR entwickelten Kriterien auch hier Berücksichtigung finden können. Ausdrücklich hält der EGMR fest, dass

- ein solches Gesetz hinreichend klar formuliert sein muss, um den Betroffenen adäquate Anhaltspunkte zu den Bedingungen und Umständen zu geben, unter denen Behörden ermächtigt sind, in das Recht auf Achtung des Privatlebens und der Korrespondenz im Sinne des Art. 8 EMRK einzugreifen;
- ein solches Gesetz im Hinblick auf die Missbrauchsgefahr, die einem System geheimer Überwachung immanent ist, besonders präzise formuliert sein muss;
- es essentiell ist, dass ein solches Gesetz klare, detaillierte Bestimmungen hinsichtlich des Gegenstandes enthalten muss, insbesondere im Hinblick darauf, dass die zur Verfügung stehende Technologie immer technisch ausgefeilter wird.

Um sicherzustellen, dass diese Grundsätze effektiv implementiert werden, verlangt der EGMR folgende Mindestsicherungsmaßnahmen, die in Gesetzesform und nicht etwa als Verordnung erlassen werden müssen:

- die Natur der Straftat, die Anlass für die Überwachung bietet;
- eine Definition jener Kategorien von Personen, die der Überwachung unterworfen werden können;
- eine zeitliche Beschränkung für derartige Überwachungsmaßnahmen;
- ein Verfahren, das bei der Prüfung, Verwendung und Speicherung der Daten einzuhalten ist;
- jene Schutzmaßnahmen, die einzuhalten sind, wenn die Daten an Dritte weitergeben werden;
- die Umstände, unter denen die Daten zu löschen oder zu vernichten sind.

Zusätzlich muss das nationale Recht im Falle solcher Überwachungsmaßnahmen aufgrund der mangelnden öffentlichen Kontrolle und der Gefahr des Missbrauchs Schutz vor willkürlichen und unbegründeten Eingriffen bieten. Der EGMR betont, dass es im nationalen Recht adäquate und effektive Garantien gegen Missbrauch geben müsse.

2. Grundzüge des Entwurfs

Grundsätzlich verfolgt der Entwurf das Ziel, die Richtlinie so umzusetzen, dass zwar ihr Zweck – die Ermittlung, Feststellung und Verfolgung von schweren Straftaten mittels auf Vorrat gespeicherter personenbezogener Daten – innerstaatlich erreicht wird, um den Strafverfolgungsbehörden die Verwendung zeitgemäßer technischer Mittel zu ermöglichen, zugleich aber über legistische Vorkehrungen sichergestellt ist, dass

- die mit der Vorratsdatenspeicherung verbundenen Grundrechtseingriffe so gering wie möglich – und damit verhältnismäßig zum verfolgten Zweck – ausfallen,
- die Sicherheit der Daten sowohl bei den Telekommunikationsbetreibern als auch bei den zur Datenanwendung berechtigten Behörden bestmöglich gewährleistet ist,
- den datenschutzrechtlich erforderlichen Informationspflichten nachgekommen wird,
- alle notwendigen Rechtsmittel zur Verfolgung der datenschutzrechtlichen und grundrechtlichen Interessen Betroffener zur Verfügung stehen,
- darüber hinausgehende unabhängige datenschutzrechtliche Kontrollen vorgesehen werden, und
- die wirtschaftlichen Auswirkungen der Vorratsdatenspeicherung auf die zur Speicherung und Auskunft verpflichteten Telekommunikationsbetreiber grundrechtskonform zu gestalten.

Hinsichtlich der Speicherdauer[12] sieht der Entwurf aus folgenden Gründen einen Zeitrahmen von sechs Monaten vor (das ist die von der Richtlinie vorgegebene Mindestdauer): Einerseits stellt eine verdachtsunabhängige Speicherung personenbezogener Daten insbesondere im Hinblick auf die Missbrauchsgefahr einen erheblichen Grundrechtseingriff dar. Anderseits ist die Verwendung von Verkehrsdaten durch Strafverfolgungsbehörden in den meisten Fällen nur in einem Zeitraum von Nutzen,

12 Zur Speicherdauer siehe ausführlicher die Erläuterungen zum besonderen Teil zu § 102a Abs. 1.

der nicht länger als drei Monate zurückliegt. In der Praxis wurden und werden in Österreich von den Betreibern die für die Verrechnung bzw. den technischen Betrieb erforderlichen Daten bis maximal sechs Monate gespeichert und den Strafverfolgungsbehörden auch zur Verfügung gestellt. Überwiegend wird ein Speicherzeitraum von sechs Monaten als wünschenswert erachtet. Die grundrechtlich gebotene Abwägung und Frage nach der Verhältnismäßigkeit der Maßnahme zeigt daher, dass kein die grundrechtlichen Interessen der Betroffenen überwiegendes (öffentliches) Interesse der Strafrechtspflege an einer längeren Speicherung der Daten vorliegen dürfte.

Der Entwurf sieht vor, dass über die schon bisher für Telekommunikationsbetreiber bestehende Berechtigung zur Speicherung und Verarbeitung von Daten für betriebsnotwendige-, insbesondere für Verrechnungszwecke (in der Regel für einen Zeitraum von drei Monaten) hinaus in Umsetzung der Vorgaben der Richtlinie bestimmte, näher umschriebene Daten (insbesondere IP-Adressen) ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation zu speichern sind (vorgeschlagener § 102a TKG). Der Begriff „Vorratsdaten“ stellt keine neue Kategorie im Sinne von Verkehrsdaten, Standortdaten, Inhaltsdaten oder Stammdaten dar, sondern stellt vielmehr auf den Zweck ab, für den die Daten von den Telekommunikationsanbietern gesammelt werden müssen.

Nach dem Entwurf dürfen Verkehrsdaten außer in den im TKG geregelten Fällen weder gespeichert noch verwendet werden und sind vom Betreiber nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren (vorgeschlagener § 99 TKG). Mit dieser abschließenden Regelung soll insoweit Rechtssicherheit geschaffen werden, als damit aus anderen gesetzlichen Bestimmungen weder eine Berechtigung noch gar eine Verpflichtung zur Speicherung von Verkehrsdaten abgeleitet werden kann.

Von der Speicherpflicht nicht erfasst sind Unternehmen, die mittels Bescheid als kleine Unternehmen oder Kleinstunternehmen gemäß der Empfehlung der EU Kommission 2003/361/EG eingestuft werden (vorgeschlagener § 102a Abs. 6 TKG). Diejenigen Telekommunikationsanbieter, die zur Speicherung verpflichtet sind, gelten zur rechtlichen Klarstellung in Bezug auf Vorratsdaten als Auftraggeber des öffentlichen Bereits (vorgeschlagener § 102a Abs. 9 TKG). Die den Anbietern aus der Umsetzung der Vorratsdatenspeicherung entstehenden Kosten werden entsprechend vergütet (vorgeschlagener § 94 TKG).

Die auf Vorrat gespeicherten Daten dürfen ausschließlich aufgrund einer gerichtlichen Bewilligung und nur nach Maßgabe ausdrücklicher Gesetzesbestimmungen, die auf § 102a Bezug nehmen, zum Zweck der Ermittlung, Feststellung und Verfolgung von schweren Straftaten an die nach der StPO zuständigen Behörden übermittelt werden (vorgeschlagener § 102b TKG).

So wie bisher haben die zuständigen Behörden nach der StPO zur Verfolgung „niederschwelliger“ Straftaten (also solcher, die keine „schweren Straftaten“ sind) das Recht auf Beauskunftung der bei den Telekommunikationsbetreibern für betriebsnotwendige Zwecke gespeicherten Verkehrsdaten, wenn eine gerichtliche Bewilligung vorliegt (vorgeschlagener § 99 Abs. 5 Z 1 TKG).

Ebenso wie bisher sind die nach dem SPG zuständigen Sicherheitsbehörden für die Erfüllung ihrer im SPG geregelten präventiven Aufgaben berechtigt, Auskünfte über die bei den Telekommunikationsbetreibern für betriebsnotwendige Zwecke gespeicherten Daten einzuholen. Darüber hinaus sieht eine Verfassungsbestimmung vor, dass Sicherheitsbehörden für die Abwehr einer konkreten Gefahr für das Leben oder die Gesundheit eines Menschen unter bestimmten engen Voraussetzungen Auskünfte über Stammdaten und Standortdaten auch dann erhalten können, wenn dafür die Verwendung von Verkehrsdaten notwendig ist und deshalb in das unter Richtervorbehalt stehende Fernmeldegeheimnis eingegriffen wird (vorgeschlagener § 99 Abs. 5 Z 2 TKG).

Der Entwurf sieht eine Trennung zwischen für betriebsnotwendige Zwecke und auf Vorrat gespeicherte Daten vor, für deren Speicherung besondere Sicherungsmaßnahmen vorgesehen sind. Die Kontrolle wird der Datenschutzkommission übertragen (vorgeschlagener § 102c Abs. 1 TKG). Jeder Zugriff auf Vorratsdaten ist zudem zu protokollieren (vorgeschlagener § 102c Abs. 2 und 3 TKG). Die Beauskunftung von Daten einer Nachrichtenübermittlung nach den Bestimmungen der StPO wie auch die Beauskunftung solcher Daten an die Sicherheitsbehörden hat verschlüsselt zu erfolgen (vorgeschlagener § 94 Abs. 4 TKG).

Schließlich sieht der Entwurf entsprechende neue Verwaltungsstraftatbestände vor (vorgeschlagener § 109 TKG).

E. Kompetenzgrundlage

Die Kompetenz des Bundes zur Gesetzgebung gründet sich hinsichtlich des Datenschutzes auf die Verfassungsbestimmung des Art. 1 § 2 Abs. 1 DSG 2000, hinsichtlich der im Entwurf vorgesehenen Verfassungsbestimmungen auf den Tatbestand „Bundesverfassung“ in Art. 10 Abs. 1. Z 1 B-VG und

hinsichtlich der einfachgesetzlichen Bestimmungen auf den Tatbestand „Post- und Fernmeldewesen“ in Art. 10 Abs. 1 Z 9 B-VG.

F. Besonderheiten des Normerzeugungsverfahrens

Für die vorgeschlagenen Verfassungsbestimmungen § 98 Abs. 2 sowie § 99 Abs. 5 Z 2 ist eine qualifizierte Mehrheit bei der Beschlussfassung im Nationalrat gemäß Art. 44 Abs. 1 B-VG erforderlich.

Besonderer Teil

Zu § 90 Abs. 6 und 7

Die Ergänzung des Abs. 6 stellt nur den Umfang von Stammdatenabfragen klar. Die Neueinführung des Abs. 7 zielt darauf ab, eine eindeutige und klare Rechtsgrundlage zur Auskunft über Stammdaten an die Strafverfolgungsbehörden nach den Bestimmungen der StPO zu schaffen. Sofern keine Verkehrsdaten, insbesondere IP-Adressen (Zugangsdaten) dafür ausgewertet werden müssen, wenn also eine Nachschau bei den Vertragsdaten genügt, bedarf es dafür keiner richterlichen Genehmigung. Bei Vorliegen einer schriftlichen und begründeten Anfrage können daher auch Anfragen der Staatsanwaltschaft, bzw. in deren Auftrag der Kriminalpolizei, beauskunftet werden. Durch den Verweis auf § 76 Abs. 2 StPO wird in der Sache klargestellt, dass es sich nicht um eine Anordnung der Sicherstellung handelt. Ein darüber hinausgehender ausdrücklicher Verweis auf das Verfahren nach der StPO ist nicht erforderlich. „Begründetes Verlangen" bedeutet die Angabe des Straftatbestandes, aufgrund dessen die Ermittlungen erfolgen, sowie die bestimmte Person, auf welche sich das Auskunftsbegehren bezieht, wobei hier keine über die StPO hinausgehenden Anforderungen normiert werden. Die Regelung des § 103 Abs. 4, welche im Zusammenhang mit den Teilnehmerverzeichnissen bisher die Rechtsgrundlage für solche Auskünfte war, kann dadurch entfallen. Wie bisher beziehen sich die Auskünfte auch auf Stammdaten, deren Eintragung ins Teilnehmerverzeichnis unterbleibt. Ob für die Auskunft eine - nach dieser Bestimmung nunmehr unzulässige - Auswertung von Verkehrsdaten notwendig ist, hängt nicht davon ab, ob eine Eintragung ins Teilnehmerverzeichnis vorliegt oder nicht.

Die Bestimmung muss im korrespondierenden Zusammenhang mit der klaren Definition zur IP-Adresse in § 92 Abs. 3 Z 16 gesehen werden. Dort wird klargestellt, dass eine IP-Adresse ein Zugangsdatum (Z 4a) und damit ein Verkehrsdatum (Z4) darstellt und nur dann zugleich auch ein Stammdatum (Z 3) ist, wenn dem Kunden im Vertrag ausdrücklich eine bestimmte IP-Adresse für die Dauer des Vertrages zur ausschließlichen Nutzung zugewiesen wurde. Damit erfolgt die gesetzliche Klarstellung im Sinne der Entscheidung des OGH zu GZ 4 Ob 41/09x, wonach dynamische IP-Adressen jedenfalls als Verkehrsdaten zu behandeln sind (so im Ergebnis auch das VfGH Erkenntnis G 31/08 vom 1. Juli 2009), mit der die sonst bestehende Judikaturdivergenz zur Entscheidung des 11. Senates (in Strafsachen) des OGH, GZ 11 Os 57/05z bereinigt wird.

Nicht als Auskunft über Stammdaten sind Fälle zu beurteilen, die eine Verarbeitung der IMEI (International Mobile Station Equipment Identity) auf Seiten der Betreiber erfordern. Dem in der Praxis vorkommenden Ersuchen, Auskunft über die Identität eines Teilnehmers zu geben, der mit einem durch eine IMEI-Nummer identifizierbaren Gerät telefoniert hat, konnte auch bisher nicht auf Grundlage des § 103 Abs. 4 entsprochen werden. Die IMEI ist nämlich nicht im Teilnehmerverzeichnis enthalten und beispielsweise bei gestohlenen Geräten auch nicht mit den sonstigen Daten eines Anbieters mit einem bestimmten Teilnehmer verknüpft. Da auch hier die Verarbeitung von Verkehrsdaten notwendig ist, um die begehrte Auskunft erteilen zu können, kann einem solchen Ersuchen nur durch eine Rufdatenrückerfassung entsprochen werden (so bereits die Erläuterungen zu § 103 Abs. 4). Eine Zuordnung der IMEI zu einem bestimmten Kommunikationsvorgang ist ohne Eingriff in die Verkehrsdaten nicht möglich.

Unabhängig von der Zuordenbarkeit zu einem bestimmten Kommunikationsvorgang kann in manchen Fällen, etwa bei gleichzeitigem Kauf eines vertragsgebundenen Endgerätes, eine bestimmte IMEI teilweise im CRM (Customer Relationship Management) - System eines Betreibers vorhanden sein. Dennoch fällt die IMEI nicht unter die abschließende Definition der Stammdaten in § 92 Abs. 3 Z 3, da es sich weder um eine Teilnehmernummer noch um sonstige Kontaktinformationen für die Nachricht handelt, sondern vielmehr ein technisches Datum sui generis vorliegt, welches ausschließlich der Kennzeichnung des Endgerätes dient. Aus der Information im CRM-System kann der Betreiber auch nicht nachvollziehen, ob das durch die IMEI bezeichnete Gerät tatsächlich mit jener Teilnehmerkennung (MS-ISDN, Mobile Subscriber Integrated Services Digital Network Number) verwendet wird bzw. wurde, mit welcher bei Vertragsabschluss zunächst ein Zusammenhang bestand. Dieser Zusammenhang ist beispielsweise dann nicht mehr gegeben, wenn der Benutzer das Gerät mit einer anderen SIM-Karte verwendet oder die IMEI des Gerätes selbst verändert hat, was bei den meisten Endgeräten auch ohne tiefere technische Kenntnisse möglich ist.

Die IMSI (International Mobile Subscriber Identity), durch welche die SIM-Karte (Subscriber Identity Module) eindeutig identifiziert ist, stellt ihrer technischen Funktion nach jedenfalls ein Zugangsdatum im Sinne des § 92 Abs. 3 Z 4a und kein Stammdatum dar und ist als solches im Kommunikationssystem des Betreibers vorhanden. Für eine Zuordnung einer IMSI zu einem bestimmten Kommunikationsvorgang ist

daher ebenfalls eine Auswertung von Zugangsdaten, somit entsprechend der Legaldefinition des § 92 Abs. 3 Z 4a von Verkehrsdaten notwendig.

Die Formulierung „nach Maßgabe des SPG“ im letzten Satz ist insbesondere so zu verstehen, dass an die Sicherheitsbehörden nicht automatisch sämtliche im TKG aufgezählten Stammdaten beauskunftet werden, sondern nur jene, die auch im SPG aufgezählt sind.

Wie bei den bisherigen Auskünften nach § 103 Abs. 4 sind bei Auskünften nach dieser Bestimmung keine Kosten gemäß der Überwachungskostenverordnung zu ersetzen.

Zu § 90 Abs. 8

Diese Bestimmung ist zur Umsetzung der Speicherpflicht gemäß Art. 5 Abs. 1 lit. f) Z 2 der RL 2006/24/EG notwendig. Die korrespondierende Bestimmung der Richtlinie zielt darauf ab, dass die Betreiber trotz sich ständig ändernder Standorte der Funkzellen bzw. Neubenennungen der Funkzellen in der Lage sein müssen, den geografischen Standort jener Funkzelle anzugeben, die zu Beginn jeder Verbindung gemäß § 102a Abs. 3 Z 6 lit. d zu speichern ist - auch wenn diese Funkzelle zwischenzeitig nicht mehr existiert oder eine andere Bezeichnung hat. Dies bedingt eine Historisierung der Cell-ID und der entsprechenden geografischen Senderstandorte.

Die Verpflichtung zur Führung eines solchen historischen Registers ist bewusst an dieser Stelle – und nicht im Rahmen der Aufzählung der einzelnen „Vorratsdaten“ in § 102a – normiert, um auch in systematischer Hinsicht klarzustellen, dass durch die Einführung der Vorratsdatenspeicherung keine Erfassung von kommunikationsunabhängigen Bewegungsprofilen erlaubt wird.

Zu § 92 Abs. 3 Z 2a

Obwohl die RL 2006/24/EG durchwegs den Begriff „Benutzerkennung“ anwendet, wird hier bewusst der Begriff „Teilnehmerkennung“ verwendet, da der zur Auskunft verpflichtete Anbieter nur Auskunft über den Teilnehmer, nicht aber zuverlässig über den tatsächlichen Benutzer geben kann. Diese Definition belässt überdies den Anbietern den Spielraum, selbst jene Kennung abhängig von der jeweils eigenen technischen Struktur zu speichern, welche zur eindeutigen Zuordnung des Kommunikationsvorgangs notwendig ist. Eine Speicherung der Kennung setzt nicht voraus, dass die Identität des Teilnehmers dem Anbieter tatsächlich bekannt ist (z. B. anonymer Prepaid-Dienst).

Teilnehmer und Benutzer sind streng voneinander zu unterscheiden. Teilnehmer ist der Vertragspartner des Dienstanbieters, Benutzer ist der tatsächliche Urheber einer Kommunikation. Der Zweck der Speicherung der Daten liegt letztlich darin, für die Strafverfolgungsbehörden jene natürliche Person zu identifizieren, die tatsächlich am Kommunikationsvorgang beteiligt war. Der tatsächliche Benutzer ist somit immer eine natürliche Person. Wenn die Behörde Auskunft zu jener natürlichen oder juristischen Person braucht, welcher ein Anschluss zurechenbar ist, erhält sie diese über die Teilnehmerkennung.

Zu § 92 Abs. 3 Z 2b

Unter E-Mail Adresse ist jene Zeichenfolge zu verstehen, die zur Adressierung von E-Mails verwendet wird und sich aus einem lokalen Teil (local part), dem Trennzeichen „@“ sowie einem globalen Teil („domain part“) nach dem Muster Benutzer@Domain.at zusammensetzt.

Auch wenn es sich bei der E-Mail Adresse grundsätzlich im Zusammenhang mit § 102a Abs. 4 um ein Verkehrsdatum handelt, ist nicht auszuschließen, dass sie Aufschluss über den Inhalt einer Nachricht geben kann. Beispielhaft angeführt sei an dieser Stelle etwa die Adressierung „hilfe@krebskrank.at, die direkte, sehr wahrscheinlich zutreffende Rückschlüsse auf den Inhalt einer Nachricht, nämlich den Gesundheitszustand einer Person, zulässt. Insofern besteht ein qualitativer Unterschied zwischen dem Verkehrsdatum E-Mail Adresse und z. B. dem Verkehrsdatum Telefonnummer, der in die Beurteilung der Zulässigkeit einer Datenverarbeitung bei der Abwägung der Verhältnismäßigkeit einfließt.

Zu § 92 Abs. 3 Z 3

Die Änderungen in dieser Bestimmung dienen ausschließlich der begrifflichen Ausdehnung auf juristische Personen, die von der bisherigen Regelung formal nicht erfasst waren, deren Daten jedoch schon bisher im obigen Sinne gehandhabt wurden.

Zu § 92 Abs. 3 Z 6a

Soweit Daten erzeugt und verarbeitet werden, sind diese Daten bei aktiven und passiven Verbindungsherstellungen vorhanden.

Die Angabe der Standortkennung erfolgt bei der Auskunft unter Angabe von Geo-Koordinaten des Standortes der Funkzelle. Siehe dazu die Erläuterungen zu § 90 Abs. 8.

Zu § 92 Abs. 3 Z 6b

Bei Vorratsdaten handelt es sich nicht um eine neue Kategorie von Daten im Sinne der im TKG bestehenden Unterteilung in Verkehrsdaten, Standortdaten, Inhaltsdaten und Stammdaten, die primär durch ihre faktische Funktion im Rahmen der Kommunikation (Nachrichtenübermittlung, Vertragsabwicklung etc.) abgegrenzt werden. Bei der Beurteilung, ob es sich bei einem Datum um ein Vorratsdatum handelt, ist vielmehr darauf abzustellen, ob es von Anbietern der in § 102a genannten Dienste ausschließlich aufgrund der Speicherverpflichtung des § 102a gesammelt bzw. gespeichert wird. Dabei ist zu beachten, dass auch beim Anbieter zunächst zu anderen Zwecken vorhandene Daten zu Vorratsdaten werden können, wenn alle anderen zulässigen Speicherzwecke (insbesondere die Betriebsnotwendigkeit der Speicherung) wegfallen. Die Einordnung von Daten als Vorratsdaten ist also durch den Zweck determiniert, zu dem die Daten gespeichert werden (dürfen).

Vorratsdaten umfassen bestimmte Standort- und Verkehrsdaten sowie mit den jeweiligen Kommunikationsvorgängen verbundenen Stammdaten, nicht aber Inhaltsdaten. Der Begriff „Vorratsdaten" verdeutlicht explizit, dass die Speicherung der Daten für die in §102a Abs. 1 festgelegte Dauer ab ihrer Entstehung deshalb flächendeckend und vorrätig erfolgt, damit sie später den Strafverfolgungsbehörden zur Verfügung stehen, falls die Auskunft zu bestimmten Daten einer Nachrichtenübermittlung in einem bestimmten Verfahren zur Ermittlung, Feststellung und Verfolgung einer bestimmten schweren Straftat notwendig ist. Die vorrätige Datensammlung selbst erfolgt also zunächst unabhängig von einem konkreten Verdacht gegen bestimmte Personen oder wegen bestimmter strafbarer Handlungen; alle auf solcherart gespeicherten Daten sind zunächst von potentiell gleichem Nutzen und müssen daher vorrätig gehalten werden, da eine allfällige spätere Verwendung noch nicht absehbar ist, zugleich aber sichergestellt werden muss, dass für den Fall einer zulässigen strafgerichtlichen Anfrage die benötigten Daten vorhanden sind.

Entsprechend dem Grundsatz des § 96, wonach Stammdaten, Verkehrsdaten und Standortdaten nur für Zwecke der Besorgung eines Kommunikationsdienstes ermittelt oder verarbeitet werden dürfen, enthält das TKG durch die TKG-Novelle 2010 eine abschließende Aufzählung der zulässigen Zwecke, für die Daten im Zusammenhang mit Kommunikationsdiensten gespeichert und verwendet werden dürfen (siehe dazu auch die Erläuterungen zu § 99).

Zu § 92 Abs. 3 Z 8

Die vorgeschlagene Änderung berücksichtigt die technische Möglichkeit von Konferenzschaltungen und passt die Bestimmung an die Legaldefinition des § 3 Z 16 an, bringt darüber hinaus aber keine Änderung des Begriffes.

Zu § 92 Abs. 3 Z 8a

Die Definition wurde wortlautgetreu aus der RL 2006/24/EG übernommen und ist notwendig, weil sich die Speicherpflichten gem. § 102a auch auf die genannten erfolglosen Anrufversuche beziehen. Hierzu ist festzuhalten, dass das Kommunikationsgeheimnis des § 93 TKG ausdrücklich auch die dabei entstehenden Daten erfasst und der Gesetzgeber den Schutz damit ganz bewusst ausgeweitet hat, obwohl gar kein Kommunikationsvorgang im engen Sinn vorliegt, sondern nur Verkehrsdaten selbst den Inhalt der Kommunikation darstellen. So erhält beispielsweise ein Teilnehmer auf seinem Mobiltelefon die Information „Vermisste Anrufe, Datum, Uhrzeit …". Auch diese Information ist bereits eine Art der Nachrichtenübermittlung.

Zu § 92 Abs. 3 Z 10

Die Änderung beinhaltet nur die Ersetzung des Punktes durch einen Strichpunkt am Ende, weil die Aufzählung mit neuen Begriffsdefinitionen fortgesetzt wird. Zur besseren Lesbarkeit wird der Text jedoch wiedergegeben.

Zu § 92 Abs. 3 Z 11

Die Einteilung des Ablagesystems in verschiedene Unterordner (z. B. Aufteilung in Posteingang, gesendete Objekte, Entwürfe etc.) ist davon nicht umfasst.

Zu § 92 Abs. 3 Z 12

Die Definition erfasst sowohl „klassisches" E-Mail als auch Webmail, soweit dabei Übermittlungen auf Basis des „Simple Mail Transfer Protocols" (SMTP) stattfinden Die Übertragung ist im Standard RFC 821 (SMTP-Definition) und darauf aufbauenden RFCs definiert.

Zu § 92 Abs. 3 Z 13

Diese Bestimmung enthält eine Klarstellung im Sinne der Rechtssicherheit. Ein Internet-Telefondienst ist als Unterfall des technologieneutralen Begriffs des „öffentlichen Telefondienstes" iSd § 3 Z 16 zu

verstehen. Im Sinne der Richtlinien für Anbieter von Voice over IP (VoIP) Diensten der RTR ist Internet-Telefondienst als Voice over IP (VoIP) Klasse A zu verstehen. Soweit die Verbindung mit denselben Vermittlungsmöglichkeiten wie das leitungsvermittelte Telefonsystem auch paketvermittelt bereitgestellt wird, fällt auch ein solches System unter diese Definition (Stratil, Kommentar 2004 zu § 3 TKG). Der Internet-Telefondienst erfasst damit all jene Voice over IP (VoIP) Dienste, die bereits jetzt dem TKG unterliegen. Die Definition dieses Begriffes ist geboten, weil sich die Speicherpflichten nach § 102a Abs. 3 auch auf Internet-Telefondienste beziehen.

Die Zusammenfassung von Voice over IP (VoIP) mit herkömmlicher Telefonie wird auch von der ERG empfohlen (Technologieneutralität, ERG (07) 56rev2). Eine neue Definition „Telefondienst" ist zur Umsetzung der RL 2006/24/EG darüber hinaus nicht notwendig, da keine Abweichung vom Begriff „öffentlicher Telefondienst" in § 3 Z 16 TKG vorliegt (siehe die Erläuterungen zu § 3 Z 16, der die erweiterte Definition nach der UniversaldienstRL 2002/22/EG Art. 2 c mit einschließt).

Zu § 92 Abs. 3 Z 16

Öffentliche IP-Adressen sind nur solche, die aus einem Adressblock aus dem sog. Provider Aggregatable Address Space (PA-Space) einem ISP zugewiesen und von diesem an seine Kunden weitergegeben wurden. Der Begriff „Rechner" ist in diesem Zusammenhang weit zu verstehen und bezeichnet jedes Gerät, welches zur selbständigen Kommunikation über ein IP-Netzwerk auf der Ebene des Internet-Protokolls fähig ist, wie beispielsweise ein Router.

IP-Adressen, unabhängig davon, ob sie dynamisch oder statisch vergeben werden, sind erforderlich für den Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen. Aus der Sicht des technischen Kommunikationsprozesses sind IP-Adressen daher jedenfalls immer Zugangsdaten im Sinne des § 92 Abs. 3 Z 4a TKG. Zugleich kann es aber auch sein, dass IP-Adressen für die Begründung und die Abwicklung sowie die Änderung und Beendigung der Rechtsbeziehung zwischen dem Teilnehmer und dem Anbieter relevant sind. Das ist dann der Fall, wenn sog. statische IP-Adressen vertraglich einem Teilnehmer zur ausschließlichen Nutzung individuell dauerhaft zugewiesen werden. Nur in diesem Fall handelt es sich bei der IP-Adresse auch um ein Stammdatum. Ihre Verknüpfung mit anderen Stammdaten ist ohne Auswertung von Verkehrsdaten möglich.

Auch wenn die IP-Adresse – insbesondere im Hinblick auf Internet-Telefonie – ähnliche Funktionen erfüllen kann, handelt es sich dabei nicht um eine mit einer Telefonnummer gleichzusetzende Teilnehmernummer. Insbesondere ist nicht verifizierbar, ob ein Datenpaket tatsächlich von der vorgeblichen IP-Adresse stammt. So kann beispielsweise beim Versenden von Datenpaketen vorgetäuscht werden, mit der IP-Adresse eines anderen Kunden den Datenverkehr zu verursachen. Die Vergleichbarkeit mit Telefonnummern ist also wirklich nur in jenen Ausnahmefällen gegeben, in denen eine bestimmte IP-Adresse unmittelbar im Vertrag einem bestimmten Teilnehmer zugewiesen wird. Dann ist eine Beauskunftung allein aufgrund einer Einsichtnahme in die Stammdaten möglich, ohne hierzu Zugangsdaten-Logfiles auswerten zu müssen. Damit sind IP-Adressen nicht automatisch zugleich Stammdaten, auch wenn sie rein technisch statische IP-Adressen sind, also nicht ständig neu (dynamisch) zugewiesen werden. Kriterium ist lediglich, ob sie ausdrücklich Bestandteil des Vertrages geworden sind. Vertragsbestandteil muss dabei eine bereits konkrete IP-Adresse sein. Vertragskonstruktionen, die einem Kunden zwar die technische Zuordnung einer statischen IP-Adresse zusichern, dabei aber nicht festlegen, welche IP-Adresse dabei zugeordnet wird, begründen keine Stammdateneigenschaft einer sodann vergebenen IP-Adresse. Der Unterschied liegt vor allem darin begründet, dass solche Konstruktionen lediglich darauf abzielen, das Protokoll der technischen Zuordnung zu fixieren, aber keinen ausschließlichen Nutzungsanspruch für die Vertragsdauer an einer bestimmten IP-Adresse begründen und diese damit nicht für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Teilnehmer und dem Anbieter notwendig ist. Der Anbieter darf also bei vorliegen sachlicher Gründe - etwa einer Reorganisation seiner Adressbereiche - und unter rechtzeitiger Ankündigung auch während der laufenden Vertragsdauer durchaus eine andere IP-Adresse zuweisen, solange die Zuweisung technisch weiterhin statisch bleibt. In den Fällen der vertraglichen Zuweisung einer bestimmten IP-Adresse ist eine solche Vorgehensweise zivilrechtlich nur mit Zustimmung des Kunden zulässig.

Zu § 93 Abs. 3

Diese Änderung stellt ausdrücklich klar, dass die Kommunikationsüberwachung nach der StPO eine zulässige Durchbrechung des Kommunikationsgeheimnisses darstellt. Der Begriff „Fangschaltung" bleibt neben der ausdrücklichen Erwähnung der „Überwachung von Nachrichten" enthalten, weil er in §106 enthalten ist und für die Anbieter klarstellt, dass jeweils nach Implementierung der Fangschaltung eine Auswertung von Verkehrsdaten zulässig ist, um die Identität des Anrufers gegen dessen Willen

festzustellen. Für die Fälle einer nach der StPO zulässigerweise eingerichteten Fangschaltung bleibt die damit verbundene Aufzeichnung von Verkehrsdaten eine zulässige Durchbrechung des Kommunikationsgeheimnisses. Ebenso bleibt eine die Überwachung von Nachrichten begleitende Feststellung von Standortdaten weiterhin zulässig.

Zu § 94 Abs. 1

Diese Änderung ist zunächst als Anpassung an die aktuellen Bestimmungen der neuen StPO erforderlich, da in der alten Fassung der StPO unter „Überwachung einer Telekommunikation" sowohl die Inhaltsüberwachung als auch die „Auskunft über Daten einer Nachrichtenübermittlung", somit also die Verkehrs- und Standortdatenauskunft, subsumiert wurde. Durch die ausdrückliche Nennung der „Auskunft über Vorratsdaten" wird klargestellt, dass die Bereitstellungspflicht sowie der Kostenersatz auch für jene Einrichtungen gilt, die bisher nicht gespeicherte Daten, die nunmehr aufgrund der Umsetzung der RL 2006/24/EG speicherpflichtig sind, betreffen, auch wenn nach den derzeit geltenden Bestimmungen der StPO (idF BGBl I 109/2007) – mangels ausdrücklichen Bezuges auf § 102a Abs. 1 – ein Zugriff auf diese Daten nicht zulässig ist. In diesem Zusammenhang wird auf die Erläuterungen zu § 92 Abs. 3 Z 6b verwiesen, wonach Vorratsdaten keine eigene Kategorie von Daten darstellen, sondern lediglich auf die Rechtsgrundlage der Speicherung abzustellen ist.

Der zweite Satz entspricht den Vorgaben des VfGH-Erkenntnisses vom 27.02.2003 zu GZ 37/02 ua (VfSlg 16.808) dar. Der VfGH hat mit diesem Erkenntnis die Überwälzung aller Kosten für die Bereitstellung von Überwachungseinrichtungen durch den Ausschluss eines Kostenersatzes an die Telekommunikationsbetreiber für verfassungswidrig erklärt.

Im Lichte dieses Erkenntnisses des VfGH ist daher die Festlegung eines angemessenen Kostenersatzes verfassungsrechtlich jedenfalls geboten. Anlässlich der Umsetzung der RL 2006/24/EG zur Vorratsdatenspeicherung wird daher eine Anpassung der (Investitionskosten-) Verordnung zu erwägen sein, da sich die derzeit gültige Investitionskostenverordnung (BGBl. II Nr. 320/2008) in § 1 Abs. 2 ausdrücklich nur auf jene Kosten bezieht, die aus der Umsetzung der Überwachungsverordnung (BGBl. II Nr. 418/2001) entstanden sind. Die tatsächliche Höhe der Kosten wird abhängig von den bestehenden Systemen der Anbieter im Einzelfall von diesen nachzuweisen sein.

Zu § 94 Abs. 2

Die Änderung beinhaltet zunächst, dass für die Verordnung eines angemessenen Kostenersatzes kein Einvernehmen mit dem Bundesministerium für Inneres und dem Bundesminister für Landesverteidigung erforderlich ist, zumal deren Ressorts durch die entstehenden Kosten gar nicht belastet werden.

Die Ergänzung der Bestimmung um die „Auskunft über Vorratsdaten" stellt klar, dass auch für derartige Auskünfte eine Mitwirkungspflicht besteht sowie Kostenersatz zu leisten ist, auch wenn ein Zugriff auf Vorratsdaten nach derzeit geltender Rechtslage (StPO 1975 idF BGBl I 109/2007) mangels ausdrücklichen Verweises auf § 102a Abs. 1 nicht zulässig ist. Da es sich bei Vorratsdaten grundsätzlich um Verkehrs-, Standort- und Stammdaten handelt (siehe dazu die Erläuterungen zu § 92 Abs. 3 Z 6b), gilt wie bisher die bereits aufgrund dieser Vorschrift erlassene Überwachungskostenverordnung, unabhängig davon, ob die übermittelten Datensätze Vorratsdaten beinhalten oder nicht.

Zu § 94 Abs. 3

Die Änderung in diesem Absatz beschränkt sich auf die notwendige Anpassung an die differenzierte Terminologie der neuen StPO und ersetzt daher „Überwachung einer Telekommunikation" durch „Überwachung von Nachrichten". Die Regelung zur „Auskunft über Daten einer Nachrichtenübermittlung" einschließlich Vorratsdaten erfolgt differenziert im neuen Abs. 4.

Zu § 94 Abs. 4

Das Dateiformat CSV beschreibt den Aufbau einer Textdatei zur Speicherung oder zum Austausch einfach strukturierter Daten. Die Dateiendung CSV ist eine Abkürzung für „Comma-Separated Values". Das Dateiformat CSV wird im RFC 4180 grundlegend beschrieben. Die Normierung dieses Dateiformats bei gleichzeitig eindeutiger Definition der Datenfelder in der technischen Richtlinie hat den großen Vorteil völliger Technikneutralität, das heißt, dass weder die Anbieter noch die staatlichen Stellen, an welche die Daten übermittelt werden, an besondere technische Voraussetzungen gebunden sind. CSV-Dateien können von allen gängigen Datenbanksystemen verwendet werden. Diese Lösung stellt daher überdies die geringste Kostenbelastung dar.

Eine verschlüsselte Übertragung per E-Mail wird bei grundsätzlich technikneutraler Formulierung normiert. Aus heutiger Sicht bietet sich hier als konkreter Standard am besten eine 'Secure / Multipurpose Internet Mail Extensions (S/MIME)' - Verschlüsselung an. S/MIME ist ein Standard für die Verschlüsselung und Signatur von MIME-gekapselten E-Mails durch ein asymmetrisches Kryptosystem.

S/MIME definiert zwei Content-Types für MIME: das Multipart/Signed-Format zur Signierung einer E-Mail und das Multipart/Encrypted-Format zu deren Verschlüsselung. S/MIME wird von den meisten modernen Mailclients unterstützt und erfordert X.509-basierte Zertifikate für den Betrieb. Diese Lösung stellt nicht nur eine hinreichend sichere, sondern auch die kostengünstigste und daher naheliegendste Variante dar. Auch die näheren technischen Details zur Verschlüsselung der Daten sind in einer technischen Richtlinie zu regeln.

Ausdrücklich gesetzlich gefordert ist eine Verschlüsselung bei der Übermittlung. Allenfalls kommt in Frage, die Verschlüsselung zusätzlich bereits in den Datenbanken der Anbieter unter Verwendung einer asymmetrischen Verschlüsselungstechnologie umzusetzen. Dies hätte den Vorteil eines deutlich höheren faktischen Schutzniveaus der Vorratsdaten schon ab dem Zeitpunkt ihrer Speicherung als Vorratsdaten, zu dem eine solche Verschlüsselung stattfinden könnte.

Der Spielraum für eine nach dieser Bestimmung zu erlassenden Verordnung ist eng determiniert. Die technische Richtlinie soll lediglich für alle einheitlich definieren, welche der zu beauskunftenden Werte an welcher Stelle innerhalb der CSV-Datei zu stehen haben und welche Zeichensätze dabei zu verwenden sind. Klar festgelegt ist auch, dass eine verschlüsselte Übermittlung per E-Mail zu erfolgen hat. Hier sind die näheren technischen Details zur Public Key Infrastructure zu definieren, allenfalls auch, ob eine Verschlüsselung erst bei der Übermittlung oder schon zu einem früheren Zeitpunkt im Sinne einer oben skizzierten Variante erfolgt. Kein Platz besteht für Vorschriften, bestimmte Programme zu verwenden oder gar eine komplexe Schnittstelle wie beispielsweise den ETSI-Standard zur Vorratsdatenspeicherung vollständig zu normieren.

Die Verwendung des Begriffs „Übermittlung“ von Auskünften legt fest, dass solche Auskünfte in jedem Fall durch aktives Handeln des Anbieters an die Behörden weitergegeben werden und kein System geschaffen wird, mit dem Zugriffe auf die Daten ohne Mitwirkung des Anbieters im Einzelfall ermöglicht werden. Die Konzeptionierung der Datenauskünfte als „push“ und nicht als „pull“ System ist dabei verfassungsrechtlich geboten. Da nämlich das auf die gegenständlichen personenbezogenen Daten anwendbare Grundrecht auf Datenschutz in § 1 Abs. 5 DSG 2000 eine sog. unmittelbare Drittwirkung normiert, steht die rechtliche Verantwortung, welche die Anbieter gegenüber ihren Kunden haben, dem einfachen Gesetzgeber nicht beliebig zur Disposition. Ein System, durch welches die Anbieter als datenschutzrechtliche Auftraggeber überhaupt keine Kontrolle mehr über die Verwendung der Daten ihrer Kunden haben, steht dieser im Verfassungsrang verankerten Verantwortung entgegen. Aus diesem Grund kommt auch eine einfachgesetzliche Normierung einer zentralen Speicherung sämtlicher Vorratsdaten aller Anbieter auf einem staatlichen Datenbanksystem nicht in Frage. Eine solche zentrale Speicherung aller Vorratsdaten würde zugleich bedeuten, dass sämtliche Daten aller Kunden verdachtsunabhängig stets zur Verfügung stünden und nicht nur für den Fall eines tatsächlichen Verdachts im Zusammenhang mit der Verfolgung einer schweren Straftat im Einzelfall. Daten durch sogenanntes „Data-Mining“[13] mit anderen Informationen automatisiert zu verknüpfen ist nach dem strengen datenschutzrechtlichen Zweckbindungsgrundsatz (Art. 6 Abs. 1 lit. b DatenschutzRL 95/46/EG bzw. § 6 Abs. 1 Z 2 DSG 2000) unzulässig. Eine dezentrale Speicherung der Vorratsdaten bei den Anbietern bietet insofern einen effektiven Schutz vor einer extensiven Verwendung der vorrätig gesammelten Datenmengen. Dass die Daten über verschiedene Anbieter „verstreut“ sind und nur mit deren Mitwirkung zur Verfügung stehen, bedeutet eine nicht unwesentliche Hemmschwelle.

Zu § 97 Abs. 1

Die Ergänzungen nehmen auf die Änderungen in den §§ 90 und 96 Bedacht.

Zu § 98 Abs. 1

Die Änderung beschränkt sich auf die Neubezeichnung des bestehenden § 98 als § 98 Abs. 1.

Zu § 98 Abs. 2

Die aktuelle Standortfeststellung des Endgeräts erfolgt regelmäßig durch eine sog. „stille SMS“ und daher grundsätzlich ohne Verarbeitung von gespeicherten Verkehrsdaten. Nur wenn eine Feststellung des aktuellen Standorts nicht möglich ist, etwa weil die Endeinrichtung zum Zeitpunkt der versuchten Standortfeststellung nicht (mehr) in Betrieb ist, ist eine Auswertung des letzten bekannten Standorts der Endeinrichtung notwendig. Allein aus diesem Grund ist der Rückgriff auf die Standortkennung (Cell-ID) zum letzten Kommunikationsvorgang dieser Endeinrichtung zulässig, dann aber auch notwendig und verhältnismäßig. Weil Standortdaten für Betriebszwecke des Anbieters keine Funktion erfüllen und daher ab ihrer Speicherung nur als Vorratsdaten gemäß § 102a Abs. 3 Z 6 lit. d vorhanden sind, wird hier wie

13 Dazu ausführlich Nathan Eagle, Alex Pentland, David Lazer, Inferring Social Network Structure using Mobile Phone Data, Proceedings of the National Academy of Sciences 2007.

auch in § 99 Abs. 5 Z 2 eine auf den letzten Kommunikationsvorgang eingeschränkte und damit eng gefasste Ausnahme von der grundsätzlich strengen Zweckbindung des § 102a Abs. 1 normiert. Aus Sicht der Praxis wird in diesen Fällen regelmäßig nicht zwingend der Notruf selbst der letzte Kommunikationsvorgang sein.

Schließlich wird wie auch in § 99 Abs. 5 Z 2 normiert, dass der Anbieter den Teilnehmer über die Erteilung einer Auskunft an Notrufträger zu informieren hat. Es bleibt dem Anbieter überlassen, ob er den Teilnehmer per SMS oder auf andere Weise informiert, etwa gemeinsam mit der Rechnungslegung. Vorgeschrieben wird nur, dass die Information spätestens mit Ablauf der Rechnungsperiode zu erfolgen hat, innerhalb derer die Auskunft über Standortdaten erteilt wurde.

Die in Abs. 2 normierte Zulässigkeit zur Verarbeitung von Verkehrsdaten erfordert eine verfassungsrechtliche Verankerung, weil dabei in das durch Art. 10a StGG verankerte Fernmeldegeheimnis eingegriffen wird und dieses für Eingriffe einen zwingenden Richtervorbehalt vorsieht. Zur bisher nicht unstrittigen Frage, ob das Fernmeldegeheimnis auch auf Verkehrsdaten anwendbar ist, siehe die Erläuterungen zu § 99 Abs. 5 Z 2.

Zu § 99 Abs. 1 und 2

Durch Ersetzung des Wortes „gesetzlich“ durch die Wortfolge „in diesem Gesetz“ wird klargestellt, dass die rechtliche Zulässigkeit und damit auch die Zwecke der Speicherung von Verkehrsdaten im TKG abschließend geregelt werden. Insbesondere soll dadurch die Rechtssicherheit geschaffen werden, dass aus materiellen Auskunftsansprüchen in anderen Materiengesetzen keine implizite Berechtigung oder gar Verpflichtung zur Speicherung von Verkehrsdaten abgeleitet werden kann. Die Bestimmung folgt damit den klaren Vorgaben des Beschlusses des VfGH vom 1.7.2009, GZ G 147,148/08-14 sowie auch der Entscheidung des OGH vom 14.7.2009, GZ 4 Ob 41/09x.

Diese Entscheidungen heben zentral den datenschutzrechtlichen Grundsatz hervor, dass die Speicherung von personenbezogenen Daten einer ausdrücklichen und klaren gesetzlichen Bestimmung bedarf, die auch eindeutige Zwecke erkennen lässt. Dass eine bestehende materielle Auskunftsverpflichtung eine Berechtigung bzw. Verpflichtung zur Speicherung bloß impliziert, genügt diesem Bestimmtheitsgebot nicht. Deshalb werden nunmehr im TKG die gesetzlichen Grundlagen für die Speicherung von Daten geschaffen, mit denen Bestimmungen zur Auskunft oder sonstigen Verwendung korrespondieren sollen.

Zu § 99 Abs. 5 Z 1

Diese Bestimmung regelt die Handhabung von Auskunftsbegehren zu Verkehrsdaten, die zwar keine schweren Straftaten betreffen, aber im Hinblick auf die derzeitigen Auskunftsgrundlagen nach § 134 ff StPO insofern gerechtfertigt sein können, als sie sich auf Informationen beziehen, die nicht bloß aufgrund der Vorratsspeicherung vorliegen. Für diesen „niederschwelligeren“ Bereich ist ein Zugriff auf Vorratsdaten jedenfalls ausgeschlossen. Nur wenn Daten im „live-System“ (z. B. bei den meisten Anbietern IP-Adressen bis zu 96 Stunden), zu Verrechnungs- oder sonstigen betriebsnotwendigen Zwecken (z. B. Telefonie-Rufdaten, regelmäßig auch bei flat-Tarifen) vorhanden sind, dürfen sie nach dieser Bestimmung beauskunftet werden. Sobald sie nur noch als Vorratsdaten vorhanden sind, ist eine Auskunft nur noch in Bezug auf „schwere Straftaten“ zulässig.

Der tatsächliche Nutzen dieser Bestimmung hängt von korrespondierenden Bestimmungen in der StPO ab, welche für die „Auskunft über Daten einer Nachrichtenübermittlung“ eine Differenzierung je nach Schwere der Straftat beinhalten.

Zu § 99 Abs. 5 Z 2

Diese Bestimmung beinhaltet das ausnahmsweise Abgehen vom Grundsatz, dass Verkehrsdaten (egal, ob es sich dabei um Vorratsdaten oder solche Daten handelt, die auch für Betriebszwecke gespeichert sein dürfen) aufgrund Art. 10a StGG nur bei Vorliegen einer richterlichen Bewilligung beauskunftet werden dürfen.

Da auch Verkehrsdaten vom Schutz des Fernmeldegeheimnisses gemäß Art. 10a StGG erfasst sind[14], darf eine Auskunft über Verkehrsdaten ausschließlich aufgrund einer richterlichen Genehmigung erfolgen.

---

14 OGH 26.7.2005, 11 Os 57/05Z = JBl 2006, 130; OGH 6.12.1995, 13 Os 161/95 = JBl 1997, 260; OGH 17.6.1998, 13 Os 68/98 = EvBl 1998/191; zuletzt VwGH 27.5.2009, GZ 2007/05/0280; Reindl, Telefonüberwachung zweimal neu? , ÖJZ 2002, 69; dies, Die nachträgliche Offenlegung der Vermittlungsdaten im Fernmeldeverkehr ("Rufdatenrückerfassung"), JBl 1999, 791; dies, WK-StPO Vor §§ 149a - c RZ, 9 (Stand: Jänner 2005); Einzinger et al., Wer ist 217.204.27.214?, MR 2005, 113; Funk et al., Zur Registrierung von Ferngesprächsdaten durch den Dienstgeber, RdA 1984, 285; Schmölzer, Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr, JBl 1997, 211 (214);

Dieser (gegenüber dem in Art. 10 StGG normierten Briefgeheimnis) erweiterte Umfang des Art. 10a StGG wurde in der Vergangenheit mehrfach bezweifelt, ergibt sich jedoch – trotz der Ähnlichkeit zwischen Brief- und Fernmeldegeheimnis und der Vorbildwirkung des Art. 10 StGG für den erst 1975 eingeführten Art. 10a StGG – klar aus den zwischen den beiden Grundrechten bestehenden Unterschieden.

Dass der Gesetzgeber für den Fernmeldeverkehr gegenüber dem Briefgeheimnis höheren Schutz normiert hat, indem er als Eingriffsvoraussetzung in allen Fällen zwingend einen richterlichen Befehl verlangt, zeigt bereits, dass die Überlegungen zum Schutzbereich des Art. 10 StGG nicht undifferenziert auf Art. 10a StGG übertragen werden können. Zudem sind die jeweils betroffenen Daten unterschiedlich schutzbedürftig.

Im Kern schützt das Fernmeldegeheimnis – in Anlehnung an Art. 10 StGG – den Inhalt der übertragenen Kommunikation. Anders als das Briefgeheimnis geht der Schutz des Art. 10a StGG jedoch weiter und umfasst auch die sogenannten „äußeren Kommunikationsdaten", also Verkehrsdaten zu Kommunikationsvorgängen.

Dieses Verständnis des Schutzbereiches war in der Vergangenheit nicht unumstritten, ist jedoch unter Berücksichtigung des Schutzzwecks des Grundrechts die einzige im Ergebnis zufriedenstellende Interpretation: Verkehrsdaten erlauben regelmäßig Rückschlüsse auf den Inhalt von Nachrichten (z. B. hilfe@anonyme-alkoholiker.at als Adressat einer E-Mail, Anruf bei einem psychosozialen Beratungsdienst) und können – bis zu einem gewissen Grad, insbesondere vom Durchschnittsanwender – nicht „vermieden" oder verschleiert werden. Im Gegensatz dazu besteht beim „klassischen" Brief immer die Möglichkeit, Nachrichten nach außen hin anonym zu übermitteln, indem z. B. auf dem Briefumschlag kein Absender angegeben wird. Aus diesem Grund war eine völlige Gleichstellung der Verkehrsdaten mit den „äußeren Kommunikationsdaten" eines Briefes schon zum Zeitpunkt der Entstehung des Art. 10a nicht möglich: Das Fernmeldegeheimnis kann für Nachrichteninhalte nur dann effektiven Schutz bieten, wenn auch die äußeren Gesprächs- oder anderen Kommunikationsdaten in den Schutzbereich einbezogen werden.

Zudem unterscheidet sich die im Rahmen des Fernmeldegeheimnisses geschützte Kommunikation auch quantitativ vom klassischen Briefverkehr: Das Kommunikationsvolumen ist mit der Entwicklung neuer Technologien – insbesondere E-Mail und Mobiltelefonie – rasant gestiegen, wobei die Anzahl der dabei entstehenden Verkehrsdaten linear mit wächst. Aus einer entsprechend großen Ansammlung von Verkehrsdaten können daher nicht nur einzelne Kommunikationspartner abgeleitet werden, sondern gleichsam Profile der Betroffenen erstellt werden, aus denen wiederum auf Kommunikationsinhalte geschlossen werden kann: So weist zum Bespiel regelmäßiger Kontakt zu Fachärzten für Onkologie auf eine Krebserkrankung hin, häufiger Kontakt zu bestimmten Uhrzeiten auf Freundschaften bzw. Arbeitskollegen usw.

Würden Verkehrsdaten aus dem Schutzbereich des Art. 10a StGG ausgeklammert, so könnte durch die Ansammlung entsprechend großer Menge solcher Daten der Schutzzweck des Fernmeldegeheimnisses faktisch ausgehöhlt werden. Insbesondere im Zusammenhang mit der Umsetzung der Vorratsdatenspeicherung wird diese Gefahr besonders aktuell, da hier gerade auf die Verfügbarkeit von Kommunikationsmustern über einen längeren Zeitraum abgestellt wird.

Zuletzt ist im Zusammenhang mit der Auslegung von Grundrechten der Grundsatz „in dubio pro libertate" relevant, der vom VwGH im Zusammenhang mit dem Grundrecht auf Glaubens- und Gewissensfreiheit angewandt wurde[15]. Aus diesem Grund ist bei der Abgrenzung des Schutzbereichs des Fernmeldegeheimnisses grundsätzlich einer grundrechtsfreundlichen Interpretation der Vorzug zu geben, sofern nicht sachliche Gründe für eine engere Auslegung sprechen. Der bloße Verweis auf die Parallelen zu Art. 10 StGG vermögen einen solchen Grund jedoch – aufgrund der teilweise unterschiedlichen Ausgestaltung der beiden Grundrechte – ebenso wenig zu belegen wie der Verweis auf die generell niedrigere Schutzwürdigkeit von Verkehrsdaten.

Aus diesen Gründen unterliegen auch Verkehrsdaten dem Schutzbereich des Fernmeldegeheimnisses, somit auch die gemäß der RL 2006/24/EG zu speichernden Verkehrsdaten. Eine Verwendung dieser Daten, insbesondere die Übermittlung an die Strafverfolgungsbehörden, ist nach Maßgabe des Art. 10a StGG nur aufgrund eines richterlichen Befehls zulässig. Die Normierung von Ausnahmebestimmungen zu diesem strengen Richtervorbehalt, im Besonderen auch in der gegenständlichen Bestimmung, muss daher im Verfassungsrang erfolgen.

---

15 VwGH 22.5.1964, 1111/63 im Zusammenhang mit Art. 14 StGG.

Darüber hinaus besteht auch dann ein Eingriff in das verfassungsrechtlich geschützte Fernmeldegeheimnis (Art. 10a StGG), wenn Gegenstand der Auskunft zwar bloß Stammdaten sind, diese jedoch durch eine Verarbeitung von Verkehrsdaten auf Seiten des Anbieters ermittelt werden. Dies betrifft in der Praxis insbesondere die Auskunft zu Name und Anschrift des Teilnehmers zu einer dynamischen IP-Adresse. Da eine derartige Verarbeitung von Verkehrsdaten – wird sie von staatlichen Behörden selbst durchgeführt – einen unzweifelhaften Eingriff in das Fernmeldegeheimnis nach Art. 10a StGG darstellt, ist der gleiche Maßstab anzuwenden, wenn die Verarbeitung durch einen privaten Rechtsträger im Auftrag des Staates und ausschließlich zu staatlichen Zwecken erfolgt. Durch die Auslagerung der staatlichen Speicherungs- und damit auch der Auskunftspflicht auf Private darf keine Umgehung von grundrechtlichen Schutzzwecken erfolgen. Die Verarbeitung der Verkehrsdaten ist daher den staatlichen Behörden zuzurechnen, welche die Grundrechte zu wahren haben, und unterlegt ebenfalls dem strengen Richtervorbehalt des Art. 10a StGG.

Der erste europäische Entwurf zur Vorratsdatenspeicherung sah neben der Verwendung zu repressiven Zwecken auch die Verwendung für präventive Zwecke vor. Der präventive Bereich, in Österreich also Datenauskünfte nach dem SPG, wurde für die geltende Fassung der RL 2006/24/EG gestrichen, nachdem das EU-Parlament massive Bedenken geäußert hatte, dass in diesem Bereich die Gefahren von Missbrauch erheblich größer seien als im Zuständigkeitsbereich der Gerichte. Durch die hier vorgeschlagene Regelung erhält die Sicherheitspolizei im Anwendungsbereich des SPG Zugriff auf die kurz oft als „Billingdaten“ bezeichneten, also betriebsnotwendigen Daten und damit auf all jene Daten, die schon bisher zulässigerweise gespeichert wurden. Sobald die Anbieter diese Daten selbst nicht mehr benötigen, sind sie nur noch als Vorratsdaten vorhanden und dürfen dann für keine anderen Zwecke als nach § 102a verwendet werden, also auch nicht mehr für eigene Zwecke. Für die Sicherheitspolizei bleibt der Zugriff auf alle Daten, die schon bisher zulässigerweise bei den Anbietern vorhanden waren. Damit korrespondiert die Regelung des § 102c Abs. 1, wonach die Speicherung der Vorratsdaten so zu erfolgen hat, dass eine Unterscheidung von nach Maßgabe der §§ 96, 97, 99, 101 und 102 gespeicherten Daten möglich ist.

In jenen Fällen, in denen eine Verarbeitung von Verkehrsdaten zur Auskunft über Stammdaten zum Zweck der Abwehr einer konkreten Gefahr für das Leben oder die Gesundheit eines Menschen notwendig ist, handelt es sich regelmäßig um Fälle der ersten allgemeinen Hilfeleistungspflicht oder der akuten Verhinderung von schweren Straftaten. In solchen Zusammenhängen werden üblicherweise ohnehin Daten aus den „live-Systemen“ der Anbieter benötigt, um auf eine gegenwärtige Gefahr reagieren zu können. Auskünfte über ältere Daten fallen in den Anwendungsbereich der Kriminalpolizei und haben daher nach den Regeln der StPO zu erfolgen.

Einen Sonderfall stellt die Auskunft über Standortdaten dar. Nach der aktuellen Bestimmung des § 53 Abs. 3b SPG dürfen die Sicherheitsbehörden nur die Standortdaten der gefährdeten Person selbst, nicht aber etwa jene des Verdächtigen, von dem die Gefahr möglicherweise ausgeht (z. B. eines mutmaßlichen Entführers) anfordern. Paradebeispiel ist – abgesehen vom Entführungsfall – der verunglückte Tourengeher. Die aktuelle Standortfeststellung des Endgeräts erfolgt regelmäßig – wie bereits zu § 98 Abs. 2 ausgeführt - durch eine sog. „stille SMS“ und daher grundsätzlich ohne Verarbeitung von gespeicherten Verkehrsdaten. Nur wenn eine Feststellung des aktuellen Standorts nicht möglich ist, etwa weil die Endeinrichtung zum Zeitpunkt der versuchten Standortfeststellung nicht (mehr) in Betrieb ist, ist eine Auswertung des letzten bekannten Standorts der Endeinrichtung notwendig. Allein aus diesem Grund ist der Rückgriff auf die Standortkennung (Cell-ID) zum letzten Kommunikationsvorgang dieser Endeinrichtung zulässig, dann aber auch notwendig und verhältnismäßig. Weil Standortdaten für Betriebszwecke des Anbieters keine Funktion erfüllen und daher ab ihrer Speicherung nur als Vorratsdaten gemäß § 102a Abs. 3 Z 6 lit. d vorhanden sind, wird hier wie auch in § 98 eine auf den letzten Kommunikationsvorgang eingeschränkte und damit eng gefasste Ausnahme von der grundsätzlich strengen Zweckbindung des § 102a Abs. 1 normiert. Betreffend Standortdaten ist diese Bestimmung praktisch komplementär zur Auskunft an Notrufträger zu sehen, nämlich für jene Fälle, in denen gerade kein Notruf abgesetzt wurde (aber möglicherweise eine Verständigung durch Angehörige o.Ä. stattgefunden hat).

Eine Information des von der Auskunft betroffenen Teilnehmers ist in diesen Fällen nach § 24 DSG 2000 deshalb nicht geboten, weil jene Bestimmung eine Pflicht zur Information „aus Anlass der Ermittlung von Daten“ vorsieht. Der durch die Standortfeststellung zugelassene Eingriff in das Grundrecht auf Datenschutz liegt aber in diesem Fall nicht in der Ermittlung sondern in der Übermittlung von Daten. Da nun eben die Übermittlung von Daten keine Informationspflicht auslöst, entsteht die Situation, dass der Betroffene von niemandem über die Verwendung seiner Daten informiert werden würde. Damit wäre aber keine wirksame Beschwerdemöglichkeit im Falle eines ungerechtfertigten Eingriffs in das

Grundrecht auf Datenschutz gegeben, da der Betroffene von vornherein keine Möglichkeit zur Kenntnisnahme hat.

Diese Problematik wird beseitigt, indem die Informationspflicht des Anbieters geregelt wird. Festzuhalten ist, dass bei der Lokalisierung der gefährdeten Person selbst keine Konstellation vorstellbar ist, in der die Information den Zweck der Datenanwendung vereiteln würde. Die ausdrückliche Anordnung der Informationspflicht soll für die Anbieter die nach der bisherigen Praxis bestehende Rechtsunsicherheit beseitigen, ob eine allfällige Information den Zweck des sicherheitspolizeilichen Vorgehens vereiteln könnte. Es bleibt dem Anbieter überlassen, ob er den Teilnehmer per SMS oder auf andere Weise informiert, etwa gemeinsam mit der Rechnungslegung. Vorgeschrieben wird nur, dass die Information spätestens mit Ablauf der Rechnungsperiode zu erfolgen hat, innerhalb derer die Auskunft über Standortdaten erteilt wurde.

Schließlich muss auch ein Auskunftsanspruch nach dieser Bestimmung auf einer klaren gesetzlichen Grundlage beruhen, welche die näheren Voraussetzungen und das Verfahren hierzu regelt.

Zu § 102 Abs. 3

Neben der systematischen Klarstellung im neuen § 90 Abs. 8 wird hier das ausdrückliche Verbot normiert, kommunikationsunabhängige Bewegungsprofile zu ermitteln und zu speichern. Die Regelung ist insbesondere zur Klärung notwendig, dass auch die Umsetzung der RL 2006/24/EG die Erfassung solcher Standortdaten nicht erlaubt.

Zu § 102a Abs. 1

Die Formulierung „nach Maßgabe der Abs. 2 - 4“ schließt „andere“ Anbieter als die von der RL 2006/24/EG anvisierten und in den Abs. 2 - 4 konkretisierten aus.

Obwohl die Richtlinie ausdrücklich auch Betreiber öffentlicher Kommunikationsnetze nennt, ist die Normierung der Speicherpflicht im Hinblick auf die Anbieter öffentlicher Kommunikationsdienste hinreichend. Es gibt nämlich hinsichtlich der zu speichernden Datenkategorien der Abs. 2 - 4 keine Fälle, in denen die Daten ausschließlich beim Netzbetreiber anfallen. Auch bei Wholesale-Kooperationen verfügt der Dienstanbieter über alle Daten, deren Speicherung vorgeschrieben ist. Diese Ausklammerung der Netzanbieter ist darüber hinaus auch aus ökonomischen Gründen sinnvoll, weil dadurch die Gefahr einer nach dem Erwägungsgrund 13 der RL 2006/24/EG zu vermeidenden Doppelspeicherung begrenzt wird.

Hinsichtlich der Speicherdauer für Vorratsdaten sieht die RL 2006/24/EG einen Zeitrahmen von mindestens sechs Monaten und höchstens zwei Jahren ab dem Zeitpunkt des Kommunikationsvorganges vor.

Da bereits durch die Verpflichtung zur vorrätigen Speicherung der Daten in verfassungsgesetzlich gewährleistete Rechte der speicherpflichtigen Anbieter (siehe dazu die Erläuterungen zu § 91 Abs. 1) wie auch in weiterer Folge (durch die Speicherung) in jene der Benutzer dieser Dienste eingriffen wird, ist bei der Normierung der Speicherdauer auf die Verhältnismäßigkeit der Maßnahme Bedacht zu nehmen.

In Anbetracht der Tatsache, dass es sich um eine verdachtsunabhängige Speicherung handelt und der Grundrechtseingriff für die Betroffenen daher besonders schwer wiegt, müsste ein überwiegendes öffentliches Interesse an einer längeren Speicherdauer bestehen, etwa ein belegbarer, nicht unwesentlicher zusätzlicher Nutzen einer über die sechsmonatige Untergrenze hinausgehenden Speicherdauer. Im Hinblick auf den Nutzen von Verkehrsdaten hat schon zum Zeitpunkt der Entstehung der RL 2006/24/EG eine von der wik Consult durchgeführte Studie[16] ergeben, dass sich zwischen 80 und 85% der Anfragen zu Verkehrsdaten durch Strafverfolgungsbehörden auf einen Zeitraum beziehen, der nicht länger als drei Monate zurückliegt. Eine 2005 im Auftrag des deutschen Bundeskriminalamtes durchgeführte Befragung innerhalb der Polizei zur Erhebung von Rechtsdefiziten im Bereich der Verkehrsdatenspeicherung[17] ergab zudem, dass unter Berücksichtigung der Notwendigkeit und Relevanz von Verkehrsdaten in verschiedenen Deliktsbereichen die gewünschte Speicherdauer sechs Monate beträgt.

16 Franz Büllingen, Aurélia Gillet, Christin-Isabel Gries, Annette Hillebrand, Peter Stamm, Stand und Perspektiven der Vorratsdatenspeicherung im internationalen Vergleich. Studie für die BITKOM Servicegesellschaft mbH, Bad Honnef, Februar 2005 (erhältlich unter http://www.wik.org).

17 Eva Mahnken, Mindestspeicherungsfristen für Telekommunikationsverbindungsdaten. Rechtstatsachen zum Beleg der defizitären Rechtslage, Bundeskriminalamt, Wiesbaden, November 2008 (erhältlich unter http://www.vorratsdatenspeicherung.de/images/bka_vorratsdatenspeicherung.pdf).

Auch eine Erhebung der Europäischen Kommission[18] aus 2008 in Mitgliedsstaaten, die die RL 2006/24/ERG bereits umgesetzt hatten, ergibt, dass der weitaus größte Anteil an angefragten Vorratsdaten nicht älter als drei Monate ist. Gleichzeitig konnten Statistiken zum Beleg der Notwendigkeit der in der RL 2006/24/EG normierten Speicherdauer von mindestens sechs Monaten bislang nicht vorgewiesen werden.

Ganz im Gegenteil zeigt ein aktueller, sehr umfassender Forschungsbericht des Max-Planck-Instituts für ausländisches und internationales Strafrecht[19], dass sich der überwiegende Anteil der Verkehrsdatenabfragen entweder auf einen Erhebungszeitraum von einem Tag oder von drei Monaten bezieht;[20] Dieser beginnt durchschnittlich 26 Tage vor dem Zeitpunkt der Anfrage, wobei etwa die Hälfte der Abfragen einen Zeitraum von lediglich vier Tagen oder weniger vor dem Anfragezeitraum betrifft[21].

In der bisherigen österreichischen Praxis wurden von den Betreibern von Kommunikationsdiensten betriebsnotwendige Daten weitgehend für eine Dauer von sechs Monaten gespeichert und im Falle einer zulässigen Anfrage einer Strafverfolgungsbehörde beauskunftet. Dies ist insofern zu berücksichtigen, als eine Verlängerung der Speicherdauer gegenüber der bisherigen Speicherpraxis zu entsprechend höheren Kosten auf Seiten der speicherpflichtigen Anbieter führen würde[22].

Im Hinblick auf die Intensität des Grundrechtseingriffs durch die Vorratsdatenspeicherung besteht kein überwiegendes Interesse an einer Verlängerung des bisherigen Speicherzeitraumes. Die Dauer der Speicherpflicht erfüllt mit sechs Monaten die Vorgaben der RL 2006/24/EG und ist im Hinblick auf sämtliche bisher vorliegenden Statistiken ausreichend, um die angestrebten Zwecke der Strafverfolgung zu erfüllen. Da auch die Europäische Kommission aus den Erhebungen in den Mitgliedsstaaten, die die RL 2006/24/EG bereits umgesetzt haben, bislang keine fundierten Nachweise für die Effizienz der Richtlinie vorlegen konnte und sich nach bisherigen Statistiken der weit überwiegende Anteil der polizeilichen Anfragen auf Daten bezieht, die jünger als sechs Monate sind und damit außerhalb des von der Richtlinie vorgegebenen Speicherzeitraumes liegen, wäre die Normierung einer längeren Speicherdauer im Hinblick auf den tatsächlichen Nutzen unverhältnismäßig.

Zu § 102a Abs. 2 Z 1

Eine Speicherpflicht bezüglich IP-Adressen trifft jenen öffentlichen Internet-Zugangsdienstanbieter (Access-Provider), dem die Verwaltung der jeweiligen öffentlichen IP-Adressen von der zuständigen IP-Adress-Verwaltungsinstitution (für Europa derzeit RIPE NCC) nach den Regeln der IANA (Internet Assigned Numbers Authority) zugewiesen ist. Dies gilt auch für die vertragliche und uU längerfristige Vergabe von IP-Adressen, unabhängig davon, ob diese statisch oder dynamisch vergeben werden. Auskunft wird darüber erteilt, wem die IP-Adresse überlassen wurde. Bezüglich des Internetzugangs werden mit dieser Bestimmung Art. 5 Z 2 lit. a i und ii der RL 2006/24/EG zusammengefasst.

Die Speicherverpflichtung im Sinne der Richtlinie bezieht sich ausschließlich auf zugewiesene öffentliche IP-Adressen; interne Adressen (z. B. gemäß RFC 1918) und IP-Ports (z. B. entstanden durch NAT gemäß RFC 1631, RFC 2663, RFC 3022) sind nicht umfasst. Der Zusammenhang zwischen dem zu beauskunftenden Kommunikationsvorgang und der IP-Adresse bzw. Teilnehmerkennung ergibt sich über den Zeitpunkt der Nachricht und der zeitlich korrespondierenden Vergabe der IP-Adresse.

Zu § 102a Abs. 2 Z 2

In der Regel existiert kein zur Anmeldung äquivalentes Abmeldungsverfahren. Die An- bzw. Abmeldung entspricht beim Internetzugang der Zuteilung bzw. dem Entzug einer öffentlichen IP-Adresse und gibt

---

18 Data retention statistics 2008 aggregated on the basis of statistics of CZ, DA, EE, IE, LT, MT, CY, Mai 2008 (erhältlich unter http://www.dataretention2009.eu/all-doc.jsp).

19 Hans J. Albrecht, Adina Grafe, Michael Kilchling, Rechtswirklichkeit der Auskunftserteilung über Telkommunikationsverbindungsdaten nach §§ 100g, 100h StPO. Forschungsbericht im Auftrag des Bundesministeriums der Justiz, Duncker & Humblot, Februar 2008.

20 A.a.O. S. 222 ff. "In 88 % der Beschlüsse betrug die Antragsdauer bis zu drei Monaten. Bei den übrigen 12 % handelte es sich fast ausschließlich um sowohl in die Zukunft als auch in die Vergangenheit gerichtete Verkehrsdatenabfragen. Lediglich in 5 Fällen konnte festgestellt werden, dass eine Verkehrsdatenabfrage von zukünftigen Daten beantragt wurde, die die zulässige Höchstdauer von 3 Monaten (§§ 100 h I 3 iVm 100b II 4 StPO) überschritt. Diese Abfragen waren auf 100 Tage ausgerichtet. Den 12 % der Beschlüsse, mit denen über einen längeren Zeitraum als 90 Tage Daten abgefragt wurden, lagen v.a. Betäubungsmitteldelikte (42 %), Schleusungen (30 %) und (schwere) Bandendiebstähle (22 %) zugrunde." (S. 223).

21 A.a.O. S. 114.

22 Vgl. die Ausführungen in G. Stampfel, W. Gansterer, M. Ilger, K. Stark, The EU Data Retention Directive 2006/24/EC from a Technical Perspective, Universität Wien, Wien, Oktober 2007.

damit lediglich Auskunft über die Möglichkeit einer Internetkommunikation für einen bestimmten Teilnehmer. Technisch erfolgt der Entzug einer IP-Adresse in der Regel durch die Neuzuteilung an denselben oder einen anderen Teilnehmer. Nicht notwendig ist die Protokollierung des Entzugs einer IP-Adresse, wenn dieser etwa wegen Verbindungsabbruch oder timeout verursacht ist. Da die öffentliche IP-Adresse zu jedem Zeitpunkt nur einmalig vergeben sein kann und jede Neuzuteilung gespeichert wird, bleibt jede Nachricht auch bei sog. „always on - Diensten" dem Teilnehmer zeitlich zuordenbar.

Zu § 102a Abs. 2 Z 3

Damit sind Dial-up Zugänge zum Internet erfasst, die mittels Modem auf dem Sprachtelefonie-Frequenzband über POTS, ISDN (Festnetz) oder CSD (Mobilfunknetz) hergestellt werden.

Zu § 102a Abs. 2 Z 4

Die eindeutige Kennung ist bei DSL-Anschlüssen, die an einen Festnetz-Anschluss gekoppelt sind, die Telefonnummer des Teilnehmers. Bei DSL-Providern, die lediglich den Zugang anbieten und somit keine Telefonnummern vergeben, ist als eindeutige Kennung die dem Kunden vergebene Zugangskennung (z. B. Benutzername) zu speichern. Die eindeutige Kennung beim Internet-Zugang über eine Mobilfunkverbindung ist die IMSI bzw. MS-ISDN (Rufnummer = Teilnehmernummer) Gegenstand der Speicherpflicht nach § 102a Abs. 3 Z 1 (Teilnehmernummer) bzw. Z 6 (IMSI).

Zu § 102a Abs. 3 Z 1

Unter „andere Kennung" ist im Sinne der gesetzlich geforderten Technologieneutralität (siehe auch Art. 8 Rahmen-RL 2002/21/EG) bei Internet-Telefondiensten (VoIP) z. B. die dem Teilnehmer zugeordnete IP-Adresse oder SIP-Adresse zu verstehen. Ein Internet-Telefondienst ist als Unterfall der „öffentlichen Telefondienste" iSd § 3 Z 16 TKG zu verstehen. Im Sinne dieser Bestimmung ist VoIP Klasse A iSd Richtlinien für Anbieter von VoIP Diensten der RTR zu verstehen. Siehe dazu auch die Ausführungen zu § 92 Abs. 3 Z 13. Eine zusätzliche Speicherpflicht bei Internet-Telefondiensten im Vergleich zu „herkömmlichen" Telefondiensten bezieht sich daher auf die IP-Adresse oder die SIP-Adresse.

Zu § 102a Abs. 3 Z 2 und 3

Auch für VoIP-Telefonie ist der Teilnehmer eindeutig definiert.

Zu § 102a Abs. 3 Z 4

Beginn und Dauer entsprechen dem Regelfall der heutigen Aufzeichnungspraxis.

Zu § 102a Abs. 3 Z 5

„Anrufe" schließt Sprachtelefonie, Sprachspeicherdienst, Konferenzschaltungen und Datenabrufungen ein; „Zusatzdienste" schließt Rufweiterleitung und Rufumleitung ein; „Mitteilungsdienste und Multimediadienste" schließt Kurznachrichtendienste (SMS), erweiterte Nachrichtendienste (EMS) und Multimediadienste (MMS) ein. Der Anbieter obiger Dienste und Anrufarten ist nicht notwendigerweise ident mit dem Netzbetreiber.

Zu § 102a Abs. 3 Z 6

Der Begriff „Mobilfunknetz" ist im TKG bislang nicht definiert (ebensowenig Mobilfunkdienst), er wird jedoch in § 3 Z 23 verwendet und damit offenbar vorausgesetzt, ebenso in § 23 Abs. 3 sowie in § 41 Abs. 2 Z 7 TKG. Eine ausdrückliche Definition ist daher rechtlich nicht zwingend geboten.

Zu § 102a Abs. 3 Z 6a und b

Die IMEI ist - abhängig vom Netzbetreiber - nicht notwendigerweise ein erzeugtes oder verarbeitetes Datum. Zum Teil werden diese Daten nur dann erzeugt oder verarbeitet, wenn es sich um Teilnehmer im „eigenen" Netz des Anbieters handelt; die Daten sind, sofern sie im eigenen Netz anfallen, zu speichern.

Ein Problem besteht hier in der Praxis, wenn sich die gerichtliche Anordnung pauschal auf alle weiteren Teilnehmernummern bezieht, mit denen die zunächst bestimmte Teilnehmernummer im angefragten Zeitraum kommuniziert hat. In diesem Fall können IMEI, IMSI und Standortkennung (Cell-ID) nur für jene weiteren Teilnehmer beauskunftet werden, die zum Netz des Anbieters gehören, an den die ursprüngliche Anordnung gerichtet ist. Für die Teilnehmer anderer Anbieter werden diese Daten nicht verarbeitet und daher auch nur beim jeweiligen anderen Anbieter gespeichert.

Zu § 102a Abs. 3 Z 6c

Der Wortlaut dieser Bestimmung stammt aus Art. 5 Abs. 1 lit. e Z 2 vi) der RL 2006/24/EG. Festzuhalten ist, dass die Standortkennung (Cell-ID) bei der Erstaktivierung von Prepaid Kunden kein Stammdatum ist, sondern als Verkehrsdatum gespeichert wird und damit ausschließlich als Vorratsdatum zur Verfügung steht.

Zu § 102a Abs. 3 Z 6d

Auch durch die Einführung der Vorratsdatenspeicherung wird nicht zulässig, dass den Strafverfolgungs- oder den Sicherheitsbehörden kommunikationsunabhängige Standortdaten beauskunftet werden.

Zu § 102a Abs. 4 Z 1 und 2

Dies erfordert entweder eine derzeit bei österreichischen E-Mail Dienstanbietern nicht verfügbare Funktionalität der Historisierung von E-Mail Adresszuordnungen (z. B. bei frei durch den Teilnehmer änder- oder ergänzbaren E-Mail Alias Adressen) zu Teilnehmerkennungen oder eine bei jeder Zustellung einer E-Mail in ein elektronisches Postfach erfolgende dynamische Zuordnung und Speicherung von E-Mail Adresse und Teilnehmerkennung. E-Mail Alias Adressen können in diesem Sinne nur verarbeitet werden, wenn sie im angegebenen Zeitraum auch verwendet werden (d.h. eine E-Mail wird gesendet oder empfangen). In Bezug auf E-Mail Alias Adressen (damit aus Benutzersicht „dynamische" E-Mail Adressen) liegt damit hinsichtlich der historischen Zuordnung solcher Adressen zu bestimmten Teilnehmern derzeit systembedingt bei allen österreichischen Anbietern der Fall vor, dass solche Daten weder erzeugt noch verarbeitet werden und daher gemäß § 102a Abs. 5 auch nicht gespeichert werden müssen.

Diese Daten sind außerdem nur dann zu speichern, soweit sie nach der Gestaltung des Dienstes bei Abschluss des Vertrages überhaupt erhoben werden, weil sie ansonsten weder erzeugt noch verarbeitet werden und damit nach Abs. 5 auch keiner Speicherpflicht unterliegen. Das bedeutet, dass bei so genannten Freemail Diensten, die anonyme Email Accounts anbieten, Name und Anschrift des Teilnehmers nicht verfügbar sind und auch künftig nicht erhoben werden müssen.

Zu § 102a Abs. 4 Z 3

Die E-Mail Adressdaten des Absenders und der Empfänger stammen vom „MAIL" und „RCPT" command der E-Mail iSd RFC 821. Absender ist die letztübermittelnde Kommunikationseinrichtung mit einer zugeordneten öffentlichen IP-Adresse, die nicht notwendigerweise mit der IP-Adresse des Absenders der E-Mail übereinstimmt, und, - z. B. bei Webmail - auch mit der IP-Adresse des versendenden Mailservers ident sein kann. Die Absender E-Mail Adresse ist nicht notwendigerweise einem bestimmten Teilnehmer zuordenbar, da im E-Mail Protokoll die dynamische Erzeugung einer Absender-Adresse durch den Endbenutzer ohne Mitwirkung des Betreibers möglich ist.

Zu § 102a Abs. 4 Z 4

Die Daten stammen vom „MAIL" und „RCPT" command der E-Mail iSd RFC 821. Daten vorangehender Kommunikationsübermittlungseinrichtungen werden vom Empfänger weder erzeugt noch verarbeitet und sind daher nicht verfügbar. Zwar sind unter „Kommunikationsübermittlungseinrichtungen" grundsätzlich „zugehörige Einrichtungen" im Sinne des § 3 Z 24 zu verstehen, doch sind diese Einrichtungen gerade nicht Bestandteil des Kommunikationsdienstes, den der Anbieter gemäß Abs. 4 betreibt. Vielmehr handelt es sich um einen beliebigen Netzknoten im Internet, über den die Nachrichtenübermittlung auf der Ebene des IP-Protokolls vor der Zustellung an den Posteingangsserver des Dienstanbieters zuletzt geroutet wurde. Nur dessen IP-Adresse wird vom E-Mail Anbieter selbst verarbeitet.

Zu § 102a Abs. 4 Z 5

Unter Anmeldung bei einem E-Mail Dienst ist zu verstehen: 1) das Login bei einem Webmaildienst, 2) die Benutzerauthentifizierung beim Zugriff auf das Postfach mittels IMAP (gemäß RFC 1730 und darauf aufbauenden RFCs, Quelle: http://www.rfc-editor.org/rfcxx00.html) oder POP (gemäß RFC 1939). Ein Datum der Abmeldung wird nur dann erzeugt oder verarbeitet, wenn von der Anwendung eine Abmeldemöglichkeit vorgesehen ist und diese vom Teilnehmer benutzt wurde (z. B. Logout bei Webmail). Technisch gesehen kennt das POP3 Protokoll ein „QUIT" commmand, das IMAP Protokoll ein „LOGOUT" command. In beiden Fällen hängt das Vorhandensein eines entsprechenden Abmeldedatums jedoch von einer tatsächlichen Abmeldung durch den Teilnehmer ab, die in der Regel kaum erfolgt. Die tatsächliche Verwendung des E-Mail Dienstes ist durch die üblicherweise nicht konsistent verwendete Abmeldung durch den Teilnehmer in der Regel nicht zeitlich einschränkbar.

Zu § 102a Abs. 5

Die Aufzählung der Daten „gemäß Abs. 2 bis 4" ist taxativ. Die Formulierung „der betreffenden Kommunikationsdienste" ist so zu verstehen, dass die Speicherpflicht richtlinienkonform nur bezüglich jener Daten besteht, welche vom jeweiligen Betreiber für die Erbringung seiner eigenen Dienste erzeugt oder verarbeitet werden, wodurch Doppelspeicherungen im Sinne des Erwägungsgrundes 13 der RL 2006/24/EG vermieden werden.

Da Art. 2 Abs. 1 der RL 2006/24/EG ausdrücklich auf die Begriffsbestimmungen der RL 95/46/EG (DatenschutzRL) verweist, ist grundsätzlich der Verarbeitungsbegriff aus Art. 2 lit. b) dieser Richtlinie maßgeblich. Die Verarbeitung umfasst demzufolge jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, insbesondere die in Art. 2 lit. b) demonstrativ aufgezählten Vorgänge.

Aufgrund der unterschiedlichen Ziele der beiden Richtlinien ist bei der Auslegung des Begriffs „verarbeiten" dennoch zu differenzieren: Während die DatenschutzRL auf einen möglichst umfassenden Grundrechtsschutz abzielt (vgl. Erwägungsgründe 10 und 12) und daher der Verarbeitungsbegriff sehr weit auszulegen ist, sollen im Rahmen der Vorratsdatenspeicherung die Pflichten, die den Providern von der RL 2006/24/EG auferlegt werden, verhältnismäßig sein und nur jene Daten gespeichert werden, die im Zuge der Bereitstellung von Kommunikationsdiensten erzeugt oder verarbeitet werden (Erwägungsgrund 23 der Richtlinie).

Auch aus dem Entstehungsprozess der RL 2006/24/EG ergibt sich, dass es sich bei den auf Vorrat zu speichernden Daten ausschließlich um solche handelt, die bei den Betreibern von Kommunikationsdiensten bereits in irgendeiner Form vorhanden sind (Erläuternder Vermerk zum vorgeschlagenen Rahmenbeschluss über die Vorratsspeicherung von Kommunikationsdaten, Dok. 8958/04).

Auf diese unterschiedlichen Ziele sowie die konkreten Entstehungsgeschichten dieser beiden Richtlinien ist bei der Beurteilung, ob ein Datum auf Vorrat zu speichern ist, insbesondere in Grenzfällen Bedacht zu nehmen. „Erzeugen oder verarbeiten" im Sinne der RL 2006/24/EG bedingt, dass es auch eine technische Komponente gibt, die auf irgendeiner Ebene dieses Datum interpretiert. Der reine Durchlauf eines Datums beim Transport ist kein Erzeugen oder Verarbeiten im Sinne der RL 2006/24/EG (z. B. MPLS Netzbetreiber). Beispielhaft sei an dieser Stelle auch die IMEI angeführt, die zwar als Verkehrsdatensatz zunächst vorhanden ist, abhängig vom System des Betreibers jedoch möglicherweise gar nicht „angenommen" und weiterverarbeitet werden kann. In einem derartigen Fall besteht keine Verpflichtung zur Speicherung dieses Datums.

Keine Speicherverpflichtung nach Z 3 und 4 besteht für die Kommunikationsdaten von Spam E-Mails, sofern diese bereits vor dem Versand bzw. der Zustellung in ein elektronisches Postfach vom Anbieter des E-Mail Dienstes herausgefiltert werden, da in diesem Fall gar kein vollständiger Kommunikationsvorgang stattfindet. Wird eine Spam E-Mail dagegen in das elektronische Postfach des Empfängers zugestellt (wenn auch möglicherweise als „Spam" oder „Junk" markiert) oder dem Empfänger in irgend einer anderen Weise ermöglicht, auf die Spam E-Mail zuzugreifen (beispielsweise durch Ablage in einem für den Benutzer zugänglichen Ordner und/oder Benachrichtigung über den Eingang der Spam E-Mail), besteht die Speicherpflicht in vollem Umfang. Im Hinblick auf die Tatsache, dass der weitaus überwiegende Anteil (über 80%) der gesamten E-Mail Kommunikation Spam ist, wird so sichergestellt, dass ausschließlich für Zwecke der Strafverfolgung potentiell nützliche Daten gespeichert werden und zudem den Anbietern von E-Mail Diensten keine unzumutbaren Verpflichtungen auferlegt werden. Eine entsprechende Vorgangsweise bei der Umsetzung der RL 2006/24/EG wird zudem von der von der Europäischen Kommission mit dem Beschluss 2008/324/EG eingesetzten Expertengruppe („the platform for electronic data retention für the investigation, detection and prosecution of serious crime") ausdrücklich empfohlen.

Zu § 102a Abs. 6

Die Grenzziehung, auf welche sich die Ausnahme kleiner Anbieter bezieht, orientiert sich an der Empfehlung der EU Kommission 2003/361/EG, ABl. Nr. L 124 vom 20.5.2003 S. 36. Diese nennt vier Kriterien für die Zuordnung der Unternehmen nach ihrer Größengliederung: Anzahl der Mitarbeiter (<50), Umsatz (≤ € 10 Millionen), Bilanzsumme (≤ € 10 Millionen) und Unabhängigkeit. Idealerweise sollten alle Kriterien zugleich erfüllt sein, was aber in der statistischen Praxis kaum umsetzbar ist. Vielmehr spielt die Anzahl der Beschäftigten die vorherrschende Rolle für die Abgrenzung.

Die Wahrung des Verhältnismäßigkeitsgrundsatzes gebietet, kleine Unternehmen von der Speicherverpflichtung auszunehmen: Einerseits würden solche Unternehmen durch die notwendigen Investitionen und Erhaltungskosten unverhältnismäßig stark belastet, andererseits wären diese kleinen Unternehmen in der Praxis nur äußerst selten tatsächlich von Auskunftsersuchen betroffen. Es ist zu berücksichtigen, dass die Instandhaltung der für die Speicherung erforderlichen Datenbanksysteme unabhängig von der tatsächlichen Zahl der gespeicherten Datensätze auch für kleine Anbieter einen Aufwand bedeuten würde, der sich grundsätzlich nicht wesentlich von einer Datenbankhaltung für große Kundenzahlen unterscheidet. Der Nutzen stünde also in keinem Verhältnis zu den jedenfalls anfallenden Kosten, zumal Auskünfte über Verkehrsdaten gemäß § 99 Abs. 5 unbenommen bleiben.

Zu § 102a Abs. 7

Diese Bestimmung ist eine notwendige Ergänzung zum Telekommunikationsgeheimnis des § 93. Damit soll kein Zweifel offen bleiben, dass auch die Umsetzung der Vorratsdatenspeicherungsrichtlinie 2006/24/EG nicht dazu führt, dass Inhaltsdaten erfasst werden. Nur demonstrativ wird dabei der wichtigste Fall angeführt, nämlich die aufgerufenen Web-Seiten (so genannte URL, Uniform Resource Locator). Erfasst sind aber alle Formen von Kommunikationsinhalten, etwa die Betreffzeile einer E-Mail, Informationen zu Newsgroup-Diensten oder zu Chaträumen wie IRC-Channels.

Zu § 102a Abs. 8

Durch die einmonatige Frist für die Löschung der Vorratsdaten ab dem Ende der Speicherpflicht wird verhindert, dass die Anbieter eine tägliche Löschung der Vorratsdaten durchführen müssen. Die Löschungsverpflichtung wird an die gängige Praxis in der Branche angepasst, Daten periodisch, d.h. zu bestimmten Teilnehmern immer an einem bestimmten Tag, zu löschen, womit eine angemessen geringe Belastung der Dienstanbieter durch die Löschungsverpflichtung erreicht wird. Nach Ende der Speicherfrist dürfen die Daten jedoch nicht mehr beauskunftet werden.

Zu § 102a Abs. 9

Diese rechtliche Klarstellung ist notwendig, weil sich allein aufgrund der Kriterien des DSG 2000 nur schwer abschließend beantworten lässt, wer datenschutzrechtlicher Auftraggeber der Datenanwendung im Hinblick auf Vorratsdaten ist. Denn einerseits stehen die Daten, sobald sie allein aufgrund §102a gespeichert sind, nur mehr der Strafverfolgung für schwere Straftaten zur Verfügung - und damit auch nicht mehr zur beliebigen Verwendung durch die Anbieter selbst. Dies würde rechtfertigen, das BMJ als Auftraggeber zu sehen. Andererseits stehen die Daten auch der Justiz nur im Einzelfall bei Vorliegen der entsprechenden Voraussetzungen zur Verfügung, und auch in diesem Fall müssen sie erst vom Anbieter übermittelt werden. Letztlich sind es aber die Anbieter, die faktisch die Kontrolle über diese Daten ausüben und damit auch für ihre Sicherheit und rechtmäßige Verwendung verantwortlich sind. Weil sie dies aber allein aufgrund der gegenständlichen Norm tun (müssen), handeln sie in Vollziehung der Gesetze und sind damit Auftraggeber des öffentlichen Bereichs iSd § 5 Abs. 2 Z 2 DSG 2000.

Im Hinblick auf Daten, die noch bzw. auch für betriebliche Zwecke des Anbieters nach § 99 vorhanden sind, gelten diese entsprechend § 5 Abs. 3 DSG 2000 als Auftraggeber des privaten Bereichs.

Die entscheidende Konsequenz dieser gesetzlichen Klarstellung ist die ausschließliche Zuständigkeit der Datenschutzkommission (DSK) für den Rechtsschutz nach dem DSG 2000. Für die Kunden der Anbieter bedeutet dies einen erleichterten Zugang zum Rechtsschutz ohne das Kostenrisiko eines Zivilprozesses. Nur in Bezug auf personenbezogene Daten, die beim Anbieter (auch) für eigene betriebliche Zwecke vorhanden sind, bleibt die Zuständigkeit der ordentlichen Gericht nach § 1 Abs. 5 DSG 2000 bestehen. Allfällige Schadenersatzansprüche, die aus einer rechtswidrigen Verwendung von Vorratsdaten durch den Anbieter resultieren, sind somit nach dem Regime des Amtshaftungsgesetzes zu beurteilen, ebenso allenfalls in weiterer Folge erwachsende Regressansprüche des Bundes gegenüber dem Anbieter.

Hinsichtlich des Rechts auf Information (§ 24 DSG 2000) bzw. des Rechts auf Auskunft (§ 26 DSG 2000) besteht aber das Problem, dass die Anbieter praktisch nicht beurteilen können, wann eine Information/Auskunft die Ermittlungen gefährden würde und damit eine Ausnahme von der Informationspflicht gemäß § 24 Abs. 4 iVm § 17 Abs. 3 Z 5 DSG 2000 vorliegt, weil dies „zur Verwirklichung des Zweckes der Datenanwendung notwendig ist“. Aus diesem Grund stellt der Verweis auf die Auskunft bzw. Information nach der StPO (gegenwärtig § 139) als lex specialis die entsprechende Rechtssicherheit für die Adressaten des TKG her.

Zu § 102b Abs. 2

Die Wendung „unverzüglich“ impliziert keinesfalls, dass Anbieter zur Einrichtung eines Journaldienstes zur Erteilung von Auskünften über Vorratsdaten verpflichtet sind. Eine Verpflichtung zur Beauskunftung außerhalb der Bürozeiten besteht daher nicht.

Eine Auskunft über Stammdaten, für die eine Auswertung von Verkehrsdaten notwendig ist, gilt als Auskunft über Daten einer Nachrichtenübermittlung im Sinne des § 134 Z 2 StPO. Damit wird die „Interpretationslücke“ in Bezug auf § 134 Z 2 StPO geschlossen, die zur Judikaturdivergenz zwischen dem 11. (Straf-)Senat des OGH, GZ 11 Os 57/05z einerseits und dem Bescheid der Datenschutzkommission vom 3.10.2007, K121.279/0017-DSK/2007, dem diese Entscheidung der DSK bestätigenden VwGH-Erkenntnis vom 27.5.2009, GZ 2007/05/0280 sowie jüngst dem 4. (Zivil-)Senat des OGH vom 14.7.2009, GZ 4 Ob 41/09x andererseits zuletzt besteht. Weil nach dem Standpunkt des 11. (Straf-)Senats des OGH eine „Auskunft über Daten einer Nachrichtenübermittlung“ dann nicht vorliegt, wenn solche Daten zwar vom Anbieter als Zwischenschritt ausgewertet werden, das Ergebnis der

Auskunft aber nur auf die Ermittlung der Identität hinter den auszuwertenden Verkehrsdaten abzielt und sich damit nur auf Stammdaten bezieht.

Gemeinsam mit der Legaldefinition „Öffentliche IP-Adresse“ in § 92 Abs. 3 Z 15, mit der IP-Adressen jedenfalls Zugangsdaten sind und nur bei vertraglich zugesicherten, konkreten IP- Adressen zugleich als Stammdatum zu qualifizieren sind, wird diese Frage geklärt, und zwar im Sinne der Entscheidung des 11. Senats des OGH vom 14.7.2009, dass der Vorgang insgesamt eine Verkehrsdatenauswertung bleibt, auch wenn die Behörden am Ende nur die Stammdaten erhalten; damit ist eine solche Auskunft den strengeren Regeln unterworfen, insbesondere der Kontrolle der staatsanwaltlichen Anordnung oder kriminalpolizeilichen Handlung durch den Haft- und Rechtsschutzrichter. Siehe dazu auch die Ausführungen zu § 99 Abs. 5 Z 2.

Zu § 102c Abs. 1

Daten sollen – wenn sie ausschließlich aufgrund § 102a beim Provider vorhanden sind – gekennzeichnet sein und strengeren Zugriffs- und Sicherheitsbestimmungen unterliegen. Dies ist erforderlich, damit die speicherpflichtigen Anbieter sicherstellen können, dass nur besonders ermächtigte Personen Zugang zu diesen Daten haben. Ansonsten richten sich die Datensicherheitsbestimmungen nach dem bestehenden Maßstab des § 14 DSG.

Die unmittelbare verfassungsrechtliche Pflicht der Provider aufgrund der Drittwirkung des § 1 Abs. 5 DSG gebietet auch eine entsprechende Dokumentation schon durch die Anbieter selbst, und nicht nur durch die Strafverfolgungsbehörden, denen die Daten im Auskunftsfall übermittelt werden.

Die Datenschutzkommission ist zwar nicht zuständig für die Kontrolle, ob im Einzelfall auch die materiellen Voraussetzungen für Auskünfte an die Strafverfolgungsbehörden gegeben waren, aber dafür, an wen und in welchen Fällen Daten von den Anbietern übermittelt wurden, auch im Hinblick auf allfällige Auskunftsansprüche Betroffener gegen die Anbieter sowie zur Überprüfung der Datensicherheitsmaßnahmen nach Art. 9 Abs. 1 der RL 2006/24/EG.

Zu § 102c Abs. 2

Die Protokollierung hat derartig zu erfolgen, dass die Bundesregierung jedenfalls über jene Rohdaten verfügt, welche sie zur Erfüllung ihrer Verpflichtung nach Art. 10 RL 2006/24/EG, der Kommission jährlich eine Statistik zu übermitteln, benötigt. Synergien sollten sich ergeben, wenn die Protokollierung im Zusammenhang mit der Verrechnung der einzelnen Auskunft erfolgen kann. Gleichzeitig soll damit auch eine wesentliche Rechtsschutzaufgabe erfüllt werden. Die Aufbereitung der Statistik für die EU-Kommission obliegt dem Justizministerium, welchem die Protokolldaten daher nach Abs. 4 zu übermitteln sind.

Zu § 102c Abs. 2 Z 1

Bei Anfragen der Journal-Staatsanwaltschaft muss zumindest die Geschäftszahl der Polizei angegeben werden, damit die Vorratsdaten beauskunftet werden dürfen. Diesfalls muss diese Geschäftszahl als entsprechende Referenz protokolliert werden.

Zu § 102c Abs. 2 Z 3

Die Aufschlüsselung nach Kategorien soll in groben Zügen darstellen, ob es sich um Internetdaten (§ 102a Abs. 2), Telefoniedaten (Abs. 3) oder E-Mail Daten (Abs. 4) handelt.

Zu § 102c Abs. 2 Z 4

Art. 10 der RL 2006/24/EG fordert auch statistische Werte über das „Alter“ der übermittelten Daten. Die Auswertung des Alters kann hier am einfachsten durch den Anbieter erfolgen, da die zu protokollierenden Informationen im Zuge der Beauskunftung automatisiert aus den übermittelten Daten berechnet bzw. abgeleitet werden.

Zu § 102c Abs. 2 Z 5

Die Protokollierung der Identität des Betroffenen dient dazu, dass die Datenschutzkommission im Zuge von Überprüfungen auch nachträglich die Möglichkeit hat, einen Teilnehmer über eine allfällige unzulässige Verwendung seiner Daten zu informieren. Oft sind der Name und die Anschrift des von der Auskunft betroffenen Teilnehmers dem auskunftspflichtigen Anbieter nicht bekannt (z. B. anonyme Wertkarte, Strafsache gegen u.T.) und damit auch nicht protokollierbar. Dies betrifft außerdem Auskünfte über Daten zu Teilnehmern, die von der überwachten Teilnehmernummer kontaktiert wurden oder diese kontaktiert haben, aber nicht zum Netz des auskunftspflichtigen Anbieters gehören.

Zu § 102c Abs. 2 Z 6

Durch die Protokollierung der internen Zugriffe auf Vorratsdaten und die entsprechende Ermöglichung einer nachträglichen Zuordnung des Zugriffs auf bestimmte Mitarbeiter im Unternehmen des Anbieters soll sichergestellt werden, dass tatsächlich nur besonders ermächtigte Personen Zugang zu diesen Daten haben.

Zu § 102c Abs. 3 und 4

Entgegen dem Entwurf 2007 sind der Justizverwaltung lediglich die Protokolldaten zu übermitteln, eine Verpflichtung der Provider zur Erstellung von Statistiken oder zur sonstigen Auswertung von Daten im Hinblick auf die Statistik nach Art. 10 der RL 2006/24/EG wird dadurch nicht normiert. Dies obliegt vielmehr den Behörden. Die Pflicht zur Berichterstattung an die Europäische Kommission ergibt sich unmittelbar aus Art. 10 der RL 2006/24/EG.

Zu § 102c Abs. 5

Durch diese Bestimmung soll ausdrücklich klargestellt werden, dass die übermittelten Daten selbst nicht gespeichert werden, weil dies ansonsten der Löschungsverpflichtung von Vorratsdaten nach Ablauf von 6 Monaten zuwider laufen würde. Die zu protokollierenden Informationen sind auch für Beweiszwecke, dass der Anbieter seiner Auskunftsverpflichtung nachgekommen ist, jedenfalls ausreichend. Eine Aufbewahrung der Verkehrsdaten selbst ist hierfür nicht notwendig.

Zu § 103 Abs. 4

Diese Bestimmung kann aufgrund der ausdrücklichen neuen Rechtsgrundlage im vorgeschlagenen § 90 Abs. 7 entfallen. Die Regelung der Auskunft über Vorratsdaten im Zusammenhang mit den Informationspflichten der Anbieter ist in Anlehnung an die bestehende Bestimmung des § 90 Abs. 6 für Stammdatenauskünfte an Verwaltungsbehörden systematisch dort jedenfalls besser aufgehoben als im Zusammenhang mit den Regelungen zum Teilnehmerverzeichnis.

Zu § 107 Abs. 1

Die Ersetzung von „das Senden“ durch „des Sendens“ erfolgt ohne Sinnänderung der Bestimmung ausschließlich aus grammatikalischen Gründen, da das Wort „einschließlich“ die Verwendung des Genetivs verlangt.

Zu § 109 Abs. 3 Z 14

Die Änderung dient der Anpassung des TKG an die differenzierte Terminologie der neuen StPO.

Zu § 109 Abs. 3 Z 17

Diese Änderung dient der Anpassung an die Neufassung des § 98 und sanktioniert Verletzungen der neu geschaffenen Informationspflicht im Falle einer Standortdatenauskunft nach dieser Bestimmung.

Zu § 109 Abs. 3 Z 17a

Der neu geschaffene Tatbestand sanktioniert die Verletzung der Informationspflicht der Anbieter gegenüber den Betroffenen im Falle einer Auskunft über Standortdaten gemäß § 99 Abs. 5 Z 2. Hinsichtlich der Einordnung des Tatbestandes in Bezug auf die Strafhöhe wurde die bestehende Systematik, insbesondere die bestehende Bestimmung zu Verletzungen der Informationspflicht bei der Ermittlung, Verarbeitung und Übermittlung von Daten (Z 16), berücksichtigt.

Zu § 109 Abs. 3 Z 25

Durch diese Verwaltungsstrafbestimmung soll bewirkt werden, dass unverschlüsselte Übermittlungen jedenfalls unzulässig sind. Diese Bestimmung dient damit ebenfalls indirekt der Datensicherheit.