Vorblatt

1. Motive und Inhalt der Novelle zum TKG

Am 3. Mai 2006 ist 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“ in Kraft getreten. Diese war gemäß ihrem Art. 15 spätestens bis zum 15. September 2007 mit der Inkraftsetzung der erforderlichen Rechts- und Verwaltungsvorschriften umzusetzen. Österreich hat im Vorfeld 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. Österreich ist der Verpflichtung zur Umsetzung der Richtlinie allerdings bislang nicht nachgekommen. Die Gründe dafür liegen in den schwierigen Rechtsfragen und technischen Problemen sowie in grundsätzlichen Bedenken gegen die Richtlinie, die sich im Zuge des Umsetzungsprozesses stellen.

Um diese Bedenken näher begründen zu können, ist ein einleitender Blick in die Entstehungsgeschichte der Richtlinie geboten:

a. Entstehungsgeschichte der Richtlinie 2006/24/EG

Vor dem Jahr 2002 hatten nur wenige europäische Staaten verbindliche Regelungen über die Vorratsspeicherung von Kommunikationsdaten auf nationaler Ebene erlassen. Erst in der zweiten Hälfte des Jahres 2002 – und damit nach den und in Reaktion auf die Ereignisse des 11. September 2001 – wurde erstmals die Einführung einer Vorratsspeicherung von Daten auf europäischer Ebene öffentlich diskutiert. Die britische Bürgerrechtsorganisation „Statewatch“ veröffentliche einen von belgischer Seite ausgearbeiteten Entwurf eines Rahmenbeschlusses (also eines Vorschlag für eine Gesetzgebung innerhalb „dritten Säule der EU“ gemäß Art. 29-42 EUV) zur europaweiten Einführung der Vorratsdatenspeicherung.

Dieser inoffizielle Entwurf sah eine Pflicht zur Vorratsspeicherung von Daten für mindestens 12 und höchstens 24 Monate vor. Gespeichert werden sollten jene Daten, die erforderlich sind, um die Quelle, das Ziel, den Zeitpunkt und die Teilnehmer einer Kommunikation sowie das Endgerät festzustellen. Der Zugriff auf Daten sollte nur für die Verfolgung ausreichend schwerwiegender Straftaten möglich sein, nicht aber für rein präventive Zwecke. In einem umfangreichen Katalog war vorgegeben, für welche Straftaten der Zugriff möglich sein sollte. Zudem enthielt der Entwurf Regeln für die grenzüberschreitende Zusammenarbeit für Zugriffe auf die gespeicherten Daten zu Strafverfolgungszwecken. Strafverfolgungsbehörden aus jedem Staat der EU sollte der Zugang zu den in den anderen Mitgliedstaaten vorhandenen Vorratsdaten möglich sein.

Nach den Bombenanschlägen vom 11. März 2004 in Madrid beauftragte der Europäische Rat den Ministerrat mit der Prüfung von Maßnahmen für die Erarbeitung von Rechtsvorschriften über die Aufbewahrung von Verkehrsdaten durch Diensteanbieter.[1] In der Folge erarbeiteten die Regierungen Frankreichs, Irlands, Schwedens und des Vereinigten Königreichs einen gemeinsamen Vorschlag für einen Rahmenbeschluss zur Vorratsspeicherung von Kommunikationsdaten und legten diesen am 29. April 2004 dem Ministerrat vor.[2] Angesichts zunehmender grenzüberschreitender Kriminalität und als Reaktion auf die in Madrid verübten terroristischen Attentate erachteten sie eine einheitliche europäische Politik der Vorratsdatenspeicherung für erforderlich. Die Initiatoren verstanden die im Entwurf vorgesehenen Maßnahmen als Vorgehen im Bereich der justiziellen Zusammenarbeit in Strafsachen.

Diesem Entwurf zufolge sollten Verkehrs- und Standortdaten einschließlich Teilnehmer- und Nutzerdaten gespeichert werden, die im Rahmen von Telefonie, SMS-Kurzmitteilungen und Internet-Protokollen einschließlich E-Mails, erzeugt werden. Der Vorschlag sah eine Speicherdauer von mindestens 12 und maximal 36 Monaten vor. Er enthielt keine Entschädigungsregelung für entstehende Kosten der Betreiber.

Im Unterschied zum Entwurf von 2002 sah dieser Entwurf die Vorratsdatenspeicherung auch zum Zweck der Vorbeugung von Straftaten und nicht nur zur Untersuchung, Feststellung und Verfolgung von Straftaten vor. Darüber hinaus fehlte eine Beschränkung auf hinreichend schwere Straftaten sowie die Pflicht zur Aufnahme bestimmter Straftaten. Auch enthielt der Entwurf die unpräzise Regelung des Zugriffs durch „zuständige Behörden“, während der Entwurf aus dem Jahr 2002 noch von „Strafverfolgungsbehörden“ sprach.

Am 27. September 2005 verabschiedete das Europäische Parlament eine legislative Entschließung, in der es die Initiative Frankreichs, Irlands, Schwedens und des Vereinigten Königreichs ablehnte und diese Mitgliedstaaten aufforderte, ihre Initiative zurückzuziehen.[3] Die ablehnende Haltung des Europäischen Parlaments hatte mehrere Gründe. Zum einen äußerte der zuständige Berichterstatter erhebliche Zweifel an der Wahl der Rechtsgrundlage. Nach Auffassung des Rechtsausschusses des Europäischen Parlaments beinhaltete der Vorschlag verschiedene Maßnahmen, die teils der ersten Säule (EG-Vertrag), teils der dritten Säule (EU-Vertrag) zuzuordnen seien. Es seien daher zwei Rechtsakte zu erstellen. Zum anderen bestanden Zweifel an der Verhältnismäßigkeit der Maßnahme. Sie stünde nicht in einer angemessenen Zweck-Mittel-Relation, da sie weder geeignet noch erforderlich sei und eine unzumutbare Härte für die Betroffenen darstellen würde. Insbesondere wurde hervor-

[1] Erklärung des Europäischen Rates zum Kampf gegen den Terrorismus vom 25. März 2004, Ratsdokument 7764/04 vom 28. März 2004.

[2] „Entwurf eines Rahmenentschlusses über die Vorratsspeicherung von Daten, die in Verbindungen mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus“, Ratsdokument 8958/04 vom 28. April 2004.

[3] Siehe „Bericht über die Initiative der Französischen Republik, Irlands, des Königreichs Schweden und des Vereinigten Königreichs für einen Rahmenbeschluss des Rates über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus (8958/2004 – C6-0198/2004 – 2004/0813(CNS))“, 31.5.2005, A6 – 0174/2005.

gehoben, dass die Notwendigkeit der Vorratsdatenspeicherung nicht belegt wäre. Zudem wurde eine Verletzung des Art. 8 der Europäischen Menschenrechtskonvention (EMRK) für möglich gehalten.

Im März 2005 hatte sich die Europäische Kommission der Rechtsauffassung angeschlossen, dass die gebotene Rechtsform für eine allfällige Einführung der Vorratsspeicherung jene der Richtlinie und nicht die des Rahmenbeschlusses wäre. Der damalige EU-Kommissar für Justiz, Freiheit und Sicherheit, *Franco Frattini*, forderte den Rat auf, vom Erlass des geplanten Rahmenbeschlusses abzusehen.

Am 21. September 2005, vorangetrieben durch die Terroranschläge vom 7. Juli 2005 in London, legte die Europäische Kommission schließlich einen eigenen Vorschlag einer Richtlinie zur Vorratsdatenspeicherung auf der Grundlage des Art. 95 EGV vor. Die gewählte Rechtsgrundlage räumte dem Europäischen Parlament das Recht zur Mitentscheidung ein. Dieser Richtlinienvorschlag wurde noch am selben Tag an das Parlament übermittelt. Die britische Ratspräsidentschaft[4] brachte dabei ihr Interesse zum Ausdruck, dass eine Regelung noch vor Ende des Jahres 2005 als Kompromiss in erster Lesung verabschiedet werden solle. Daraufhin nahm das Parlament rasch seine Arbeit auf. In einem Bericht des Europäischen Parlaments wurde der Hoffnung Ausdruck verliehen, dass dieses Vorgehen die Ausnahme bleiben möge und nicht zur Regel werde; es wurde von einem „extrem beschleunigten Gesetzgebungsverfahren“ gesprochen. Folge dieses Schnellverfahrens wären etwa – so der Bericht weiter – fehlerhafte Übersetzungen wie auch unzureichende Beratungszeiten gewesen.[5]

Der Entwurf sah, wie bereits der Entwurf des Rahmenbeschlusses aus dem Jahr 2004, die Verhütung von Straftaten neben der Ermittlung, Feststellung und Verfolgung von Straftaten als Zweck der Vorratsspeicherung vor. Auch die zu speichernden Datenkategorien entsprachen weitestgehend jenen des damaligen Entwurfs, wobei im Richtlinienentwurf eine genauere Umschreibung erfolgte. Ähnlich wie bereits der Entwurf von 2004 sprach der Richtlinienentwurf nur von den „zuständigen Behörden“, die Zugang zu den auf Vorrat gespeicherten Daten haben sollten. Eine Zugriffsmöglichkeit durch Geheimdienste als von den Mitgliedstaaten zu bestimmende zuständige Behörden war somit nicht ausgeschlossen. Im Unterschied zum Entwurf des Rahmenbeschlusses sah der Richtlinienentwurf eine grundsätzliche Speicherfrist von einem Jahr vor, mit Ausnahme von auf das Internet bezogenen Daten, für die eine Speicherdauer von sechs Monaten vorgesehen war. Auch enthielt er eine Erstattungsregelung hinsichtlich zusätzlicher Kosten, welche den Betreibern/Anbietern durch die Vorratsspeicherung entstehen würden.

Der federführende Ausschuss des Parlaments, der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE – Ausschuss), hatte 250 Änderungsanträge zu berücksichtigen.

[4] 1. Juli 2005 bis 31. Dezember 2005.

[5] Siehe „Bericht des Europäischen Parlaments über den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rats über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (KOM(2005)0438 – C6 0293/2005 – 2005/0182(COD)“, 28.11.2005, A6-0365/2005, S. 34.

Schließlich verständigte man sich mit den mit beratenden Ausschüssen[6] auf 87 Änderungsanträge, die dem Plenum des Europäischen Parlaments vorgelegt wurden. Fast alle Anträge hatten eine Entschärfung des Kommissionsentwurfs zum Gegenstand.

Abermals wurde Kritik an dem Umstand geübt, dass die Notwendigkeit der Maßnahme nicht hinreichend belegt wäre. So kritisierte der ITRE – Ausschuss: „Ähnlich wie beim diskutierten Rahmenbeschluss führt auch die Kommission nur den sehr pauschalen Nachweis, dass es durch die vorgeschlagenen Maßnahmen tatsächlich zu einer Verbesserung der Verbrechens- und Terrorbekämpfung kommt. Dieser Nachweis ist jedoch Grundvoraussetzung, um die erheblichen Auswirkungen und Belastungen für Bürger und Unternehmen zu rechtfertigen."[7] Es folge nämlich aus Art. 6 Abs. 1 b der Datenschutzrichtlinie 95/46/EG, dass personenbezogene Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Dies gebiete bereits der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit, denn verhältnismäßig könne eine Datenverarbeitung nur im Hinblick auf einen legitimen Zweck sein.

Wenige Tage vor der Beschlussfassung verhandelte der Ministerrat inoffiziell mit maßgeblichen EU-Parlamentariern der großen Fraktionen, jedoch ohne Beisein des zuständigen parlamentarischen Berichterstatters *Alexander Alvaro*, den Entwurf. Diese einigten sich im Rahmen einer Absprache mit dem britischen Innenminister *Charles Clarke* informell auf eine Position. Das Ergebnis dieser Verhandlungen wurde schließlich dem Parlament als Kompromissvorschlag zur Abstimmung vorgelegt.

Der zuständige Berichterstatter *Alvaro* äußerte an diesem Vorgehen massive Kritik, erinnerte an den Umstand, dass der Ausschussbericht und somit auch die Änderungsanträge mit deutlicher Mehrheit und fraktionsübergreifend (also auch mit Zustimmung der großen Fraktionen) beschlossen wurden und wies darauf hin, das diese informelle Einigung die Arbeit des Ausschusses ignoriere.

Am 14. Dezember stimmte das Europäische Parlament mit 378 zu 197 Stimmen für den Kompromissvorschlag. Der Ministerrat stimmte seinerseits am 21. Februar 2006 zu. Schließlich wurde am 15. März 2006 die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten,[8] die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG vom Europäischen Parlament und vom Rat der Europäischen Union erlassen.

[6] Mitberaten haben der Ausschuss für Industrie, Forschung und Energie (ITRE – Ausschuss) sowie der Ausschuss für Binnenmarkt und Verbraucherschutz (IMCO – Ausschuss).

[7] Siehe „Bericht über den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (KOM(2005)0438 – C6 0293/2005 – 2005/0182(COD)", 28.11.2005, A6-0365/2005, S. 41.

[8] 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.

In den Erwägungsgründen der Richtlinie wird zur Begründung ihrer Erlassung im Rahmen der ersten Säule unter anderem ausgeführt, dass die rechtlichen und technischen Unterschiede zwischen den nationalen Vorschriften zur Vorratsdatenspeicherung zum Zwecke der Ermittlung, Feststellung und Verfolgung von Straftaten den Binnenmarkt für elektronische Kommunikation beeinträchtigen, da Diensteanbieter mit unterschiedlichen Anforderungen in Bezug auf die zu speichernden Arten von Verkehrs- und Standortdaten, die für die Vorratsdatenspeicherung geltenden Bedingungen und die Dauer der Vorratsdatenspeicherung konfrontiert sind.[9] Demnach verfolgt die Richtlinie als – letztlich wettbewerbsrechtliches – Ziel die Harmonisierung der Pflichten für Diensteanbieter bzw. Netzbetreiber in Bezug auf die Vorratsdatenspeicherung, damit diese Daten für die genannten Zwecke auch tatsächlich zur Verfügung stehen, was im Sinne des in Art. 5 EGV normierten Subsidiaritätsprinzip besser auf Gemeinschaftsebene zu erreichen ist.[10]

Mit Urteil vom 10. Februar 2009 bestätigte der EuGH in einem von Irland angestrengten Nichtigkeitsverfahren gemäß Art. 230 EGV die für die Richtlinie gewählte Rechtsgrundlage des Art 95 EGV, weil „die Richtlinie 2006/24 in überwiegendem Maß das Funktionieren des Binnenmarkts betrifft", und lehnte damit die Rechtsmeinung ab, wonach die in der Richtlinie geregelte Materie in den Anwendungsbereich des Titels VI EUV fiele und statt einer Richtlinie ein Rahmenbeschluss zu erlassen gewesen wäre.[11]

b. Zur grundrechtlichen Bedenklichkeit der Richtlinie 200/24/EG

Ungeachtet der datenschutzrechtlichen Bestimmungen der Richtlinie – wie insbesondere über Sicherung des Datenzugangs gemäß den Bestimmungen des Art 8 EMRK (Art 4), Datenschutz und Datensicherheit (Art 7), unabhängige Kontrollstellen (Art 9) sowie Rechtsbehelfe, Haftung und Sanktionen (Art 13) – stellt sich angesichts neuester Entwicklungen und Studien die Frage, ob die Richtlinie *per se* mit den grundrechtlichen Anforderungen des Rechts auf Achtung des Privatlebens gemäß Art. 8 der Europäischen Menschenrechtskonvention (EMRK),[12] aus dem der Europäischen Gerichtshof für Menschenrechte (EGMR) auch ein Recht auf Datenschutz ableitet, sowie dem Recht auf Achtung des Privatlebens und dem Recht auf Schutz personenbezogener Daten gemäß Art. 7 und 8 der Charta der Grundrechte

[9] Erwägungsgrund (6) der Richtlinie.
[10] Erwägungsgrund (21) der Richtlinie.
[11] EuGH Urteil vom 10.2.2009, Rs. C-301/06, Irland (unterstützt von der Slowakischen Republik) gegen Europäisches Parlament und Rat der Europäischen Union.
[12] Die in der Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) garantierten Rechte stellen gemäß Art. 6 EUV allgemeine Grundsätze des Gemeinschaftsrechts dar und bilden so einen primärrechtlichen Prüfungsmaßstab für das Sekundärrecht, insbesondere für Verordnungen und Richtlinien.
Art. 8 EMRK („Recht auf Achtung des Privat- und Familienlebens") lautet:
„(1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.
(2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer."

der EU[13] insbesondere im Hinblick auf den Grundsatz der Verhältnismäßigkeit in Einklang gebracht werden kann. Auf Grundlage der Entstehungsgeschichte[14] und des Verweises in Art. 52 Abs. 3 der Charta auf die EMRK als grundrechtlichem Mindeststandard kann davon ausgegangen werden, dass die Tragweite der Schutzbereiche der Art. 7 und 8 der Charta sich im Wesentlichen mit Art 8 EMRK in der Auslegung durch den EGMR deckt.

Es stellt sich mit anderen Worten die Frage, ob die mit der Richtlinie verfügte Vorratsspeicherung – also die verdachtsunabhängige Speicherung von Kommunikations- und Standortdaten zum Zweck der Ermittlung, Feststellung und Verfolgung schwerer Straftaten – einerseits aus grundrechtlicher Perspektive als geeignetes Mittel zur Erreichung dieses Zwecks angesehen werden kann und anderseits, ob die grundrechtlichen Konsequenzen für den Einzelnen, aber auch die Auswirkungen auf die Gesellschaft insgesamt, in einem angemessenen Verhältnis zu den öffentlichen Interessen stehen, die mit dem genannten Zweck verfolgt werden.

Grundsätzlich sollte das Verhältnis zwischen einem demokratischen Verfassungsstaat und seiner Gesellschaft von Vertrauen geprägt sein. Der Einzelne soll darauf vertrauen können, dass in seine grundrechtlich geschützten Positionen im Zuge von Ermittlungstätigkeiten bzw. Strafverfolgungsmaßnahmen grundsätzlich nur bei Vorliegen entsprechender Verdachtsmomente, also als *ultima ratio*, unter Wahrung der rechtstaatlichen Prinzipien, insbesondere unter Beachtung des Verhältnismäßigkeitsprinzips eingegriffen wird. Der Grundsatz, dass gegen eine bestimmte Person ausschließlich bei Vorliegen von Verdachtsmomenten Ermittlungs- bzw. Verfolgungsmaßnahmen gesetzt werden, zieht sich einem roten Faden gleich durch wohl alle rechtsstaatlichen Gesetzgebungen. Die vorliegende Richtlinie geht von diesem Grundsatz nun ab, indem sie eine verdachtsunabhängige, gleichsam antizipierte „Sicherung von Beweismitteln“ vorschreibt.

Zwar werden schon derzeit vielfältig personenbezogene Daten ermittelt und verarbeitet. Diese Datenanwendungen erfolgen in aller Regel aber entweder zur individuellen Aufklärung und Verfolgung konkret begangener Straftaten, zur Erfüllung eines Vertrages und somit zumindest mittelbar auf Wunsch bzw. mit Zustimmung der datenschutzrechtlich Betroffenen, oder aber mit dem Ziel, der Gesellschaft die unterschiedlichsten Leistungen der öffentlichen Daseinsversorgung zur Verfügung zu stellen. Davon unterscheidet sich die Vorratsdaten-

[13] Die Charta entfaltet – obgleich (noch) nicht rechtsverbindlich – bereits heute für die Organe der EU für deren Rechtssetzung und für deren Mitgliedstaaten in der Umsetzung von EU-Recht eine auslegungssteuernde Wirkung.
Art. 7 der Charta der Grundrechte der EU („Achtung des Privat- und Familienlebens“) lautet:
„Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.“
Art. 8 der Charta der Grundrechte der EU („Schutz personenbezogener Daten“) lautet:
„(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.“

[14] Siehe dazu *Bernsdorff* in *Jürgen Meyer* (Hrsg.), Kommentar zur Charta der Grundrechte der Europäischen Union, 155 ff.

speicherung im Sinne der Richtlinie schon alleine durch ihre Zielsetzung in fundamentaler Weise, da personenbezogene Telekommunikations- und Bewegungsdaten aller Kunden, die Dienste eines Telekommunikationsunternehmens in Anspruch nehmen, präventiv zum Zwecke der Ermittlung, Feststellung und Verfolgung von Straftaten ohne irgendeinen konkreten Tatverdacht gesammelt und verarbeitet werden.

Mit der eingangs beschriebenen, grundrechtliche Eingriffe minimierenden rechtsstaatlichen Tradition bricht die Richtlinie. Während verarbeitete Verkehrs- und Standortdaten derzeit noch teilweise sofort, grundsätzlich aber jedenfalls dann gelöscht werden müssen, wenn und soweit sie etwa für die Bereitstellung von Telekommunikationsdiensten und in weiterer Folge für die Abrechnung nicht mehr erforderlich sind, wird diese im Sinne eines effektiven und grundrechtskonformen Datenschutzes normierte Löschungsverpflichtung nun in eine verdachtsunabhängige, flächendeckende Speicherungspflicht verkehrt, um „schwere Straftaten“, insbesondere Terrorakte und organisierte Kriminalität, bekämpfen zu können. Dies stellt im Ergebnis einen Paradigmenwechsel dar, der aus grundrechtlicher Sicht einer entsprechenden Rechtfertigung bedarf.

Es ist also der Frage nachzugehen, ob der Regelungsgehalt der Richtlinie durch die Eingriffsvorbehalte des Art. 8 EMRK gedeckt ist. Eingriffe in diese Rechte sind nach der Rechtsprechung des EGMR und des Verfassungsgerichtshofes (VfGH) nur dann zulässig, wenn diese zur Erreichung einer der in Art 8 Abs 2 EMRK genannten Ziele in einer demokratischen Gesellschaft notwendig sind. Zweifellos fällt die „Ermittlung, Feststellung und Verfolgung von schweren Straftaten“, wie es Art. 1 Abs. 1 der Richtlinie als Zweck der Vorratsdatenspeicherung bestimmt, unter die in Art. 8 Abs. 2 genannten zulässigen Ziele, insbesondere – aus generalpräventiver Sicht – zur „Verhinderung von strafbaren Handlungen“.[15]

Auch wenn das Speichern von Verkehrs- und Standortdaten auf den ersten Blick harmlos erscheinen mag, offenbart sich doch bei genauerem Hinsehen, dass die Vorratspeicherung in grundrechtlich geschützte Positionen eingreift: Im Vergleich zum Inhalt aufgezeichneter Gespräche können die gewonnen Verkehrs- und Standortdaten elektronisch unterstützt ungleich leichter, in kürzerer Zeit und größerem Umfang ausgewertet werden. Soziale Netzwerke können bis in Details ebenso nachvollzogen werden, wie – je nach Kommunikationsverhalten – mehr oder weniger genaue Bewegungsprofile jedes Menschen erstellt werden können. Schließlich können Verkehrsdaten auch Rückschlüsse über sensible Inhalte einer Kommunikation ermöglichen.[16]

Weder im Vorfeld noch im Zuge der Beschlussfassung der Richtlinie wurde allerdings – wie bereits ausgeführt – ein aussagekräftiger Nachweis der Notwendigkeit bzw. des Mehrwerts der Vorratsdatenspeicherung zum Zweck der Ermittlung, Feststellung und Verfolgung von

[15] Bei strenger Lesart dieses Eingriffsziels könnte die Ermittlung, Feststellung und Verfolgung von schweren Straftaten nicht darunter fallen, da in diesem Fall eine strafbare Handlung ja schon begangen wurde, eine systematische Interpretation aller Eingriffstatbestände begründet jedoch die Zulässigkeit der Maßnahme.

[16] Dazu ausführlich Nathan Eagle, Alex Pentland, David Lazer, Inferring Social Network Structure using Mobile Phone Data, Proceedings of the National Academy of Sciences 2007; vgl. die Erläuterungen zum Besonderen Teil zu § 94 Abs. 4.

schweren Straftaten geführt.[17] Dafür hätte über einen längeren Zeitraum hinweg beobachtet werden müssen, in wie vielen Fällen welche Daten in welchem Umfang zur Aufklärung welchen Vergehens und/oder Verbrechens beigetragen haben und wie viel Zeit zwischen der Erfassung und der An- bzw. Abfrage verstrich.

Bei näherer Analyse der Richtlinie im Zuge der Vorarbeiten zu ihrer innerstaatlichen Umsetzung in Österreich zeigte sich, dass dem klaren Eingriff in die Grundrechte der Betroffenen ein nur ausgesprochen bescheidener Mehrwert für die Strafverfolgung gegenüber steht, wie sich nicht zuletzt anhand neuerer Studien nachweisen lässt.[18] So ist es etwa für den Bereich der Festnetz- aber auch Mobiltelefonie ein Leichtes, durch Verwendung von öffentlichen Telefonzellen oder Wertkarten- bzw. im (nicht EU-)Ausland angemeldeter Handys der unmittelbar auf konkrete Personen rückführbaren Datenaufzeichnung zu entgehen. Die Aufzeichnung von E-Mail-Daten im Rahmen der Vorratsspeicherung kann etwa durch Verwendung außereuropäischer E-Mail-Provider leicht vermieden werden. Sollte zum Beispiel ein Angehöriger einer Terrororganisation oder ein Mitglied einer anderen kriminellen Vereinigung der Vorratspeicherung seiner Daten (bzw. genauer: der Möglichkeit der Rückführung der Daten auf seine Person) entgehen wollen, so ist dies ohne jedes technische Spezialwissen mit einfachsten Mitteln möglich. Stehen diese und ähnliche Möglichkeiten schon jedem „Normalverbraucher“ zur Verfügung, verfügen – und davon kann wohl mit gutem Grund ausgegangen werden – terroristische oder andere kriminelle Vereinigungen, deren Bekämpfung die Vorratsspeicherung ja in erster Linie bezweckt, über ungleich bessere technische Möglichkeiten und Kenntnisse der Umgehung der Speicherung ihrer Daten. Letztendlich werden somit fast ausschließlich Daten jener Personen erfasst, die entweder keine Kenntnis vom Umstand der Vorratsdatenspeicherung haben oder aber kein Interesse an den Tag legen, der Datenaufzeichnung zu entgehen, also die Daten ganz normaler Bürger und Bürgerinnen oder anders gesagt, sogenannter „Durchschnittsverbraucher und -verbraucherinnen“.

Nach der Rechtsprechung des EGMR stellen die Ermittlung und Aufbewahrung von Informationen über das Privatleben einer Person in einer elektronischen Datenbank sowie die Verwendung personenbezogener Daten durch eine öffentliche Behörde einen Eingriff in das durch Art 8 EMRK geschützte Recht auf Achtung des Privatlebens dar.[19] Ein solcher Eingriff

[17] Dazu *Westphal*, Die Richtlinie zur Vorratsdatenspeicherung von Verkehrsdaten – Brüsseler Stellungnahme zum Verhältnis von Freiheit und Sicherheit in der „Post-911-Informationsgesellschaft“, EuR 2006/5, 706 ff (715 mwN); *Westphal* war zum damaligen Zeitpunkt Referent beim deutschen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI).

[18] Siehe dazu etwa Deutsches Bundeskriminalamt (Autorin: *Eva Mahnken*), Mindestspeicherungsfristen für Telekommunikationsdaten, 2005.

[19] Siehe EGMR, 2.8.1984, Urteil *Malone gegen Vereinigtes Königreich* (Telefonüberwachung und Weitergabe von Verkehrsdaten durch die Postverwaltung an die Polizei), Z 62 ff (vor allem 64, 83-89); EGMR, 26.3.1987, Urteil *Leander gegen Schweden* (Speicherung in einem Sicherheitsdatenregister), Z 47-48; EGMR, 16.2.2000, *Amann gegen Schweiz* (Speicherung nach polizeilicher Telefonüberwachung), Z 68-70; EGMR, 4.5.2000, Urteil *Rotaru gegen Rumänien* (Speicherung in einem Geheimdienstregister), Z 43; EGMR, 6.6.2006, Urteil *Segerstedt-Wiberg u.a. gegen Schweden* (Speicherung in einer elektronischen Datenbank der Sicherheitspolizei), Z 70-72; EGMR, 29.6.2006, Unzulässigkeitsentscheidung *Weber und Saravia gegen Deutschland* (strategische Überwachung und Speicherung von Telekommunikationsbeziehungen aufgrund des „G 10“), Beschwerde-Nr. 54.934/00, Z 76-79 (insb. Z 79), deutschsprachige Zusammenfassung und Fundstelle der Entscheidung in: Newsletter des Österreichischen Instituts für Menschenrechte, NL 2006, 177 f (www.menschenrechte.at → online-Archiv), siehe dazu auch das vorangegangene Urteil des EGMR zu „G 10“ vom 6.9.1978 im Fall *Klass u.a. gegen Deutschland* (Telefonüberwachung wegen des Verdachts strafbarer Handlungen); EGMR, 1.8.2008, Urteil *Liberty u.a. gegen Verei-*

liegt jedoch nicht erst dann vor, wenn Inhaltsdaten verarbeitet oder aus Stamm- und Verkehrsdaten Rückschlüsse auf Inhaltsdaten gezogen werden können,[20] sondern schon bei einer Verarbeitung von Stamm- und Verkehrsdaten selbst. Jede Anwendung personenbezogener Daten schlechthin führt nach Ansicht des EGMR zu einem Eingriff in dieses Recht. Sogar das Sammeln und Speichern personenbezogener Daten ohne deren weitere Verwendung,[21] die Aufbewahrung öffentlich zugänglicher personenbezogener Informationen, wenn sie von Behörden systematisch erfasst werden,[22] sowie die Speicherung personenbezogener Daten ohne konkreten Verdacht strafbarer Handlungen[23] fällt demnach in den Schutzbereich des Art 8 EMRK.

Diese (nach eigenen Worten des EGMR: weite) Interpretation des Schutzbereichs des – das Recht auf Datenschutz einschließenden – Art 8 EMRK folgt unter anderem daraus, dass der EGMR in den Urteilen *Amann* und *Rotaru* zur Begründung auf Art 1 und 2 der Datenschutzkonvention des Europarates Bezug nimmt, die sich auf jede Form automatischer Verarbeitung personenbezogener Daten erstreckt.[24] Schon im Urteil *Malone* hielt der EGMR fest, dass Art 8 EMRK nicht nur die Überwachung von Inhaltsdaten, sondern auch die Registrierung von Verkehrsdaten schützt:[25] „… Die Registrierung unterscheidet sich daher von der

---

nigtes Königreich (systematische polizeiliche Überwachung der gesamten Telekommunikation), Z 56-57; EGMR 4.12.2008, Urteil *S. und Marper* (Speicherung von Fingerabdrücken und DANN-Proben nach einem Freispruch).

[20] Zur Überwachung von Inhaltsdaten siehe weiters EGMR, 24.4.1990, Urteil *Huvig gegen Frankreich*; EGMR, 24.4.1990, Urteil *Kruslin gegen Frankreich*; EGMR, 25.6.1997, Urteil *Halford gegen Vereinigtes Königreich*; EGMR, 25.3.1998, Urteil *Kopp gegen Schweiz*; EGMR, 24.8.1998, Urteil *Lambert gegen Frankreich*; EGMR, 3.4.2007, *Copland gegen Vereinigtes Königreich* (dieses bezieht sich auch auf E-Mail-Kommunikation und die Verwendung des Internet, die vom Schutzbereich des Art. 8 EMRK mit umfasst sind).

[21] So der EGMR im Urteil *Copland*, Z 43.

[22] EGMR Urteil *Rotaru*, Z 43; Urteil *Segerstedt-Wiberg u.a.*, Z 72; Urteil *Copland*, Z 43.

[23] Siehe EGMR Urteil *Segerstedt-Wiberg u.a.*, Z 49, wobei die Angaben der schwedischen Regierung in Richtung verdachtsunabhängiger Speicherung von Vorratsdaten zur Erfüllung präventiver Aufgaben der Sicherheitspolizei gehen. Zur grundrechtlichen Bedenklichkeit von Vorratsdatenspeicherungen siehe auch *European Union Agency for Fundamental Rights (FRA)*, Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, 28 October 2008 (http://fra.europa.eu → Products → FRA Opinions).
Siehe dazu auch das laufende Verfahren vor dem deutschen BVerfG zur Umsetzung der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten (www.vorratsdatenspeicherung.de).

[24] Urteil *Amann*, Z 65; Urteil *Rotaru*, Z 43. Siehe dazu das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Jänner 1981 (ETS No. 108), ergänzt durch das Zusatzprotokoll vom 8. November 2001 (ETS No. 181).
Dessen Art. 1 („Gegenstand und Zweck“) lautet:
„Zweck dieses Übereinkommens ist es, im Hoheitsgebiet jeder Vertragspartei für jedermann ungeachtet seiner Staatsangehörigkeit oder seines Wohnorts sicherzustellen, daß seine Rechte und Grundfreiheiten, insbesondere sein Recht auf einen Persönlichkeitsbereich, bei der automatischen Verarbeitung personenbezogener Daten geschützt werden (‚Datenschutz’).“
Und Art. 2 („Begriffsbestimmungen“) lautet:
„In diesem Übereinkommen:
a. bedeutet ‚personenbezogene Daten’ jede Information über eine bestimmte oder bestimmbare natürliche Person (‚Betroffener’);
b. bedeutet "automatisierte Datei/Datensammlung" jede zur automatischen Verarbeitung erfaßte Gesamtheit von Informationen;
c. umfaßt ‚automatische Verarbeitung’ die folgenden Tätigkeiten, wenn sie ganz oder teilweise mit Hilfe automatisierter Verfahren durchgeführt werden: das Speichern von Daten, das Durchführen logischer und/ oder rechnerischer Operationen mit diesen Daten, das Verändern, Löschen, Wiedergewinnen oder Bekanntgeben von Daten;
d. bedeutet ‚Verantwortlicher für die Datei/Datensammlung’ die natürliche oder juristische Person, die Behörde, die Einrichtung oder jede andere Stelle, die nach dem innerstaatlichen Recht zuständig ist, darüber zu entscheiden, welchen Zweck die automatisierte Datei/Datensammlung haben soll, welche Arten personenbezogener Daten gespeichert und welche Verarbeitungsverfahren auf sie angewendet werden sollen.“

[25] EGMR Urteil *Malone*, Z 56, 64 und 83-89 („Metering“).

Natur der Sache her von der Kommunikationsüberwachung, die, falls nicht gerechtfertigt, zumeist unerwünscht und illegitim ist in einer demokratischen Gesellschaft. Dennoch ist der Gerichtshof nicht der Meinung, dass die Nutzung derart zusammengetragener Fakten niemals zu Problemen im Bereich des Art. 8 EMRK führen könnte. Ein so zusammengestelltes Verzeichnis enthält Informationen – insbesondere die angewählten Nummern – die Bestandteil der Telefongespräche sind. In den Augen des Gerichtshofs führt die Freigabe dieser Informationen an die Polizei ohne Zustimmung des Teilnehmers zu einem Eingriff in ein von Art. 8 EMRK garantiertes Recht."[26] Im neueren Urteil *Copland* bestätigte der EGMR seine Rechtsauffassung aus dem Urteil *Malone* und weitet sie auf E-Mail-Korrespondenz und Nutzung des Internet aus: „Der Gerichtshof erinnert daran, dass die Verwendung von Informationen über den Zeitpunkt und die Länge eines Telefongesprächs und im Besonderen über die gewählten Nummern einen Aspekt des Art 8 EMRK betreffen, da diese Informationen einen ‚integralen Bestandteil der Telefonkommunikation darstellen'. … Daher erachtet der Gerichtshof das Sammeln und Speichern persönlicher Informationen sowohl in Bezug auf die Telefongespräche der Beschwerdeführerin als auch ihre E-Mail- und Internet-Nutzung ohne ihr Wissen als Eingriff in ihr Recht auf Achtung ihres Privatlebens und Korrespondenz im Sinne des Art 8 EMRK."[27]

Schon in den Urteilen *Klass u.a.* und *Malone* als auch zuletzt in der Unzulässigkeitsentscheidung *Weber und Saravia* sowie im Urteil *Liberty u.a.* führt der EGMR aus, dass selbst das bloße Bestehen von Gesetzen, die ein System der geheimen Überwachung der Kommunikation erlauben, als solche für alle Personen, auf die sie Anwendung finden können, die Gefahr einer Überwachung mit sich bringt. Diese Gefahr greift nach dem EGMR notwendigerweise in die Freiheit der Kommunikation zwischen Benutzern von Telekommunikationseinrichtungen ein und stellt daher ungeachtet tatsächlich gegen sie ergriffener Maßnahmen einen Eingriff in Art 8 EMRK dar.[28]

Von der Vorratsdatenspeicherung sind durch die Richtlinie und deren nationale Umsetzungsgesetze alle Menschen im EU-Raum betroffen, in deren Grundrechtssphäre dadurch eingegriffen wird. Zu bedenken ist auch, dass im Fall einer konkreten Datenanwendung durch Strafverfolgungsbehörden aber nicht nur in die Rechtssphäre etwa eines möglichen Straftäters oder dessen Komplizen eingegriffen wird, sondern auch in die Rechtssphäre derjenigen Personen, die mit den Adressaten der Maßnahme über Telekommunikationseinrichtungen nur zufällig in Verbindung standen oder stehen.[29] Dies schafft aber nach der Ansicht des EGMR ein System der Überwachung zum Schutz der Sicherheit des Staates und der Gesellschaft, das die Demokratie bzw. die Rechtsstaatlichkeit, die es schützen soll, aushöhlen bzw. umgehen könnte.[30]

[26] Ibid, Z 84 (deutsche Übersetzung aus EuGRZ 1985, 23).
[27] EGMR Urteil *Copland*, Z 43 und 44, unter Zitierung des Urteils *Malone*, Z 84 (deutsche Übersetzung vom Autor).
[28] EGMR Urteil *Klass u.a.*, Z 41; EGMR Urteil *Malone*, Z 64; EGMR Beschluss *Weber und Saravia*, Z 78, sowie Urteil *Liberty u.a.*, Z 56.
[29] Vgl. dazu BVerfGE 109, 279 (308).
[30] Siehe in diesem Sinn den EGMR im Urteil *Leander*, Z 60; und im Urteil *Klass u.a.*, Z 49.

Aus all dem folgt in systematischer Auslegung der Rechtsprechung des EGMR, dass die Vorratsdatenspeicherung einen Eingriff in das Recht auf Achtung des Privatlebens gemäß Art 8 EMRK und das daraus abgeleitete Recht auf Datenschutz bewirkt. Zur Beantwortung der Frage, ob die verdachtsunabhängige Speicherung von Daten auf Vorrat aber mit Art 8 EMRK in Einklang steht, sind vor allem zwei Urteile des EGMR zu beachten:

Im Urteil *S. und Marper gegen Vereinigtes Königreich* zur Speicherung von Fingerabdrücken und DNA-Proben nach einem Freispruch hat der EGMR die Bedeutung des Datenschutzes für das Privatleben, wie es in Art 8 EMRK gewährleistet ist, noch einmal ausdrücklich betont und auf die Notwendigkeit des Schutzes dieser Daten bei ihrer Anwendung durch das nationale Recht hingewiesen.[31] Fingerabdrücke enthalten einmalige Informationen über eine Person, die ihre präzise Identifizierung erlauben. Sie sind nach Auffassung des EGMR daher geeignet, ihr Privatleben zu beeinträchtigen. Die Speicherung solcher Informationen ohne Zustimmung der betroffenen Person könne nicht als neutral oder unbedeutend abgetan werden. Die Speicherung von Fingerabdrücken in den Aufzeichnungen der Behörden im Zusammenhang mit einer identifizierbaren Person kann daher für sich gewichtige Bedenken hinsichtlich ihres Privatlebens aufwerfen. Im vorliegenden Fall wurden die Fingerabdrücke in einem Strafverfahren abgenommen und in einer landesweiten Datenbank gespeichert, um dort für Zwecke der Ausforschung von Straftätern aufbewahrt und regelmäßig verarbeitet zu werden. Wenngleich hinsichtlich der Rechtfertigung zwischen der Speicherung von Zellproben und DNA-Profilen einerseits und Fingerabdrücken andererseits unterschieden werden muss, begründet auch die Speicherung von Fingerabdrücken einen Eingriff in das Recht auf Achtung des Privatlebens.

Zur Rechtfertigung des Eingriffs führt der EGMR aus, dass die Speicherung der Fingerabdrücke und DNA-Informationen dem legitimen Ziel der Aufklärung und damit der Verhütung von Straftaten dient. Ohne Zweifel bedürfe, so der EGMR, der Kampf gegen das Verbrechen der Verwendung moderner wissenschaftlicher Methoden der Ermittlung und Identifizierung. Die Frage sei nicht, ob die Aufbewahrung von Fingerabdrücken, Zellproben und DNA-Profilen im Allgemeinen als konventionskonform angesehen werden kann. Die einzige zu prüfende Frage ist, ob die Speicherung der Fingerabdrücke und DNA-Daten bestimmter Straftaten verdächtiger, aber nicht verurteilter Personen nach Art 8 Abs 2 EMRK gerechtfertigt ist. Unter Berücksichtigung des Rechts und der Praxis der Konventionsstaaten führt der EGMR aus, dass die Grundprinzipien des Datenschutzes verlangen, dass die Speicherung von Daten im Hinblick auf den Zweck der Datensammlung verhältnismäßig und die Aufbewahrung zeitlich beschränkt ist. Der EGMR verweit darauf, dass die meisten Staaten sich dazu entschieden haben, der Speicherung und Verwendung solcher Daten Grenzen zu setzen, um einen angemessenen Ausgleich mit dem Interesse am Schutz des Privatlebens zu erreichen. Der starke Konsens zwischen den Konventionsstaaten engt nach Ansicht des EGMR den Ermessensspielraum der Staaten auf diesem Gebiet ein. Der EGMR anerkennt, dass eine Datenbank zur Aufklärung und Verhütung von Straftaten beitragen kann. Dennoch bleibe die Frage offen, ob eine solche Speicherung verhältnismäßig ist und einen gerechten Ausgleich zwischen den widerstreitenden öffentlichen und privaten Interessen trifft. Der

[31] EGMR 4.12.2008, Urteil *S. und Marper.*

EGMR gelangt zum Schluss, dass die umfassende und wahllose Befugnis zur Speicherung von Fingerabdrücken, Zellproben und DNA-Profilen von verdächtigten, aber nicht verurteilten Personen, keinen gerechten Ausgleich zwischen den widerstreitenden öffentlichen und privaten Interessen trifft und der belangte Staat in dieser Hinsicht jeden akzeptablen Ermessensspielraum überschritten hat. Die umstrittene Speicherung begründe daher einen unverhältnismäßigen Eingriff in das Recht auf Achtung des Privatlebens, der nicht als in einer demokratischen Gesellschaft notwendig angesehen werden kann. Daher stellte der EGMR in diesem Fall einstimmig eine Verletzung von Art 8 EMRK fest. Das Urteil ist im vorliegenden Zusammenhang deshalb von besonderem Gewicht, weil selbst die Speicherung personenbezogener Daten von Personen, die einmal im Verdacht standen, eine strafbare Handlung begangen zu haben, vom EGMR als Verletzung des Art 8 EMRK betrachtet wird. Umso mehr wirft die völlig verdachtsunabhängige Speicherung von Vorratsdaten die Frage nach einer Verletzung dieses Konventionsrechts auf.

Aus diesen Überlegungen folgt, dass die Frage, ob die Richtlinie mit Art 8 EMRK in Einklang steht, derzeit noch nicht endgültig beantwortet werden kann. Eine rechtsverbindliche Antwort darauf werden mit großer Wahrscheinlichkeit entweder das deutsche Bundesverfassungsgericht (BVerfG) und/oder der Europäische Gerichtshof (EuGH) und/oder der Europäische Gerichtshof für Menschenrechte (EGMR) geben:

Zum einen ist beim BVerfG derzeit eine Beschwerde von ca. 30.000 Personen anhängig, die sich gegen das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“[32] wendet, in der unter anderem auch ein Verstoß der Richtlinie gegen das aus Art. 8 Abs. 2 EMRK abgeleitete Recht auf Datenschutz geltend gemacht wird.[33] Der Antrag hatte vorläufig teilweise Erfolg und führte zur Erlassung einer einstweiligen Anordnung, mit der die Anwendung einiger der angefochtenen gesetzlicher Bestimmungen bis zur Entscheidung über die Verfassungsbeschwerde außer Kraft gesetzt wurden.[34] Denkbar ist, dass das BVerfG zur Klärung dieser Frage ein Vorabentscheidungsverfahren vor dem EuGH anstrengt, in der Sache selbst entscheidet und/oder im Fall der Abweisung der Beschwerde die Angelegenheit von den nicht erfolgreichen Beschwerdeführern und Beschwerdeführerinnen dem EGMR vorgelegt wird.

Zum anderen hat die Republik Österreich im ebenfalls derzeit laufenden und von der Europäischen Kommission eingeleiteten Vertragsverletzungsverfahren gemäß Art. 226 Abs. 2

[32] BGBl I 70/2007 vom 31.12.2007, S. 3198.
[33] Siehe die Dokumentation des Verfahrens in www.vorratsdatenspeicherung.de
[34] BVerfG, 1 BvR 256/08 vom 11.3.2008 http://www.bverfg.de/entscheidungen/rs20080311_1bvr025608.html, BGBl I 13/2008, S. 659; unter den GZ 1 BvR 263/08 und 1 BvR 586/08 sind weitere Beschwerden beim BVerfG erfasst, die Verfahren werden unter einem geführt. Mit Beschluss vom 1.10.2008, 1 BvR 256/08 verlängerte das BVerfG diese einstweilige Anordnung um weitere sechs Monate, längstens jedoch bis zur Entscheidung in der Hauptsache. Erneuert und erweitert wurde die einstweilige Anordnung durch Beschluss des BVerfG vom 28.10.2008, 1 BvR 256/08: http://www.bverfg.de/entscheidungen/rs20081028_1bvr025608.html, BGBl I 53/2008, S. 2239. Zuletzt wurde mit Beschluss des BVerfG vom 22.04.2009, 1 BvR 256/08, die einstweilige Anordnung wiederholt: http://www.bverfg.de/entscheidungen/rs20090422_1bvr025608.html, BGBl I 27/2009, S. 1139.

EGV wegen Nichtumsetzung der Richtlinie[35] in ihrer Klagebeantwortung gemäß Art. 241 EGV Einwände im Hinblick auf die Vereinbarkeit der Richtlinie mit dem Recht auf Datenschutz gemäß Art. 8 EMRK und Art. 8 der EU-Grundrechtecharta vorgebracht.

Vor diesem Hintergrund ergibt sich, dass in absehbarer Zeit mit einer verbindlichen Entscheidung über die Frage der Grundrechtskonformität der Richtlinie gerechnet werden kann, die bis dahin zum Rechtsbestand der Europäischen Union zählt und von den Mitgliedstaaten umzusetzen ist, soweit dies noch nicht geschehen ist. Die innerstaatliche Umsetzung der Richtlinie hat rasch zu erfolgen, um eine Verurteilung Österreichs durch den EuGH im Vertragsverletzungsverfahren möglichst zu vermeiden.

2. Alternativen zur Umsetzung der Richtlinie 2006/24/EG

Keine: Eine weitere Nichtumsetzung der Richtlinie – aus welchen Gründen auch immer – würde zu einer Verurteilung Österreichs zu Strafzahlungen gemäß Art. 230 EGV im bereits anhängigen Vertragsverletzungsverfahren führen, dem eine von der Europäischen Kommission gegen Österreich gerichtete Klage gemäß Art. 226 EGV zugrunde liegt. Ob die in diesem Verfahren von Österreich gemäß Art. 241 EGV erhobenen Einwendungen gegen die Richtlinie wegen grundrechtlicher Bedenken zum Erfolg führen, ist zwar ungewiss, aber eher unwahrscheinlich. Hier ist anzumerken, dass die Republik Österreich seinerzeit im Rat der europäischen Union für die Erlassung der Richtlinie 2006/24/EG gestimmt hat und in der Folge auch keinen Gebrauch von der Möglichkeit gemacht hat, binnen offener Frist ein Nichtigkeitsverfahren gemäß Art. 230 EGV gegen diese Richtlinie anzustrengen.

Sollte allerdings der EuGH oder der EGMR in allenfalls bei ihnen anhängig gemachten Verfahren auf einen Verstoß der Richtlinie gegen Art. 8 EMRK erkennen, so müsste die innerstaatliche gesetzliche Umsetzung der Richtlinie rückgängig gemacht werden.

3. Innerstaatlicher Anpassungsbedarf

a) Strafprozessordnung (StPO)

Die vorgeschlagene TKG-Novelle erfordert jedenfalls deshalb eine Anpassung der StPO, weil die neue Bestimmung des § 99 Abs. 5 TKG eine Verarbeitung von Verkehrsdaten für Auskünfte über Daten einer Nachrichtenübermittlung (§ 134 StPO) nur aufgrund einer gesetzlichen Bestimmung erlaubt, die „auf diesen Absatz zu verweisen, die konkreten Datenkategorien aufzuzählen, die berechtigten Behörden zu benennen und den Datenumfang auf das notwendige und verhältnismäßige Ausmaß zu beschränken“ hat. Außerdem darf gemäß der neuen Bestimmung § 102b TKG „eine Auskunft über Vorratsdaten (…) nur nach Maßgabe einer ausdrücklich auf § 102a verweisenden gesetzlichen Bestimmung erteilt werden. Dadurch ist zumindest ein insofern „formeller“ Verweis auf die genannten Bestimmungen des

[35] EuGH Rs. C-189/09, Kommission der Europäischen Gemeinschaften gegen Republik Österreich.

TKG in der StPO perpetuiert, als ansonsten eine Verarbeitung von Verkehrsdaten zu Auskunftszwecken nicht zulässig ist. Darüber hinaus scheint im Hinblick auf die Zulässigkeit der Verwendung von Vorratsdaten eine Anpassung der StPO aus nachfolgenden Erwägungen indiziert:

Die Richtlinie sieht vor, dass bestimmte Kommunikationsdaten zum Zweck der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie jeweils vom nationalen Recht bestimmt werden, gespeichert werden sollen. Die vorgeschlagene Novellierung des TKG zur Umsetzung der Richtlinie verweist zwar auf den Zweck der Vorratsdatenspeicherung und legt fest, dass diese nur zur Ermittlung, Feststellung und Verfolgung von „schweren Straftaten" erfolgen darf (§ 102a TKG), was aber unter einer „schweren Straftat" zu verstehen ist, kann aus Gründen der Sachzuständigkeit nicht über das TKG, könnte aber wohl im Rahmen des 5. Abschnitts der StPO geregelt werden (§§ 134 StPO). Um diesbezüglich schon von Gesetzes wegen Rechtssicherheit herzustellen und die Auslegung des Begriffs nicht der Rechtsprechung zu überlassen, ergibt sich ein entsprechender Anpassungsbedarf, der von folgenden Überlegungen geleitet sein könnte:
Auch wenn die Richtlinie die Definition ins nationale Recht verweist, so ergeben sich doch aus der Entstehungsgeschichte Hinweise darauf, woran der europäische Gesetzgeber gedacht hat. Ursprünglich dominierte der Gedanke der Bekämpfung des Terrorismus und schwerer Kriminalität als Zweckbindung der Vorratsdatenspeicherung. Im ursprünglichen Vorschlag der Kommission hieß es sogar im Normtext ausdrücklich „… Verfolgung von schweren Straftaten wie Terrorismus und organisierter Kriminalität".[36] Auch in den Erwägungsgründen (7)-(9) der beschlossenen Richtlinie wird der Zusammenhang mit der Bekämpfung von Terrorismus und organisierter Kriminalität nach wie vor mehrfach deutlich.
In der Gemeinsamen Erklärung des Rates und der Kommission vom 17. Februar 2006[37] findet sich schließlich die Aussage, dass die Mitgliedstaaten bei der Auslegung der schweren Straftat die Taten im Sinne des Art. 2 Abs. 2 des Rahmenbeschlusses über den Europäischen Haftbefehl[38] sowie Straftaten unter Einsatz von Telekommunikationseinrichtungen angemessen zu berücksichtigen haben. Zu Taten im Sinne des Art. 2 Abs. 2 des Rahmenbeschlusses zählen nun die folgenden 32 Deliktsgruppen:

1. Beteiligung an einer kriminellen Vereinigung,
2. Terrorismus,
3. Menschenhandel,
4. sexuelle Ausbeutung von Kindern und Kinderpornografie,
5. illegaler Handel mit Drogen und psychotropen Stoffen,
6. illegaler Handel mit Waffen, Munition und Sprengstoffen,
7. Korruption,
8. Betrugsdelikte, einschließlich Betrug zum Nachteil der finanziellen Interessen der Europäischen Gemeinschaften im Sinne des Übereinkommens vom 26. Juli 1995 über den Schutz der finanziellen Interessen der Europäischen Gemeinschaften,

[36] KOM (2005) 438 endg.
[37] 5777/06 ADD 1 REV 1 COPEN 7 TELECOM 3 CODEC 78.
[38] Rahmenbeschluss des Rates vom 13.06.2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten, ABl L 190, 1 vom 18.07.2002.

9. Wäsche von Erträgen aus Straftaten,
10. Geldfälschung, einschließlich der Euro-Fälschung,
11. Cyberkriminalität,
12. Umweltkriminalität, einschließlich des illegalen Handels mit bedrohten Tierarten oder mit bedrohten Pflanzen- und Baumarten,
13. Beihilfe zur illegalen Einreise und zum illegalen Aufenthalt,
14. vorsätzliche Tötung, schwere Körperverletzung,
15. illegaler Handel mit Organen und menschlichem Gewebe,
16. Entführung, Freiheitsberaubung und Geiselnahme,
17. Rassismus und Fremdenfeindlichkeit,
18. Diebstahl in organisierter Form oder mit Waffen,
19. illegaler Handel mit Kulturgütern, einschließlich Antiquitäten und Kunstgegenstände,
20. Betrug,
21. Erpressung und Schutzgelderpressung,
22. Nachahmung und Produktpiraterie,
23. Fälschung von amtlichen Dokumenten und Handel damit,
24. Fälschung von Zahlungsmitteln,
25. illegaler Handel mit Hormonen und anderen Wachstumsförderern,
26. illegaler Handel mit nuklearen und radioaktiven Substanzen,
27. Handel mit gestohlenen Kraftfahrzeugen,
28. Vergewaltigung,
29. Brandstiftung,
30. Verbrechen, die in die Zuständigkeit des Internationalen Strafgerichtshofs fallen,
31. Flugzeug- und Schiffsentführung,
32. Sabotage.

Selbst wenn aber ein Tatbestand in eine der genannten Deliktsgruppen einzuordnen ist, bedarf es zusätzlich noch einer Höchststrafe von mindestens drei Jahren Freiheitsstrafe. Schon diese Überlegungen auf europäischer Ebene zeigen, dass das neue Ermittlungsinstrument nicht für jede, sondern – gemessen an der österreichischen Rechtsordnung – nur für wegen ihrer Verbindung zu Terrorismus und besonderer Kriminalität schwerer wiegende Delikte eingesetzt werden sollte. Auch wenn die Richtlinie letztlich zur Definition auf das nationale Recht verweist, ist den Vorarbeiten und der Gemeinsamen Erklärung doch eine gewisse der europäischen Gesetzgebung immanente Wertung dahingehend erkennbar, welcher Art die Taten sein müssen, die den Einsatz der Vorratsdatenspeicherung erlauben sollen – nämlich terroristische Straftaten, organisierte Kriminalität, signifikante Formen von Vermögens- und Gewaltdelikten sowie staatsgefährdende Handlungen.

Vor dem Hintergrund des Zwecks der Richtlinie und des mit der Vorratsdatenspeicherung verbundenen Grundrechtseingriffs ist die nationale Umschreibung der schweren Straftat als jede Vorsatz- oder Fahrlässigkeitstat mit einer Strafdrohung von mehr als einem Jahr Freiheitsstrafe iSd § 17 SPG (ergänzt um die gefährliche Drohung und beharrliche Verfolgung, wie dies noch im Ministerialentwurf einer TKG-Novelle vorgeschlagen worden war[39]) jeden-

[39] BMVIT, Zl. 630.333/0001-III/PT2/2007.

falls problematisch. Es besteht im Übrigen auch keine Notwendigkeit, auf die Definition des SPG zurückzugreifen: Erstens hat der österreichische Strafgesetzgeber selbst für Zwecke der Strafverfolgung in § 17 StGB eine Einteilung in leichtere und schwerere Straftaten getroffen: nämlich in Vergehen und Verbrechen. Letztere sind nur Vorsatztaten, die mit mehr als drei Jahren Freiheitsstrafe geahndet werden. Und zweitens berücksichtigt das Kriminalstrafrecht schon seit langem auch bei der Einteilung in Vergehen und Verbrechen Gefahrenabwehraspekte: Grundsätzlich hat jede Strafverfolgung auch die Funktion der Gefahrenabwehr und Prävention. Im Besonderen bezwecken Vorbereitungs- und Organisationsdelikte, gerade auch im Bereich des Terrorismus, die Erfassung und Abwehr von Gefahren im Vorfeld. Zu nennen sind dabei die Delikte der kriminellen Organisation (§ 278a StGB) und terroristischen Vereinigung (§ 278b StGB) sowie der Terrorismusfinanzierung (§ 278d StGB), die allesamt den Verbrechensbegriff erfüllen. Insofern wäre es konsequent und sachgerecht, die Definition des Verbrechens als Umschreibung der schweren Straftat zu verwenden.[40]
Zu bedenken sind bei der Auslegung weiters prozessuale Aspekte, die diese Definition der schweren Straftat als Verbrechen zu stützen vermögen: Der Gesetzgeber öffnet geheime Maßnahmen in unterschiedlicher Breite für Ermittlungen. Schon für die traditionelle Überwachung der Telekommunikation zieht er eine Schwelle, die oberhalb des § 17 SPG liegt. Denn ohne Zustimmung des Betroffenen ist eine Überwachung nur bei Vorsatztaten und nur bei mehr als einem Jahr Freiheitsstrafdrohung zulässig. Betrachtet man die weiteren geheimen Maßnahmen, so fällt auf, dass der Gesetzgeber bei der derzeit wohl eingriffsintensivsten geheimen Maßnahme die Eingriffsschwelle sehr hoch anlegt: Immerhin geht es beim großen Lauschangriff (§ 136 Abs 1 Z 3 StPO) um Organisationsdelikte und Verbrechen mit mehr als zehn Jahren Freiheitsstrafe. Dass die Vorratsdatenspeicherung nicht mit dem großen Lauschangriff gleichgesetzt werden kann, liegt auf der Hand. Immerhin geht es bei der Vorratsdatenspeicherung um „bloße“ äußere Kommunikations- und Standortdaten, wohingegen beim großen Lauschangriff im Überwachungszeitraum sowohl Äußerungen wie auch das Verhalten der überwachten Person umfassend erhoben werden. Daher wäre es nicht sachgerecht, die Verwendung von Vorratsdaten auf die Fälle des großen Lauschangriffs zu beschränken.

Für den Bereich zwischen § 17 SPG und § 17 StGB hat sich der Gesetzgeber erst kürzlich dahingehend geäußert, dass ein schwerwiegendes Verbrechen in der Regel dann vorliegt, wenn es um ein Verbrechen mit einer Strafdrohung von mehr als fünf Jahren Freiheitsstrafe geht oder sonst ein schwerer Schaden oder Nachteil verursacht wurde.[41] Obgleich es in diesem Zusammenhang um die Berichtspflicht der Kriminalpolizei an die Staatsanwaltschaft geht, lässt sich dennoch auch daraus eine Gewichtung erkennen. Eine solche Bedeutung, dass von Anfang an die Staatsanwaltschaft ins Verfahren involviert sein muss, haben nicht alle Straftaten, nicht einmal alle Verbrechen, sondern nur schwere Verbrechen. Bei ihnen bedarf es offensichtlich besonderer Verfahrensführung und besonderer Maßnahmen. Daher ist davon auszugehen, dass bei Verbrechen mit einer Strafdrohung von mehr als fünf Jahren

[40] Ähnlich BKA-VD, Stellungnahme zum Ministerialentwurf einer TKG-Novelle, 10 SN-61/ME XXIII.GP.
[41] EBRV 25 BlgNR XXII.GP 133.

Freiheitsstrafe jedenfalls eine schwere Straftat im Sinne des nationalen Rechts vorliegt.[42] Einzuräumen ist allerdings, dass diese Schwelle weit über den Vorstellungen der Gemeinsamen Erklärung von Rat und Kommission liegt, weshalb dieser Zugang zur Begriffsdefinition vor dem Hintergrund europäischer Wertungen eher problematisch erscheint.

Freilich ließe aber auch eine Festlegung auf den Verbrechensbegriff des § 17 StGB zur Definition des Begriffs „schwere Straftat" Wertungswidersprüche und Probleme zu Tage treten: So wäre etwa der Entzug der persönlichen Freiheit gemäß Art. 2 Abs. 2 Z. 1 des Bundesverfassungsgesetzes über den Schutz der persönlichen Freiheit oder die Überwachung von Nachrichten gemäß § 135 StPO, also die Überwachung von Gesprächsinhalten, unter geringeren Anforderungen zulässig als der Zugriff auf Vorratsdaten. Und schließlich könnte es die Strafverfolgung in ein Dilemma bringen, wenn eine Auskunft über Verkehrsdaten ab dem Moment nur mehr bei Verbrechen – und nicht bei sonstigen, „niederschwelligeren" Straftaten – zulässig wäre, ab dem diese nicht mehr für Verrechnungszwecke benötigt werden und zu Vorratsdaten werden.

Dennoch scheint die Festlegung auf den Verbrechensbegriff des § 17 StGB zur Definition einer „schweren Straftat" im Sinne der Richtlinie aus grundrechtlichen Erwägungen heraus geboten: Da die Verwendung von Vorratsdaten einen über die traditionelle Überwachung hinausgehenden Grundrechtseingriff darstellt, ist damit auch aus dem bisherigen System heraus zwingend, dass für diese neue Maßnahme keine niedrigere Eingriffsschwelle möglich ist. Bedenkt man auch die Zielsetzung der Richtlinie einerseits und die Reichweite des Grundrechtseingriffs andererseits, so erscheint das Verständnis der schweren Straftat als Verbrechen iSd § 17 StGB als adäquate, verhältnismäßige Auslegung. Auch wenn die Strafdrohung als Schwelle damit nicht mit Art. 2 Abs. 2 des Rahmenbeschlusses zum Europäischen Haftbefehl identisch ist, so können diese Taten im Sinne der Gemeinsamen Erklärung ebenso angemessene Berücksichtigung finden wie Straftaten, die unter dem Einsatz von Telekommunikationsmitteln begangen werden, vorausgesetzt, sie haben den im österreichischen Wertesystem traditionell erforderlichen Störwert, der sie zum Verbrechen macht. Das ist allerdings aufgrund der zumeist vorgesehenen Erfolgs- und Handlungsqualifikationen häufig der Fall. Und schließlich können auch Vergehen im Sinne des § 17 StGB weiterhin unter Zuhilfenahme von Verkehrsdaten ermittelt und verfolgt werden, soweit diese Daten – so wie bisher auch – für betriebsnotwendige-, insbesondere Verrechungszwecke mindestens drei Monate bei den Telekommunikationsbetreibern gespeichert sind, bevor sie zu löschen sind, und den Strafverfolgungsbehörden in diesem Zeitraum für Auskünfte zur Verfügung stehen. Jedenfalls im Bereich der Telefonrufdaten würde sich damit zur bisherigen Situation praktisch nichts ändern. In Bezug auf IP-Adressen muss hier festgehalten werden, dass nicht wenige Anbieter von Internet-Zugangsdiensten in den letzten Jahren auf Druck der Justiz diese Daten länger aufbewahrt haben, als sie diese für Zwecke der Störungsbehebung oder sonstige betrieblich notwendige Zwecke benötigt hätten, damit ohne ausdrückliche rechtliche

[42] Ähnlich *Otto/Seitlinger*, Die „Spitzel"Richtlinie – Zur (Umsetzungs)Problematik der Data Retention Richtlinie 2006/24/EG, MR 2006, 227, die als Kriterium für die schwere Straftat entweder eine deutlich höhere Strafdrohung als die Verbrechensschwelle fordern oder auch eine taxative Aufzählung der Delikte für möglich halten.

Grundlage. Diese Daten werden künftig nach einigen Tagen (je nach System des Betreibers) ausschließlich als Vorratsdaten vorhanden sein, sodass nach dem vorgeschlagenen TKG-Entwurf für den Bereich der „niederschwelligeren“ Straftaten in Bezug auf IP-Adressen tatsächlich weniger Daten zur Verfügen stünden als nach der bisherigen grundrechtswidrigen und insbesondere datenschutzrechtswidrigen Praxis.

Im Übrigen empfiehlt sich aber für allfällige weitere gesetzgeberische Schritte die Erhebung, in welchen Verfahren die Möglichkeit, auf Vorratsdaten zuzugreifen, in der Praxis tatsächlich genützt wird. Im Idealfall sollte auch eine Auswertung über den Nutzen der Erhebung durchgeführt werden. Ein erster Schritt zur Sammlung der für solche Evaluierungen notwendigen Daten könnte die Erfassung der Maßnahme in den jeweiligen Endverfügungen zu den Verfahren sein.

b) Sicherheitspolizeigesetz (SPG) und Datenschutzgesetz 2000 (DSG 2000)

Ähnlich wie zur StPO unter a) ausgeführt, erfordert die vorgeschlagene TKG-Novelle jedenfalls deshalb eine Anpassung des SPG, weil nach der neuen Bestimmung des § 99 Abs. 5 TKG der „Auskunft über Verkehrsdaten und zur Auskunft über Stammdaten, wenn hierfür die Verarbeitung von Verkehrsdaten erforderlich ist, sowie zur Auskunft über Standortdaten an nach dem SPG zuständige Sicherheitsbehörden“ eine gesetzliche Bestimmung zugrunde liegen muss, die „auf diesen Absatz zu verweisen, die konkreten Datenkategorien aufzuzählen, die berechtigten Behörden zu benennen und den Datenumfang auf das notwendige und verhältnismäßige Ausmaß zu beschränken“ hat. Außerdem darf gemäß der neuen Bestimmung § 102b TKG „eine Auskunft über Vorratsdaten (…) nur nach Maßgabe einer ausdrücklich auf § 102a verweisenden gesetzlichen Bestimmung“ erteilt werden. Die gemäß § 102b TKG grundsätzlich nur „zum Zweck der Ermittlung, Feststellung und Verfolgung schwerer Straftaten an die nach den Bestimmungen der StPO (…) zuständigen Behörden“ zulässige Auskunft über Vorratsdaten ist nur deshalb auch für den Anwendungsbereich des SPG relevant, weil § 99 Abs. 5 Z 2 eine eng determinierte Ausnahme für Standortdaten, nämlich einen Zugriff auf gemäß § 102a Abs. 3 Z 6 lit d) gespeicherte Vorratsdaten vorsieht. Dadurch ist aber zumindest ein insofern „formeller“ Verweis auf die genannten Bestimmungen des TKG im SPG perpetuiert, als ansonsten die in diesem Fall notwendige Verarbeitung von Verkehrsdaten zur Auskunft über Standortdaten nicht zulässig ist. Darüber hinaus scheint im Hinblick auf die Zulässigkeit der Verwendung von Verkehrsdaten ein Anpassungsbedarf des SPG aus nachfolgenden Erwägungen indiziert:

Mit den durch die Novelle BGBl Nr. I 114/2007 neu geschaffene Bestimmungen des SPG werden die Sicherheitsbehörden im Rahmen der Sicherheitspolizei unter näher bestimmten Voraussetzungen zum Zweck der Abwehr von Gefahren unter anderem ermächtigt, von Betreibern öffentlicher Telekommunikationsdienste näher bestimmte personenbezogene Auskünfte über Stamm-, Verkehrs- und Standortdaten zu verlangen und zu verarbeiten, oh-

ne dass die Betroffenen im Nachhinein – nachdem der Zweck der Datenanwendung weggefallen ist – von den Sicherheitsbehörden über die Datenverwendung informiert werden.

Im Hinblick auf die im Entwurf vorgeschlagene Ermächtigung von Sicherheitsbehörden, unter bestimmten Voraussetzungen auch auf Vorrat gespeicherte Standortdaten beauskunften zu lassen (siehe den vorgeschlagenen § 99 Abs. 5 Z. 2 TKG), stellt sich angesichts des Umstands, dass die davon betroffenen Personen über die Datenverwendung auch im Nachhinein nicht informiert werden, ein grundrechtliches und rechtsstaatliches Problem. Dieses Problem ist auch in allen Fällen evident, in denen die Sicherheitsbehörden gemäß § 53 SPG von Betreibern öffentlicher Telekommunikationsdienste zwar personenbezogene Auskünfte verlangen können, die davon Betroffenen aber nicht einmal nach Erreichen oder Wegfall des Zwecks der Maßnahme über diese informiert werden, um allenfalls in einem Verfahren vor der DSK überprüfen lassen zu können, ob die Datenabfrage gesetzeskonform gewesen ist oder nicht. Dies wirft erhebliche Bedenken im Hinblick auf Art. 8 EMRK und das Recht auf eine wirksame Beschwerdemöglichkeit vor einer nationalen Instanz im Sinne des Art. 13 EMRK auf.[43]

Grundsätzlich haben Auftraggeber einer Datenanwendung (und hier fungieren die Sicherheitsbehörden als solche) aus Anlass der Ermittlung von Daten die Betroffenen gemäß § 24 DSG 2000 (der nach § 51 Abs 2 SPG subsidiär anzuwenden ist) in geeigneter Weise über den Zweck der Datenverwendung sowie den Namen und die Adresse des Auftraggebers zu informieren. Nur stellt sich das Problem, dass § 24 DSG im vorliegenden Zusammenhang nicht zur Anwendung kommt. Werden nämlich Daten durch Übermittlung von Daten aus Anwendungen anderer Auftraggeber (hier: die Betreiber von Telekommunikationsdiensten) ermittelt, darf die Information gemäß § 24 DSG 2000 entfallen, wenn die Datenanwendung durch Gesetz oder Verordnung vorgesehen ist. Dies wird in der Praxis auch so gehandhabt.[44]

Eine Reparatur des § 24 DSG 200 könnte derart erfolgen, dass einerseits die Informationspflicht nicht nur aus Anlass der „Ermittlung“, sondern auch der „Übermittlung“ von Daten vorgeschrieben wird. Andererseits könnte geregelt werden, dass die Information eines Betroffenen dann, wenn ansonsten der Zweck der Datenanwendung (zB Gefahrenabwehr) gefährdet wäre, erst nach Erreichen oder Wegfall des Zwecks erfolgen kann. Schließlich sollte jedenfalls der in § 24 Abs. 4 DSG 2000 pauschal normierte Entfall der Informationspflicht bei Datenanwendungen gemäß § 17 Abs. 3 DSG 2000 aufgehoben oder zumindest materiell eingeschränkt werden. Damit würde die Informationspflicht, die in § 99 Abs. 5 Z 2 TKG vorgeschlagen wird, sachgerecht bei den Sicherheitsbehörden liegen und müsste nicht im TKG substituiert werden, um eine grundrechtskonforme Rechtslage zu schaffen.

[43] Siehe zu diesem Thema ausführlich *Tretter*, Grundrechtliche Probleme der Anwendung personenbezogener Daten durch Sicherheitsbehörden, in: *ÖJK*, Alles unter Kontrolle, Überwachung – Privatsphäre – Datenschutz, 2009, 55 ff.; *Feiler* und *Raschhofer* in *Zankl* (Hg.), Auf dem Weg zum Überwachungsstaat ? – Neue Überwachungsmaßnahmen im Bereich der Informations- und Kommunikationstechnologie, 2009, 43 ff und 91 ff.

[44] Bestätigt vom BM.I durch die Beantwortung der Parlamentarischen Anfrage 4148/AB vom 23. Juni 2008 zu 4130/J, XXIII. GP.-NR.

4. Auswirkungen auf die Beschäftigung und den Wirtschaftsstandort Österreich

Für die von der Speicherungspflicht für Verkehrsdaten betroffenen Unternehmen entsteht durch die Erfüllung der in § 102a TKG vorgesehenen Speicherungspflichten zusätzlicher Aufwand.
Abhängig von der jeweiligen Größe des betroffenen Unternehmens und dessen bisheriger Handhabung bei der Speicherung der Daten kann der Mehraufwand zwischen einigen Tausend und mehreren Hunderttausend Euro betragen. Kleine Unternehmen, die von einer Speicherpflicht durch die notwendigen Investitions- und Erhaltungskosten unverhältnismäßig stark belastet würden und die in der Praxis nur selten von Auskunftsersuchen betroffen wären, sind von der Verpflichtung zur vorrätigen Datenspeicherung ausgenommen.
Der größte Anteil an Kosten entsteht durch die neu hinzukommenden Speicherpflichten im Bereich von Internet-Zugang und E-Mail, da die zu speichernden Daten (im Gegensatz zu Telefoniedaten) bisher von den betroffenen Unternehmen nicht oder nur für kurze Zeiträume (bzgl. IP-Logdaten) zu betriebsnotwenigen Zwecken gespeichert wurden. Einer Schätzung zufolge werden aufgrund der Speicherpflicht hinsichtlich dieser Daten bei einem (fiktiven) Modell-Internetdienstanbieter (Internetzugang, E-Mail Dienst und Internet-Telefonie) mit einem Kundenstock von 500.000 Kunden Erstinvestitionskosten in der Höhe von € 275 240 im ersten Jahr sowie laufende Betriebskosten von € 118 440/Jahr entstehen. Die Kosten für die Abfrage dieser Daten werden nach dieser Schätzung weitere Erstinvestitionen in Höhe von € 131 200 sowie laufende Betriebskosten von € 347 520/Jahr erfordern.
Soweit diese Aufwendungen für die Bereitstellung von Einrichtungen und die Mitwirkung an Datenauskünften nicht im Rahmen eines Kostenersatzes (§ 94 TKG) rückerstattet werden, ist zu erwarten, dass die betroffenen Unternehmen die zusätzlichen Kosten bei ihrer Preisgestaltung einkalkulieren und - soweit der EU-weit von der Speicherungspflicht betroffene Telekommunikationsmarkt dies zulässt - an die Kunden weiter geben werden. Das Verbraucherpreisniveau im Bereich der Telekommunikationsdienstleistungen kann daher geringfügig steigen.
Darüber hinaus entstehen für die Wirtschaft, insbesondere für mittelständische Unternehmen, keine Kosten. Weitere Auswirkungen auf Einzelpreise, das allgemeine Preisniveau und insbesondere das Verbraucherpreisniveau sind damit nicht zu erwarten.

5. Finanzielle Auswirkungen

Die Inpflichtnahme von Anbietern von Kommunikationsdiensten durch den Staat im Zuge der Umsetzung der Vorratsdatenspeicherungsrichtlinie 2006/24/EG durch Einführung einer Speicherverpflichtung bezüglich Verkehrs- und Standortdaten wird in verschiedenen Bereichen zusätzliche Kosten für die Republik Österreich verursachen.
Zunächst ist den speicherpflichtigen Anbietern von Kommunikationsdiensten ein Investitionskostenersatz, dessen Höhe in einer noch zu erlassenden Verordnung festzulegen ist, zu gewähren.

Durch die künftige zusätzliche Verfügbarkeit von Internet-Zugangs- und E-Mail Daten wird die Abfragemöglichkeit für Strafverfolgungsbehörden zudem erweitert. Ein Aufwandersatz für die Beauskunftung dieser zusätzlichen, von der geltenden Überwachungskostenverordnung nicht erfassten Daten ist in noch zu bestimmender Höhe in der Überwachungskostenverordnung aufzunehmen oder in einer noch zu erlassenden Verordnung zu normieren. Diese zusätzlichen Datenabfragen werden künftig laufende Kosten in noch unbestimmter Höhe verursachen.
Die Übertragung der Vorratsdaten an die Strafverfolgungsbehörden hat auf verschlüsseltem Weg zu erfolgen, weshalb die Schaffung entsprechender Infrastruktur bei den Strafverfolgungsbehörden weitere Kosten verursachen wird.
Zusätzliche Personalressourcen auf Seiten der Strafverfolgungsbehörden sind nicht zu erwarten.
Aufgrund der seit langem sehr angespannten Personalsituation der Datenschutzkommission ist derzeit nicht sichergestellt, dass diese ihrer Kontroll- und Prüfungsfunktion im Zusammenhang mit der Speicherung und Übermittlung von Vorratsdaten auf Seiten der speicherpflichtigen Anbieter hinreichend wahrnehmen kann. Eine effiziente, wirksame Kontrolle ist jedoch im Hinblick auf den Umfang der auf Vorrat zu speichernden Daten und die damit verbundenen Begehrlichkeiten und Missbrauchgefahren unabdingbar. Aus diesem Grund sind mindestens eine zusätzliche Personalstelle sowie eine Aufstockung der finanziellen Ressourcen der Datenschutzkommission erforderlich.

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.[45] 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.[46]

[45] 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.

[46] 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

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,[47] 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.[48]

Obgleich von den zuständigen Ausschüssen des EU-Parlaments zahlreiche Änderungsanträge mit datenschutzrechtlicher Schwerpunktsetzung ausgearbeitet und in den Ausschüssen fraktionsübergreifend bestätigt worden waren, finden sich in der Richtlinie keine weiteren, über die vorgenannten Regelungen hinausgehenden datenschutzrechtlichen Bestimmungen.

iii. Zugang zu Daten

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.

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

[48] 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.

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 – wie eingangs ausgeführt – 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).[49] 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).[50]

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 Ver-

[49] 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.

[50] 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.“[50] Da weder der Rahmenbeschlussentwurf des Jahres 2004 noch der Richtlinienentwurf der Kommission eine Kontrollstelle iSd Art. 9 vorsah, ist mit gutem Grund anzunehmen, dass der eben angesprochene Änderungsantrag in Art. 9 aufgenommen wurde.

folgung 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 Schwe-

den), 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.

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.[51] Der Gesetzesentwurf 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 (siehe dazu die Ausführungen im Allgemeinen Teil der Erläuterungen). 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

[51] 61/ME XXIII. GP – Ministerialentwurf.

weitergegeben werden“.[52] Keinesfalls dürfen gemäß Art. 5 der Richtlinie Daten auf Vorrat gespeichert werden, die Aufschluss über den Inhalt einer Kommunikation geben.[53]

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[54] 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.[55] Zwar ist die 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;

[52] Siehe auch die Verweise auf Art. 7 und 8 der EU-Grundrechtecharta in Erwägungsgrund (22).
[53] Jedoch dürfen bzw. müssen Verkehrsdaten gespeichert werden, selbst wenn aus ihnen gewisse Rückschlüsse auf Kommunikationsinhalte gezogen werden können, etwa zu E-Mail Kommunikationsvorgängen.
[54] Siehe Fn 8.
[55] 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.

- 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[56] 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, 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 vorliegt. Schließlich ist auch aus der Perspektive des Rechts auf Achtung des Eigentums gemäß Art. 5 StGG und Art. 1 des 1. Zusatzprotokolls zur EMRK zu berücksichtigen, dass eine längere Speicherdauer zu erheblichen Mehrkosten führen würde, die letztlich von der öffentlichen Hand zu tragen wären, um eine Verletzung des Rechts auf Achtung des Eigentums zu vermeiden.

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).

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

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

Informationspflichten

§ 90. (1)……..

(6) Betreiber von Kommunikationsdiensten sind verpflichtet, Verwaltungsbehörden auf deren schriftliches und begründetes Verlangen Auskunft über Stammdaten im Sinne von § 92 Abs. 3 Z 3 lit. a bis e von Teilnehmern zu geben, die in Verdacht stehen, durch eine über ein öffentliches Telekommunikationsnetz gesetzte Handlung eine Verwaltungsübertretung begangen zu haben, soweit dies ohne Verarbeitung von Verkehrsdaten möglich ist.

(7) Betreiber von Kommunikationsdiensten sind auf schriftliches und begründetes Verlangen der zuständigen Gerichte, Staatsanwaltschaften oder der Kriminalpolizei (§ 76 Abs. 2 StPO) verpflichtet, diesen zur Aufklärung und Verfolgung bestimmter Straftaten Auskunft über Stammdaten (§ 92 Abs. 3 Z 3 lit. a bis e) von Teilnehmern zu geben, soweit dies ohne Verarbeitung von Verkehrsdaten möglich ist. Gleiches gilt sinngemäß für Sicherheitsbehörden nach Maßgabe des SPG, soweit sie diese Auskunft als wesentliche Voraussetzung für die Erfüllung der ihnen nach dem SPG übertragenen Aufgaben benötigen.

Erläuterungen:

Die Neueinführung dieses Absatzes 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 (systematisch nicht optimal platzierte) 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 nunmehr klaren Definition zur IP-Adresse in § 92 Abs. 3 Z 15 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.

(8) Betreiber von Mobilfunknetzen haben Aufzeichnungen über den geografischen Standort der zum Betrieb ihres Dienstes eingesetzten Funkzellen zu führen, sodass jederzeit die richtige Zuordnung einer Standortkennung (Cell-ID) zum tatsächlichen geografischen Standort unter Angabe von Geo-Koordinaten für jeden Zeitpunkt innerhalb eines sechs Monate zurückliegenden Zeitraums gewährleistet ist.

Erläuterungen:

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.

§ 92. (1)……

(3)…….

2a. "Teilnehmerkennung" jene Kennung, welche die eindeutige Zuordnung eines Kommunikationsvorgangs zu einem Teilnehmer ermöglicht;

Erläuterungen:

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.

2b. "E-Mail Adresse" die eindeutige Kennung, die einem elektronischen Postfach von einem Internet-E-Mail Anbieter zugewiesen wird;

Erläuterungen:

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.

3. "Stammdaten" alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Teilnehmer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind; dies sind:

a) Name (Familienname und Vorname bei natürlichen Personen, Name bzw. Bezeichnung bei juristischen Personen),

b) akademischer Grad bei natürlichen Personen,

c) Anschrift (Wohnadresse bei natürlichen Personen, Sitz bzw. Rechnungsadresse bei juristischen Personen),

Erläuterungen:

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.

6a. "Standortkennung" (Cell-ID) die Kennung einer Funkzelle, über welche eine Mobilfunkverbindung hergestellt wird;

Erläuterungen:

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.

6b. "Vorratsdaten" Daten, die ausschließlich aufgrund der Speicherverpflichtung gemäß § 102a gespeichert werden;

Erläuterungen:

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).

8. "Anruf" eine über einen öffentlichen Telefondienst aufgebaute Verbindung, die eine zwei- oder mehrseitige Echtzeit-Kommunikation ermöglicht;

Erläuterungen:

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.

8a. "erfolgloser Anrufversuch" einen Telefonanruf, bei dem die Verbindung erfolgreich aufgebaut wurde, der aber unbeantwortet bleibt oder bei dem das Netzwerkmanagement eingegriffen hat;

Erläuterungen:

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.

10. "elektronische Post" jede über ein öffentliches Kommunikationsnetz verschickte Text-, Sprach-, Ton- oder Bildnachricht, die im Netz oder im Endgerät des Empfängers gespeichert werden kann, bis sie von diesem abgerufen wird;

Erläuterungen:

Die Änderung beinhaltet nur die Ersetzung des Punktes durch einen Strichpunkt am Ende, weil die Aufzählung mit neuen Begriffsdefinitionen fortgesetzt wird.

11. "elektronisches Postfach" ein elektronisches Ablagesystem, das einem Teilnehmer eines E-Mail Dienstes zugeordnet ist;

Erläuterungen:

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

12. "E-Mail" elektronische Post, die über das Internet auf Basis des "Simple Mail Transfer Protocol" (SMTP) versendet wird;

Erläuterungen:

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.

13. "Internet-Telefondienst" einen öffentlichen Telefondienst im Sinne des § 3 Z 16, der auf paketvermittelter Nachrichtenübertragung über das Internet-Protokoll basiert;

Erläuterungen:

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 dringend 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).

14. "Internet-Zugangsdienst" einen Kommunikationsdienst im Sinne von § 3 Z 9, der in der Bereitstellung von Einrichtungen und/oder Diensten zur Erbringung von Zugangsleistungen zum Internet besteht;

15. "E-Maildienst" einen Kommunikationsdienst im Sinne von § 3 Z 9, welcher den Versand und die Zustellung von E-Mails auf Basis des "Simple Mail Transfer Protocol" (SMTP) umfasst;

16. "Öffentliche IP-Adresse" eine einmalige numerische Adresse aus einem Adressblock, der durch die Internet Assigned Numbers Authority (IANA) oder durch eine regionale Vergabestelle (Regional Internet Registries) einem Anbieter eines Internet-Zugangsdienstes zur Zuteilung von Adressen an seine Kunden zugewiesen wurde, die einen Rechner im Internet eindeutig identifiziert und im Internet geroutet werden kann. Öffentliche IP-Adressen sind

Zugangsdaten im Sinne des § 92 Abs. 3 Z 4a. Wenn eine konkrete öffentliche IP-Adresse einem Teilnehmer für die Dauer des Vertrages zur ausschließlichen Nutzung zugewiesen ist, handelt es sich zugleich um ein Stammdatum im Sinne des § 92 Abs. 3 Z 3.

Erläuterungen:

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.

§ 93. (1)……

(3) Das Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten sowie die Weitergabe von

Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Benutzer ist unzulässig. Dies gilt nicht für die Aufzeichnung und Rückverfolgung von Telefongesprächen im Rahmen der Entgegennahme von Notrufen und die Fälle der Fangschaltung, der Überwachung von Nachrichten und der Auskunft über Daten einer Nachrichtenübermittlung einschließlich Vorratsdaten nach den Vorschriften der StPO sowie für eine technische Speicherung, die für die Weiterleitung einer Nachricht erforderlich ist.

Erläuterungen:

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.

§ 94. (1) Der Anbieter ist nach Maßgabe der gemäß Abs. 3 und 4 erlassenen Verordnungen verpflichtet, alle Einrichtungen bereitzustellen, die zur Überwachung von Nachrichten sowie zur Auskunft über Daten einer Nachrichtenübermittlung einschließlich der Auskunft über Vorratsdaten nach den Bestimmungen der StPO erforderlich sind. Der Bundesminister für Verkehr, Innovation und Technologie hat im Einvernehmen mit dem Bundesminister für Justiz und dem Bundesminister für Finanzen durch Verordnung einen angemessenen Kostenersatz vorzusehen.

Erläuterungen:

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 stellt die positiv-rechtlich Umsetzung 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.

Da die Vorratsdatenspeicherung (zwangsläufig) nur durch die Betreiber von Kommunikationsdiensten vorgenommen werden kann, bei denen die speicherpflichtigen Daten erzeugt bzw. verarbeitet werden, wird durch die Normierung der Speicherpflicht eine Inpflichtnahme Privater durch den Staat begründet. Im konkreten Fall wird durch diese Inpflichtnahme in verfassungsrechtlich geschützte Rechtspositionen der betroffenen Anbieter, nämlich die durch Art. 5 StGG und Art. 1 1. ZProtMRK verfassungsgesetzlich normierte Eigentumsfreiheit, eingegriffen, da die Anbieter zur Erfüllung ihrer Verpflichtung erhebliche Investitionen

vornehmen müssen, die sich aus Erstinvestitions- sowie laufenden Kosten zusammensetzen.
Der Verfassungsgerichtshof hat (beginnend mit VfSlg 6884/1972; 7234/1972) im Hinblick auf derartige Eigentumseingriffe aus dem Gleichheitsgrundsatz Pflichten zur Enteignungsentschädigung abgeleitet, um das Erfordernis der Verhältnismäßigkeit bei Eigentumseinschränkung zu erfüllen. Insbesondere dürfen „auch im besonderen öffentlichen Interesse gelegene Verpflichtungen, die mit einer erheblichen Vermögensbelastung verbunden sind, […] nur auferlegt werden […], wenn dies unter Bedachtnahme auf das Prinzip der Verhältnismäßigkeit wirtschaftlich zumutbar ist" (VfSlg 13.587/1993).

Die derzeit geltende Rechtslage verpflichtet Anbieter einerseits zur Bereitstellung von Einrichtungen zur Überwachung einer Telekommunikation (soweit diese nach der StPO erforderlich sind), andererseits zur Mitwirkung im erforderlichen Ausmaß (§ 94 Abs 1 und 2 TKG 2003, BGBl I 70/2003 idgF). Dabei ist allerdings zu berücksichtigen, dass die daraus resultierenden, den Inpflichtgenommenen zugemuteten Aufwendungen verhältnismäßig sein müssen. Insbesondere ist eine wirtschaftliche Belastung der Telekommunikationsbetreiber bzw. die Bereithaltung aufwändiger Vorkehrungen nur bei Vorliegen besonderer Umstände nach Maßgabe einer Interessensabwägung gerechtfertigt: „Mag auch die Inpflichtnahme privater Betreiber von Telekommunikationsdiensten für die Überwachung des Fernmeldeverkehrs und die Bereitstellung entsprechender Einrichtungen eine sachlich gerechtfertigte und daher verfassungsmäßige Mitwirkungspflicht Privater an einer staatlichen Aufgabe darstellen, so ist dennoch auch bei der Regelung der Kostentragung der Verhältnismäßigkeitsgrundsatz zu beachten." (VfSlg 16.808)

Aufgrund der bisher vorliegenden Schätzungen und Äußerungen zu den erforderlichen Investitionskosten für die Speicherung von Daten im Rahmen der RL 2006/24/EG[57] ist davon auszugehen, dass diese jene, die für die bisherigen Kosten der Telekom-Überwachung anzusetzen waren, wesentlich übersteigen werden. Im Lichte dieses Erkenntnisses des VfGH ist daher die Festlegung eines angemessenen Kostenersatzes verfassungsrechtlich jedenfalls geboten. Daher wird anlässlich der Umsetzung der RL 2006/24/EG zur Vorratsdatenspeicherung neuerlich eine (Investitionskosten-) Verordnung zu erlassen 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.

(2) Der Betreiber ist verpflichtet, an der Überwachung von Nachrichten sowie der Auskunft über Daten einer Nachrichtenübermittlung einschließlich der Auskunft über Vorratsdaten nach den Bestimmungen der StPO im erforderlichen Ausmaß mitzuwirken. Der Bundesminister für Justiz hat im Einvernehmen mit dem Bundesminister für Verkehr, Innovation und Technologie und dem Bundesminister für Finanzen durch Verordnung einen angemessenen Kostenersatz vorzusehen. Dabei ist insbesondere auf die wirtschaftliche Zumutbarkeit des Aufwandes, auf ein allfälliges Interesse des betroffenen Unternehmers an den zu erbringenden Leistungen und auf eine allfällige durch die gebotenen technischen Möglichkeiten bewirkte Gefährdung, der durch die verlangte Mitwirkung entgegengewirkt werden soll, Bedacht zu nehmen.

Erläuterungen:

[57] Laut einer Studie der Fakultät für Informatik der Universität Wien im Auftrag der ISPA belaufen sich die Kosten pro Kunde auf ca. zwei Euro im ersten Jahr und einen Euro in den folgenden Jahren, siehe *Stampfel* ua, The EU Data Retention Directive 2006/24/EC from a Technical Perspective (2008) 81 ff; Kosten von 50 bis zu 75 Mio Euro in der BRD, http://futurezone.orf.at/stories/187376/; Die Kosten für die Vorratsdatenspeicherung belaufen sich für die Deutsche Telekom angeblich im Jahr 2008 auf zwölf Mio Euro, dazu kommen schätzungsweise jährliche Kosten in Höhe von etwa zwei Mio Euro, http://www.tagesschau.de/inland/vorratsdatenspeicherung42.html.

Die Änderung beinhaltet zunächst, dass für die Verordnung eines angemessenen Kostenersatzes kein Einvernehmen mit dem Bundesministeri 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.

(3) Durch Verordnung kann der Bundesminister für Verkehr, Innovation und Technologie im Einvernehmen mit den Bundesministern für Inneres und für Justiz dem jeweiligen Stand der Technik entsprechend die näheren Bestimmungen für die Gestaltung der technischen Einrichtungen zur Gewährleistung der Überwachung von Nachrichten nach den Bestimmungen der StPO und zum Schutz der zu übermittelnden Daten gegen die unbefugte Kenntnisnahme oder Verwendung durch Dritte festsetzen. Nach Erlass der Verordnung ist unmittelbar dem Hauptausschuss des Nationalrates zu berichten.

Erläuterungen:

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.

(4) Die Übermittlung von Verkehrsdaten, Standortdaten und Stammdaten, welche die Verarbeitung von Verkehrsdaten erfordern, einschließlich der Übermittlung von Vorratsdaten, nach den Bestimmungen der StPO sowie des SPG hat unter Verwendung einer verschlüsselten Übertragung per E-Mail und eines 'Comma-Separated Value (CSV)' - Dateiformats zu erfolgen. Durch Verordnung kann der Bundesminister für Verkehr, Innovation und Technologie im Einvernehmen mit den Bundesministern für Inneres und für Justiz die näheren Bestimmungen zur einheitlichen Definition der Syntax, der Datenfelder und der Verschlüsselung zur Übermittlung der Daten in einer technischen Richtlinie festsetzen. Nach Erlass der Verordnung ist unmittelbar dem Hauptausschuss des Nationalrates zu berichten.

Erläuterungen:

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 geringst 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. Da zugleich das Bundeskriminalamt, welches die Übermittlung der beauskunfteten Daten (auch) im Dienste der Strafjustiz besorgen kann, bereits über eine Public Key Infrastruktur für S/MIME Verschlüsselungen verfügt, stellt diese Lösung 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 Ablauf dieser Variante lässt sich grob wie folgt skizzieren:
1. Der Anbieter verschlüsselt die Vorratsdaten bei deren Entstehen mit dem Public Key des Staates.
2. Die Strafverfolgungsbehörde übermittelt ein genehmigtes Auskunftsbegehren an eine zentrale Vorratsdatenspeicherungs-Kontrollinstanz (z.B. bei der Datenschutzkommission oder dem Bundesrechenzentrum)
3. Die Vorratsdatenspeicherungs-Kontrollinstanz übermittelt das genehmigte Auskunftsbegehren an den Anbieter.
4. Der Anbieter verschlüsselt die Daten des Auskunftsbegehrens und sucht in den verschlüsselten Vorratsdaten.
5. Der Anbieter übermittelt die verschlüsselten Suchergebnisse (mit deren Qualifikation als Spaltenbeschriftung: IP-Adresse, Name, ...) an die Vorratsdatenspeicherungs-Kontrollinstanz.
6. Die Vorratsdatenspeicherungs-Kontrollinstanz entschlüsselt die Suchergebnisse mit dem Private Key und übermittelt die entschlüsselten Suchergebnisse an die Strafverfolgungsbehörde weiter.
7. Die Strafverfolgungsbehörde nutzt die Daten.
Zu bedenken ist, dass in diesem Zusammenhang noch wesentliche Fragen der Umsetzbarkeit zu untersuchen sind, nicht zuletzt weil es hierfür einer entsprechenden staatlichen Infrastruktur bedarf. Eine Einbindung der Anbieter ist zur Definition einer solchen Verschlüsselungsvariante jedenfalls unabdingbar. Der Vorteil für diese würde darin bestehen, dass ab dem Zeitpunkt der Verschlüsselung für die Anbieter haftungsträchtige Vorfälle im Hinblick auf Vorratsdaten kaum mehr möglich wären.

Jedenfalls ist der Spielraum für eine nach dieser Bestimmung zu erlassenden Verordnung 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 Puklic 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 staatliche 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 dem Staat 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. Die dem Staat dadurch faktisch eröffnete Möglichkeit, diese Daten durch sogenanntes „Data-Mining“[58] mit anderen Informationen automatisiert zu verknüpfen, könnte nur allzu verlockend sein: Auch wenn gegenwärtig solche Verknüpfungen nach dem strengen datenschutzrechtlichen Zweckbindungsgrundsatz (Art 6 Abs 1 lit b DatenschutzRL 95/46/EG bzw. § 6 Abs 1 Z 2 DSG 2000) unzulässig sind, besteht doch die Gefahr, dass allein das Vorhandensein solcher Datenbestände künftig Begehrlichkeiten weckt und damit allmählich in Vergessenheit gerät, dass die Sammlung dieser Daten nur zum Zweck der Ermittlung, Aufklärung und Verfolgung schwerer Straftaten zugelassen wird. Selbst innerhalb dieses Zwecks ist zu bedenken, dass (automatisierte) Abgleiche mit anderen Datenbeständen letztlich eine Rasterfahndung mit elektronischen Mitteln bedeuten. Allein die abstrakte Möglichkeit würde die Intensität des durch die Speicherung ohnehin gegebenen Eingriffs in Art 8 EMRK um ein Vielfaches erhöhen. Auch wenn solche Mittel teilweise nützlich erscheinen mögen, so ist ihre Notwendigkeit und Verhältnismäßigkeit stark zu bezweifeln. Eine dezentrale Speicherung der Vorratsdaten bei den Anbietern bietet insofern einen effektiven Schutz vor einer ausufernden Verwendung der vorrätig gesammelten Datenmengen. Dass die Daten über verschiedene Anbieter „verstreut“ sind und nur mit deren Mitwirkung dem Staat zur Verfügung stehen, bedeutet eine nicht unwesentliche Hemmschwelle.

Weil die in dieser Bestimmung festgelegten technischen Definitionen von den Anbietern in ihren Systemen umzusetzen sind, sollten die Unternehmen und die Interessenvertretungen der Telekom- und IT-Branche bereits in den Prozess der Ausarbeitung der technischen Richtlinie eingebunden sein, um möglichst effiziente Strukturen festzulegen und damit dem Gebot einer sparsamen Verwaltung gerecht zu werden. Hierzu eignet sich am besten das bereits etablierte Gremium des AK-TK (Arbeitskreis für technische Koordination für Kommunikationsnetze und –dienste), das sich in der Vergangenheit bei der Ausarbeitung der Überwachungsverordnung (ÜVO)bereits als nützlich erwiesen hat.

§ 97. (1) Stammdaten dürfen unbeschadet der §§ 90 Abs. 6 und 7 sowie 96 Abs. 1 und 2 von Betreibern nur für folgende Zwecke ermittelt und verwendet werden:

Erläuterungen:

Damit wird bei gleichzeitiger Einführung des neuen § 90 Abs. 7 die Informationspflicht an die Gerichte im Hinblick auf Teilnehmerverzeichnisse (§ 103 Abs. 4) obsolet.

§ 98. (1) Betreiber haben Betreibern von Notrufdiensten auf deren Verlangen Auskünfte über Stammdaten im Sinne von § 92 Abs. 3 Z 3 lit. a bis d sowie über Standortdaten im Sinne des § 92 Abs. 3 Z 6 zu erteilen. In beiden Fällen ist Voraussetzung für die Zulässigkeit der Übermittlung ein Notfall, der nur durch Bekanntgabe dieser Informationen abgewehrt werden

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

kann. Die Notwendigkeit der Informationsübermittlung ist vom Betreiber des Notrufdienstes zu dokumentieren und dem Betreiber unverzüglich, spätestens jedoch innerhalb von 24 Stunden nachzureichen. Der Betreiber darf die Übermittlung nicht von der vorherigen Darlegung der Notwendigkeit abhängig machen. Den Betreiber des Notrufdienstes trifft die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens.

Erläuterungen:

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

(2) (Verfassungsbestimmung) Ist eine aktuelle Standortfeststellung nicht möglich, darf ausnahmsweise die Standortkennung (Cell-ID) zum letzten Kommunikationsvorgang der Endeinrichtung des gefährdeten Menschen verarbeitet werden, obwohl hierfür ein Zugriff auf gemäß § 102a Abs. 3 Z 6 lit d) gespeicherte Vorratsdaten erforderlich ist. Der Anbieter hat den betroffenen Teilnehmer über eine Auskunft über Standortdaten nach dieser Ziffer spätestens mit Ablauf der Rechnungsperiode zu informieren.

Erläuterungen:

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 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.

§ 99. (1) Verkehrsdaten dürfen außer in den in diesem Gesetz geregelten Fällen weder gespeichert noch verwendet werden und sind vom Betreiber nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren.

Erläuterungen:

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.

(4) Dem Betreiber ist es außer in den in diesem Gesetz besonders geregelten Fällen untersagt, einen Teilnehmeranschluss über die Zwecke der Verrechnung hinaus nach den von diesem Anschluss aus angerufenen Teilnehmernummern auszuwerten. Mit Zustimmung des Teilnehmers darf der Betreiber die Daten zur Vermarktung für Zwecke der eigenen Telekommunikationsdienste oder für die Bereitstellung von Diensten mit Zusatznutzen verwenden.

(5) Eine Verarbeitung von Verkehrsdaten zu Auskunftszwecken ist nur zulässig

1. zur Auskunft über Daten einer Nachrichtenübermittlung (§ 134 StPO) an die nach der StPO zur Ermittlung, Feststellung und Verfolgung von Straftaten zuständigen Behörden, wenn eine gerichtliche Bewilligung vorliegt;

Erläuterungen:

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.

Die Schwierigkeit dabei ist allerdings, dass hier Unklarheiten bestehen bleiben, welche Anbieter welche Daten wie lange für Betriebszwecke haben (dürfen). Der tatsächliche Nutzen dieser Bestimmung hängt zugleich davon ab, inwieweit durch Änderungen in der StPO korrespondierende Bestimmungen geschaffen werden, welche für die "Auskunft über Daten einer Nachrichtenübermittlung" eine Differenzierung je nach Schwere der Straftat beinhalten. Darüber hinaus ist fraglich, ob diese Bestimmung nicht zu einer Aufweichung eines restriktiven Umgangs mit Datenauskünften führt, zumal sich die zu Betriebszwecken vorhandenen Daten zum Teil mit den Vorratsdaten decken. Andererseits bringt dies den Vorteil, dass da-

mit nicht der Begriff der "schweren Straftat" nach unten nivelliert werden muss, nur um die Auskunftsansprüche nach der StPO an die Zweckbindung anzupassen.

2. (Verfassungsbestimmung) zur Auskunft über Verkehrsdaten und zur Auskunft über Stammdaten, wenn hierfür die Verarbeitung von Verkehrsdaten erforderlich ist, sowie zur Auskunft über Standortdaten an nach dem SPG zuständige Sicherheitsbehörden, wenn diese Auskunft als wesentliche Voraussetzung zur Abwehr einer konkreten Gefahr für das Leben oder die Gesundheit eines Menschen notwendig ist. Ist eine aktuelle Standortfeststellung nicht möglich, darf ausnahmsweise die Standortkennung (Cell-ID) zum letzten Kommunikationsvorgang der Endeinrichtung des gefährdeten Menschen verarbeitet werden, obwohl hierfür ein Zugriff auf gemäß § 102a Abs. 3 Z 6 lit d) gespeicherte Vorratsdaten erforderlich ist. Der Anbieter hat den betroffenen Teilnehmer über eine Auskunft über Standortdaten nach dieser Ziffer spätestens mit Ablauf der Rechnungsperiode zu informieren.

In beiden Fällen hat die gesetzliche Auskunftsermächtigung ausdrücklich auf diesen Absatz zu verweisen, die konkreten Datenkategorien aufzuzählen, die berechtigten Behörden zu benennen und den Datenumfang auf das notwendige und verhältnismäßige Ausmaß zu beschränken. Eine Verpflichtung zur Speicherung von Verkehrsdaten allein aufgrund dieses Absatzes besteht nicht. Eine über die genannte Ausnahme hinausgehende Verarbeitung von Vorratsdaten aufgrund dieses Absatzes ist unzulässig. Auf Auskünfte nach diesem Absatz ist eine gemäß § 94 Abs. 2 erlassene Verordnung zur Kostenerstattung anzuwenden.

Erläuterungen:

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[59], darf eine Auskunft über Verkehrsdaten ausschließlich aufgrund einer richterlichen Genehmigung erfolgen. 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

[59] 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);

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[60]. 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.

[60] 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.

Weil es sich im Anwendungsbereich des SPG gerade um den "eigenen Wirkungsbereich" der Sicherheitsbehörden handelt und gerade keine Handlung im Dienste der Strafjustiz vorliegt, müsste für die Befassung eines Gerichts für eine solche Bewilligung, allenfalls nach den Regeln der "Gefahr im Verzug", eine gerichtliche Zuständigkeit samt Verfahren geschaffen werden. Dem würde jedoch das gewaltenteilende Verfassungsprinzip, konkret Art. 94 B-VG, entgegenstehen, da zwischen Verwaltungsbehörden und Gerichten eine Trennung in allen Instanzen einzuhalten ist. Weil es sich dabei um einen Verfassungsgrundsatz im Sinne des Art. 44 Abs. 3 B-VG handelt, dürfte eine solche Regelung streng genommen (ohne Volksabstimmung) nicht einmal im Verfassungsrang getroffen werden.

Eine Alternative hierzu stellt eine Genehmigung durch den Rechtsschutzbeauftragten des Innenministeriums (§ 91a SPG) dar, die dem zur Auskunft verpflichteten Anbieter unverzüglich vorzulegen wäre. Eine derartige Bestimmung wäre jedoch aus o.g. verfassungsrechtlichen Gründen im Verfassungsrang zu beschließen ist, da der Rechtsschutzbeauftragte nicht über jene Unabhängigkeitsgarantien verfügt, welche das Richteramt auszeichnen. Eine entsprechende Regelung wäre im Rahmen des SPG zu treffen.

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 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 nur „aus Anlass der Ermittlung von Daten“ vorsieht. Der durch die Standortfeststellung zugelassene Eingriff in das Grundrecht auf Datenschutz liegt aber gerade nicht in der Ermittlung sondern in der Übermittlung von Daten. Sachgerecht wäre daher, dass eine Information durch die Sicherheitsbehörden erfolgt, aus deren Sicht sehr wohl eine „Ermittlung“ von Daten vorliegt. Diese trifft aber - wie im Vorblatt unter 3 b) ausgeführt - aufgrund einer Ausnahme keine Informationspflicht. Werden nämlich Daten aus Anwendungen anderer Auftraggeber (aus der Perspektive der Sicherheitsbehörden hier: der Betreiber von Telekommunikationsdiensten) ermittelt, darf die Information gemäß § 24 DSG 2000 entfallen, wenn die Datenanwendung wie hier durch Gesetz oder Verordnung vorgesehen ist. Für den Anbieter würde diese Ausnahme nicht greifen, da aus dessen Perspektive keine Datenanwendung eines anderen Auftraggebers vorliegt, sondern seine eigene. 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 muss. Damit ist 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 datenschutzrechtlich und grundrechtlich äußerst bedenkliche Rechtslage wird deshalb für die gegenständlichen Fälle beseitigt, indem die Informationspflicht des Anbieters im TKG 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, was bei Bestehen einer Informationspflicht nach DSG 2000 eine Ausnahme gemäß § 24 Abs. 4 iVm § 17 Abs. 3 DSG 2000 begründen 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.

Die Ausdehnung des Kostenerstattungsanspruchs auf Anfragen nach dem SPG ist einerseits sachlich geboten, weil es für den Aufwand der Anbieter keinen Unterschied macht, ob die Anfrage nach der StPO oder nach SPG gestellt wird. Außerdem soll damit verhindert wer-

den, dass Anfragen, die richtigerweise nach der StPO zu stellen sind, nur aus Gründen der Kostenersparnis nach dem SPG gestellt werden.

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

§ 102. (1)…….

(3) Die Verarbeitung anderer Standortdaten als Verkehrsdaten gemäß Abs. 1 und 2 muss auf das für die Bereitstellung des Dienstes mit Zusatznutzen erforderliche Maß sowie auf Personen beschränkt werden, die im Auftrag des Betreibers oder des Dritten, der den Dienst mit Zusatznutzen anbietet, handeln. Unbeschadet des § 93 Abs. 3 ist die Ermittlung und Verwendung von Standortdaten, die nicht im Zusammenhang mit einem Kommunikationsvorgang stehen, zu Auskunftszwecken jedenfalls unzulässig.

Erläuterungen:

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.

Der letzte Satz wird zur ausdrücklichen Klarstellung eingeführt, dass kommunikationsunabhängige Standortdaten (und damit die Möglichkeit, Bewegungsprofile zu erstellen) auch durch die Einführung der Vorratsdatenspeicherung keinesfalls zulässig sind. Bei begleitenden Rufdaten (sog. S-Records) zu einer Telefonüberwachung müssen auch sog. Location Updates übermittelt werden. Allerdings stehen auch solche Standortdaten mit einem Kommunikationsvorgang, nämlich mit dem Überwachten, in Zusammenhang.

Vorratsdaten

§ 102a. (1) Über die Berechtigung zur Speicherung oder Verarbeitung gemäß den §§ 96, 97, 99, 101 und 102 hinaus haben Anbieter von öffentlichen Kommunikationsdiensten nach Maßgabe der Abs. 2 bis 4 Daten ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation zu speichern. Die Speicherung erfolgt ausschließlich zum Zweck der Ermittlung, Feststellung und Verfolgung schwerer Straftaten.

Erläuterungen:

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. Zudem sind Alternativen zu einer derartigen verdachtsunabhängigen obligatorischen Speicherung in Betracht zu ziehen. Dies gilt insbesondere für das sog. Quick Freeze - Verfahren, das in den USA eingesetzt wird und im Vergleich zur Vorratsdatenspeicherung ein gelinderes Mittel darstellen würde: Eine generelle Sammlung aller Daten findet bei diesem Verfahren nicht statt, die Strafverfolgungsbehörden können jedoch im Verdachtsfall eine Speicheranordnung hinsichtlich jener Daten erlassen, die beim Anbieter (insbesondere für Abrechnungszwecke) vorhanden sind, womit deren routinemäßige Löschung unterbunden und auch ein späterer Zugriff auf diese Daten ermöglicht wird.
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[61] 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[62] ergab zudem, dass unter Berücksichtigung der Notwendigkeit und Relevanz von Verkehrsdaten in verschiedenen Deliktsbereichen die gewünschte Speicherdauer sechs Monate beträgt.
Auch eine Erhebung der Europäischen Kommission[63] 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[64], dass sich der überwiegende Anteil der Verkehrsdatenabfragen entweder auf einen Erhebungszeitraum von einem Tag oder von drei Monaten bezieht;[65] Dieser beginnt durchschnittlich 26 Tage vor dem Zeitpunkt der

[61] 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).
[62] 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).
[63] 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).
[64] 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.
[65] 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).

Anfrage, wobei etwa die Hälfte der Abfragen einen Zeitraum von lediglich vier Tagen oder weniger vor dem Anfragezeitraum betrifft[66].
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[67].
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.

(2) Anbietern von Internet-Zugangsdiensten obliegt die Speicherung folgender Daten:

1. Name, Anschrift und Teilnehmerkennung des Teilnehmers, dem eine öffentliche IP-Adresse zu einem bestimmten Zeitpunkt unter Angabe der zugrundeliegenden Zeitzone zugewiesen war;

Erläuterungen:

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.

2. Datum und Uhrzeit der Zuteilung und des Entzugs einer öffentlichen IP-Adresse bei einem Internet-Zugangsdienst unter Angabe der zugrundeliegenden Zeitzone;

Erläuterungen:

[66] A.a.O. S. 114.
[67] 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.

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 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.

3. die Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluss;

Erläuterungen:

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

4. die eindeutige Kennung des Anschlusses, über den der bestimmte Internet-Zugang erfolgt ist.

Erläuterungen:

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).

(3) Anbietern öffentlicher Telefondienste einschließlich Internet-Telefondiensten obliegt die Speicherung folgender Daten:

1. Teilnehmernummer oder andere Kennung des anrufenden und des angerufenen Anschlusses;

Erläuterungen:

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.

2. bei Zusatzdiensten wie Rufweiterleitung oder Rufumleitung die Teilnehmernummer, an die der Anruf geleitet wird;

3. Name und Anschrift des anrufenden und des angerufenen Teilnehmers;

Erläuterungen:

Auch für VoIP-Telefonie ist der Teilnehmer eindeutig definiert.

4. Datum, Uhrzeit des Beginns und Dauer eines Kommunikationsvorganges unter Angabe der zugrundeliegenden Zeitzone;

Erläuterungen:

Beginn und Dauer entsprechen dem Regelfall der heutigen Aufzeichnungspraxis.

5. die Art des in Anspruch genommenen Dienstes (Anrufe, Zusatzdienste und Mitteilungs- und Multimediadienste).

Erläuterungen:

"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.

6. Betreibern von Mobilfunknetzen obliegt zudem die Speicherung

Erläuterungen:

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.

a) der internationalen Mobilteilnehmerkennung (IMSI) des anrufenden und des angerufenen Anschlusses;

b) der internationalen Mobilfunkgerätekennung (IMEI) des anrufenden und des angerufenen Anschlusses;

Erläuterungen:

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 Teil-

nehmer anderer Anbieter werden diese Daten nicht verarbeitet und daher auch nur beim jeweiligen anderen Anbieter gespeichert.

Anzumerken ist, dass derartige Abfragen auch aus grundrechtlicher Sicht bedenklich sind. Neben IMEI, IMSI und Standortdaten zur überwachten Rufnummer müssen diese Daten auch von nicht in der Anordnung definierten Teilnehmern, die die überwachte Rufnummer aktiv oder passiv kontaktiert haben, beauskunftet werden. In diesen Fällen ist nämlich nicht von vornherein bestimmt, auf wen sich der Grundrechtseingriff bezieht. Damit ist aber eine Beurteilung, ob der Grundrechtseingriff auch im Einzelfall bezüglich der weiteren Teilnehmer verhältnismäßig ist, oft nicht möglich. Es sollte daher für den Fall einer Beauskunftung bereits in der gerichtlichen Anordnung klargestellt werden, dass die IMEI und IMSI sowie die Standortkennung (Cell-ID) ausschließlich für die durch gerichtliche Anordnung exakt definierte Teilnehmerkennung (= zu überwachende Teilnehmernummer) in Fällen von aktiven und passiven Verbindungen beauskunftet werden müssen. Wenn diese Daten zu kontaktierten Teilnehmern beauskunftet werden sollen, so können die Daten zu diesen Teilnehmern nur mit gesonderten Anordnung erhoben werden, die jeweils an den Anbieter zu richten sind, in dessen Netz die Daten als Vorratsdaten vorliegen.

c) Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Kennung des Standortes (Cell-ID), an dem der Dienst aktiviert wurde, wenn es sich um vorbezahlte anonyme Dienste handelt;

Erläuterungen:

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.

d) der Standortkennung (Cell-ID) bei Beginn einer Verbindung.

Erläuterungen:

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

(4) Anbietern von E-Mail Diensten obliegt die Speicherung folgender Daten:

1. die einem Teilnehmer zugewiesene Teilnehmerkennung;

2. Name und Anschrift des Teilnehmers, dem eine E-Mail Adresse zu einem bestimmten Zeitpunkt zugewiesen war;

Erläuterungen:

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 dyna-

mische 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. Eine Umstellung der E-Mail Serversysteme, um die Zuordnung einer Absender E-Mail Adresse zu einem Teilnehmer zu einem bestimmten Zeitpunkt auch in diesen Fällen zu ermöglichen, wäre nur mit unverhältnismäßig hohem technischem Aufwand möglich.

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.

3. bei Versenden einer E-Mail die E-Mail Adresse und die öffentliche IP-Adresse des Absenders sowie die E-Mail Adresse jedes Empfängers der E-Mail;

Erläuterungen:

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.

4. beim Empfang einer E-Mail und deren Zustellung in ein elektronisches Postfach die E-Mail Adresse des Absenders und des Empfängers der Nachricht sowie die öffentliche IP-Adresse der letztübermittelnden Kommunikationsnetzeinrichtung;

Erläuterungen:

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.

5. bei An- und Abmeldung beim E-Mail Dienst Datum, Uhrzeit, Teilnehmerkennung und öffentliche IP-Adresse des Teilnehmers unter Angabe der zugrundeliegenden Zeitzone;

Erläuterungen:

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.

Weiters treten bei POP und IMAP durch vom Teilnehmer oder Anbieter festgelegte Automatismen sehr häufig Verbindungen auf (z.B. im Minutentakt), die zwar einen maschinellen Zugriff auf das elektronische Postfach festhalten, aber über das tatsächliche Downloaden oder Lesen von E-Mails durch den Teilnehmer keine Auskunft geben, wodurch einerseits vorratsdatenseitig sehr große Datenmengen entstehen, anderseits durch die de-facto-Permanenzverbindung keine sinnvolle Zeiteinschränkung der Dienstverwendung des Teilnehmers möglich ist. Das Loggen solcher Verbindungen stellt einen hohen technischen Aufwand dar, der eine große Datenmenge zur Folge hat, die gleichzeitig für die Strafverfolgung (wenn überhaupt) nur von äußerst geringem Nutzen ist. Zur Wahrung eines angemessenen Verhältnisses zwischen Aufwand und Nutzen sollte diesbezüglich bei der praktischen Umsetzung der Speicherung eine Lösung gefunden werden, welche diesem Problem gerecht wird.

(5) Die Speicherpflicht nach Abs. 1 besteht nur für jene Daten gemäß Abs. 2 bis 4, die im Zuge der Bereitstellung der betreffenden Kommunikationsdienste erzeugt oder verarbeitet werden. Im Zusammenhang mit erfolglosen Anrufversuchen besteht die Speicherpflicht nach Abs. 1 nur, soweit diese Daten im Zuge der Bereitstellung des betreffenden Kommunikationsdienstes erzeugt oder verarbeitet und gespeichert oder protokolliert werden.

Erläuterungen:

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.

(6) Die Speicherpflicht nach Abs. 1 besteht nicht für solche Anbieter, deren Unternehmen als kleines Unternehmen oder als Kleinstunternehmen gemäß der Empfehlung der Europäischen Kommission 2003/361/EG einzustufen ist. Eine solche Befreiung von der Speicherverpflichtung hat der Bundesminister für Verkehr, Innovation und Technologie auf Antrag mit Bescheid auszusprechen. Der Anbieter hat alle für die Einstufung erforderlichen Daten zu bescheinigen. Gegen diesen Bescheid ist kein ordentliches Rechtsmittel zulässig. Der Anbieter hat dem Bundesminister für Verkehr, Innovation und Technologie anzuzeigen, wenn die zur Einstufung wesentlichen Schwellenwerte überschritten werden.

Erläuterungen:

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 not-

wendigen 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.

(7) Der Inhalt der Kommunikation und insbesondere Daten über im Internet aufgerufene Adressen dürfen auf Grund dieser Vorschrift nicht gespeichert werden.

Erläuterungen:

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.

(8) Die nach Abs. 1 zu speichernden Daten sind nach Ablauf der Speicherfrist unbeschadet des § 99 Abs. 2 unverzüglich, spätestens jedoch einen Monat nach Ablauf der Speicherfrist, zu löschen.

Erläuterungen:

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.

(9) Im Hinblick auf Vorratsdaten gilt der jeweilige Anbieter, der die Daten den vorstehenden Absätzen entsprechend zu speichern hat, als Auftraggeber des öffentlichen Bereichs gemäß § 4 Z 4 in Verbindung mit § 5 Abs. 2 Z 2 DSG 2000. Im Hinblick auf Vorratsdaten, die gemäß § 102b übermittelt werden, richten sich die Ansprüche auf Information oder Auskunft über diese Datenverwendung ausschließlich nach den Bestimmungen der StPO.

Erläuterungen:

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.

Auskunft über Vorratsdaten

§ 102b. (1) Eine Auskunft über Vorratsdaten darf ausschließlich aufgrund einer gerichtlichen Bewilligung und nur nach Maßgabe einer ausdrücklich auf § 102a verweisenden gesetzlichen Bestimmung erteilt werden. Die Auskunft ist nur zum Zweck der Ermittlung, Feststellung und Verfolgung schwerer Straftaten an die nach den Bestimmungen der StPO über die Auskunft über Daten einer Nachrichtenübermittlung zuständigen Behörden zulässig.

(2) Die nach § 102a zu speichernden Daten sind so zu speichern, dass sie unverzüglich an die nach den Bestimmungen der StPO und nach dem dort vorgesehenen Verfahren für die Erteilung einer Auskunft über Daten einer Nachrichtenübermittlung zuständigen Behörden übermittelt werden können.

Erläuterungen:

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.

(3) Die Übermittlung der Daten hat in angemessen geschützter Form nach Maßgabe des § 94 Abs. 4 zu erfolgen.

Datensicherheit und Protokollierung

§ 102c. (1) Die Speicherung der Vorratsdaten hat so zu erfolgen, dass eine Unterscheidung von nach Maßgabe der §§ 96, 97, 99, 101 und 102 gespeicherten Daten möglich ist. Die Daten sind durch geeignete technische und organisatorische Maßnahmen vor unrechtmäßiger Zerstörung, zufälligem Verlust oder unrechtmäßiger Speicherung, Verarbeitung, Zugänglichmachung und Verbreitung zu schützen. Ebenso ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den Vorratsdaten ausschließlich besonders ermächtigten Personen vorbehalten ist. Die Kontrolle über die Einhaltung dieser Vorschriften obliegt der für die Datenschutzkontrolle gemäß § 30 DSG 2000 zuständigen Datenschutzkommission.

Erläuterungen:

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, ohnehin hohen 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 sehr wohl 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.

Im Hinblick auf diese nunmehr hinzukommende Aufgabe der Datenschutzkommission ist jedoch auch auf deren schwierige Personalsituation hinzuweisen: Die Datenschutzkommis-

sion besitzt im Vergleich mit anderen Datenschutz-Kontrollstellen in der EU – gemessen an der Einwohnerzahl – nur einen Personalstand von 50% und ist zudem in den vergangenen Jahren in der europäischen Skala weiterhin zurückgefallen und rangiert nunmehr auf Platz 27 von 31 (Datenschutzkommission, Datenschutzbericht 2005-2007). Diese Ressourcenknappheit wirkt sich insbesondere im Rahmen der Prüfungsfunktionen der Datenschutzkommission bezüglich Datenanwendungen bei Auftraggebern negativ aus, weshalb eine Aufstockung des Personalstandes dringend erforderlich ist, um die Einhaltung der Datenschutzbestimmungen für Vorratsdaten sicherzustellen.

(2) Die gem. § 102a zur Speicherung verpflichteten Anbieter gewährleisten, dass jeder Zugriff auf Vorratsdaten sowie jede Anfrage und jede Auskunft über Vorratsdaten nach § 102b protokolliert wird. Diese Protokollierung umfasst

Erläuterungen:

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.

1. die dem Anbieter mit dem Auskunftsbegehren bekannt gegebene Referenz zur staatsanwaltschaftlichen oder gerichtlichen Anordnung gemäß den Bestimmungen der StPO, die der Übermittlung der Daten zugrunde liegt;

Erläuterungen:

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.

2. das Datum der Anfrage sowie das Datum und den genauen Zeitpunkt der erteilten Auskunft;

3. die nach Datum und Kategorien gemäß § 102a Abs. 2 bis 4 aufgeschlüsselte Anzahl der übermittelten Datensätze;

Erläuterungen:

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.

4. die Speicherdauer der übermittelten Daten zum Zeitpunkt der Anordnung der Übermittlung;

Erläuterungen:

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.

5. den Namen und die Anschrift des von der Auskunft über Vorratsdaten betroffenen Teilnehmers, soweit der Anbieter über diese Daten verfügt;

Erläuterungen:

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.

6. eine eindeutige Kennung, welche eine Zuordnung der Person ermöglicht, die im Unternehmen des Anbieters auf Vorratsdaten zugegriffen hat.

Erläuterungen:

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.

(3) Anbieter übermitteln

1. die Protokolldaten gemäß Abs. 2 auf schriftliches Ersuchen der für die Datenschutzkontrolle gemäß § 30 DSG 2000 zuständigen Datenschutzkommission;

2. die Protokolldaten gemäß Abs. 2 Z 1 bis 4 jährlich bis zum 31.1. für das vorangegangene Kalenderjahr oder auf schriftliches Ersuchen dem Bundesminister für Justiz.

(4) Protokolldaten dürfen der Datenschutzkommission ausschließlich für die Zwecke der Kontrolle des Datenschutzes und zur Gewährleistung der Datensicherheit sowie dem Bundesminister für Justiz zum Zweck der jährlichen Berichterstattung an die Europäische Kommission und an das Parlament übermittelt werden.

Erläuterungen:

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. Eine jährliche Berichterstattung gegenüber dem Parlament wird dringend empfohlen, zumal von der flächendeckenden vorrätigen Speicherung nahezu die gesamte Bevölkerung betroffen ist und so eine gewisse öffentliche Kontrolle ausgeübt werden könnte.

(5) Über die Protokollierungspflichten nach Abs. 2 hinaus ist eine Speicherung der übermittelten Datensätze selbst unzulässig.

Erläuterungen:

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.

§ 103. (1)……..

~~(4) Die Bestimmungen der vorstehenden Absätze über die zulässige Verwendung, Auswertung und Übermittlung der einen Teilnehmer betreffenden Daten sind gegenüber Ersuchen der Gerichte, die sich auf die Aufklärung und Verfolgung einer bestimmten Straftat beziehen, nicht anzuwenden. Der Betreiber hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass solchen Ersuchen auch hinsichtlich der Daten entsprochen werden kann, deren Eintragung nach § 69 Abs. 5 unterbleibt.~~

Erläuterungen:

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.

§ 107. (1) Anrufe - einschließlich des Sendens von Fernkopien - zu Werbezwecken ohne vorherige Einwilligung des Teilnehmers sind unzulässig. Der Einwilligung des Teilnehmers steht die Einwilligung einer Person, die vom Teilnehmer zur Benützung seines Anschlusses ermächtigt wurde, gleich. Die erteilte Einwilligung kann jederzeit widerrufen werden; der Widerruf der Einwilligung hat auf ein Vertragsverhältnis mit dem Adressaten der Einwilligung keinen Einfluss.

Erläuterungen:

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.

§ 109. (1)……..

(3)……..

14. entgegen § 94 Abs. 2 nicht an der Überwachung von Nachrichten oder an der Auskunft über Daten einer Nachrichtenübermittlung im erforderlichen Ausmaß mitwirkt;

Erläuterungen:

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

17. entgegen § 98 nicht Auskünfte über Stammdaten oder Standortdaten erteilt oder die Teilnehmer nicht informiert;

Erläuterungen:

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

17a. entgegen § 99 Abs. 5 Z 2 die Teilnehmer nicht informiert;

Erläuterungen:

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.

22. entgegen § 99 Abs. 5 Auskunft über Verkehrsdaten erteilt oder Verkehrsdaten zu Auskunftszwecken verarbeitet;

23. entgegen § 102a Daten nicht speichert; die Strafbarkeit besteht nicht, wenn die hierfür erforderlichen Investitionskosten noch nicht aufgrund einer nach § 94 Abs. 1 erlassenen Verordnung abgegolten wurden;

24. entgegen § 102a Abs. 6 die Anzeige unterlässt, wenn die zur Einstufung als "kleiner Anbieter" wesentlichen Schwellenwerte überschritten werden;

25. entgegen § 102b Daten ohne Vorliegen einer gerichtlichen Bewilligung beauskunftet;

26. entgegen § 102b Daten in nicht verschlüsselter Form über ein Kommunikationsnetz übermittelt;

Erläuterungen:

Durch diese Verwaltungsstrafbestimmung soll bewirkt werden, dass unverschlüsselte Übermittlungen jedenfalls unzulässig sind. Diese Bestimmung dient damit ebenfalls indirekt der Datensicherheit Darauf können und sollen sich Anbieter durchaus auch berufen, falls eine Behörde die unverschlüsselte Übermittlung fordert.

27. entgegen § 102c nicht protokolliert oder die notwendigen Auskünfte erteilt.