Gericht

Verfassungsgerichtshof

Entscheidungsdatum

28.11.2012

Geschäftszahl

G47/12 ua

Sammlungsnummer

******

Leitsatz

Vorlage von Fragen an den EuGH betreffend die Vereinbarkeit von Bestimmungen der Richtlinie über die Vorratsdatenspeicherung mit der Grundrechte-Charta sowie die Auslegung des Datenschutzgrundrechts der Charta aus Anlass von Gesetzesprüfungsverfahren bezüglich der im Telekommunikationsgesetz 2003 enthaltenen Speicherungsverpflichtungen

Spruch

I. Dem Gerichtshof der Europäischen Union werden

gemäß Art267 AEUV folgende Fragen zur Entscheidung vorgelegt:

1. Zur Gültigkeit von Handlungen von Organen der Union:

Sind die Art3 bis 9 der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsdatenspeicherung 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 mit Art7, 8 und 11 der Charta der Grundrechte der Europäischen Union vereinbar?

2. Zur Auslegung der Verträge:

2.1. Sind im Lichte der Erläuterungen zu Art8 der Charta, die gemäß Art52 Abs7 der Charta als Anleitung zur Auslegung der Charta verfasst wurden und vom Verfassungsgerichtshof gebührend zu berücksichtigen sind, die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und die Verordnung (EG) 45/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr für die Beurteilung der Zulässigkeit von Eingriffen gleichwertig mit den Bedingungen nach Art8 Abs2 und Art52 Abs1 der Charta zu berücksichtigen?

2.2. In welchem Verhältnis steht das in Art52 Abs3 letzter Satz der Charta in Bezug genommene "Recht der Union" zu den Richtlinien im Bereich des Datenschutzrechts?

2.3. Sind angesichts dessen, dass die Richtlinie 95/46/EG und die Verordnung (EG) 45/2001 Bedingungen und Beschränkungen für die Wahrnehmung des Datenschutzgrundrechts der Charta enthalten, Änderungen als Folge späteren Sekundärrechts bei der Auslegung des Art8 der Charta zu berücksichtigen?

2.4. Hat unter Berücksichtigung des Art52 Abs4 der Charta der Grundsatz der Wahrung höherer Schutzniveaus in Art53 der Charta zur Konsequenz, dass die nach der Charta maßgeblichen Grenzen für zulässige Einschränkungen durch Sekundärrecht enger zu ziehen sind?

2.5. Können sich im Hinblick auf Art52 Abs3 der Charta, Abs5 der Präambel und die Erläuterungen zu Art7 der Charta, wonach die darin garantierten Rechte den Rechten nach Art8 EMRK entsprechen, aus der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte zu Art8 EMRK Gesichtspunkte für die Auslegung des Art8 der Charta ergeben, die die Auslegung des zuletzt genannten Artikels beeinflussen?

II. Die Gesetzesprüfungsverfahren werden nach

Vorliegen der Entscheidung des Gerichtshofes der Europäischen Union fortgesetzt werden.

Begründung

Begründung:

I.

1. Die Richtlinie 2006/24/EG des Europäischen

Parlaments und des Rates vom 15. März 2006 über die Vorratsdatenspeicherung 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 (im Folgenden: Vorratsdatenspeicherungsrichtlinie) dient gemäß ihrem Art1 Abs1 der Harmonisierung der 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, um sicherzustellen, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von den Mitgliedstaaten jeweils im nationalen Recht bestimmt werden, zur Verfügung stehen. Gemäß Art1 Abs2 der Vorratsdatenspeicherungsrichtlinie gilt diese für Verkehrs- und Standortdaten sowohl von juristischen als auch von natürlichen Personen sowie für alle damit in Zusammenhang stehenden Daten, die zur Feststellung des Teilnehmers oder registrierten Benutzers erforderlich sind; Inhalte elektronischer Nachrichtenübermittlungen sind nicht vom Anwendungsbereich der Vorratsdatenspeicherungsrichtlinie erfasst. Die Daten sind für einen Zeitraum von mindestens sechs Monaten und höchstens zwei Jahren ab dem Zeitpunkt der Kommunikation auf Vorrat zu speichern.

2. Das Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 - TKG 2003), enthält bereits in seiner Stammfassung Bestimmungen, die den Betreiber eines Telekommunikationsnetzes dazu verpflichten, bestimmte Daten zu speichern. Mit der Novelle BGBl. I 27/2011 wurde die Vorratsdatenspeicherungsrichtlinie umgesetzt und wurden die Speicherungsverpflichtungen in einem neu eingefügten §102a TKG 2003 (unten Pkt. II.2.) erweitert. Diese Novelle trat am 1. April 2012 in Kraft, der entsprechende Umsetzungshinweis findet sich in §1 Abs4 Z5 TKG 2003.

3. Die Kärntner Landesregierung (im Folgenden: antragstellende Landesregierung) brachte auf Grund ihres Beschlusses vom 27. März 2012 am 6. April 2012 beim Verfassungsgerichtshof einen Antrag gem. Art140 Abs1 Bundes-Verfassungsgesetz (B-VG) ein, mit dem sie die Aufhebung näher genannter Bestimmungen des TKG 2003 begehrt (G47/12), unter anderem des §102a, der mit der Novelle BGBl. I 27/2011 eingefügt wurde.

4. Am 25. Mai 2012 brachte Mag. M S, ein Angestellter der A1 Telekom Austria AG, einen Antrag gem. Art140 Abs1 B-VG ein, in dem er behauptet, u.a. durch die Verfassungswidrigkeit des §102a TKG 2003 unmittelbar in seinen Rechten verletzt zu sein. Er bringt vor, über vier Teilnehmeranschlüsse zu verfügen, die er sowohl beruflich als auch privat für Sprachtelefonie bzw. Internet-Zugang einschließlich E-Mail-Dienste nutze. Die angefochtene Bestimmung verpflichte den Betreiber seines Kommunikationsnetzes, näher genannte Daten des Antragstellers ohne Anlass, unabhängig von technischen Notwendigkeiten oder von Verrechnungszwecken und unabhängig von oder gar gegen dessen Willen zu speichern. Darin erblickt der Antragsteller u.a. einen Verstoß gegen Art8 Charta der Grundrechte der Europäischen Union (im Folgenden: Grundrechte-Charta).

5. Am 15. Juni 2012 langte ein weiterer Antrag gem. Art140 B-VG beim Verfassungsgerichtshof ein, in dem ebenfalls behauptet wird, dass die - insgesamt 11.130 - Antragsteller durch die Verfassungswidrigkeit der in §102a TKG 2003 festgeschriebenen Speicherungsverpflichtung unmittelbar in ihren Rechten verletzt seien, da sämtliche Antragsteller (zumindest) einen Vertrag zur Nutzung eines oder mehrerer der in §102a Abs2 bis 4 TKG 2003 aufgezählten Dienste abgeschlossen hätten und daher mit ihren Teilnehmerdaten ("Stammdaten") zu den jeweiligen Verkehrsdaten von der Vorratsdatenspeicherung erfasst würden. Auch die Antragsteller in diesem Verfahren erblicken in der verdachtsunabhängigen und anlasslosen Speicherung ihrer Daten u.a. einen Verstoß gegen Art8 Grundrechte-Charta.

II.

Die maßgebliche Rechtslage stellt sich wie folgt dar:

1. Die Bestimmungen der Richtlinie 2006/24/EG vom 15. März 2006 über die Vorratsdatenspeicherung 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 lauten:

"Artikel 1

Gegenstand und Anwendungsbereich

(1) Mit dieser Richtlinie sollen 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.

(2) Diese Richtlinie gilt 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 nicht für den Inhalt elektronischer Nachrichtenübermittlungen einschließlich solcher Informationen, die mit Hilfe eines elektronischen Kommunikationsnetzes abgerufen werden.

Artikel 2

Begriffsbestimmungen

(1) Für die Zwecke dieser Richtlinie finden die Begriffsbestimmungen der Richtlinie 95/46/EG, der Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie) und der Richtlinie 2002/58/EG Anwendung.

(2) Im Sinne dieser Richtlinie bezeichnet der Ausdruck

a) 'Daten' Verkehrsdaten und Standortdaten sowie alle damit in Zusammenhang stehende Daten, die zur Feststellung des Teilnehmers oder Benutzers erforderlich sind;

b) 'Benutzer' jede juristische oder natürliche

Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst notwendigerweise abonniert zu haben;

c) 'Telefondienst' Anrufe (einschließlich Sprachtelefonie, Sprachspeicherdienst, Konferenzschaltungen und Datenabrufungen), Zusatzdienste (einschließlich Rufweiterleitung und Rufumleitung) und Mitteilungsdienste und Multimediadienste (einschließlich Kurznachrichtendienste (SMS), erweiterte Nachrichtendienste (EMS) und Multimediadienste (MMS));

d) 'Benutzerkennung' eine eindeutige Kennung, die Personen zugewiesen wird, wenn diese sich bei einem Internetanbieter oder einem Internet-Kommunikationsdienst registrieren lassen oder ein Abonnement abschließen;

e) 'Standortkennung' die Kennung der Funkzelle, von der aus eine Mobilfunkverbindung hergestellt wird bzw. in der sie endet;

f) 'erfolgloser Anrufversuch' einen Telefonanruf, bei dem die Verbindung erfolgreich aufgebaut wurde, der aber unbeantwortet bleibt oder bei dem das Netzwerkmanagement eingegriffen hat.

Artikel 3

Vorratsspeicherungspflicht

(1) Abweichend von den Artikeln 5, 6 und 9 der Richtlinie 2002/58/EG tragen die Mitgliedstaaten durch entsprechende Maßnahmen dafür Sorge, dass die in Artikel 5 der vorliegenden Richtlinie genannten Daten, 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.

(2) Die Verpflichtung zur Vorratsspeicherung nach Absatz 1 schließt die Vorratsspeicherung von in Artikel 5 genannten Daten im Zusammenhang mit erfolglosen Anrufversuchen ein, wenn diese Daten von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes im Rahmen der Zuständigkeit des betreffenden Mitgliedstaats im Zuge der Bereitstellung der betreffenden Kommunikationsdienste erzeugt oder verarbeitet und gespeichert (bei Telefoniedaten) oder protokolliert (bei Internetdaten) werden. Nach dieser Richtlinie ist die Vorratsspeicherung von Daten im Zusammenhang mit Anrufen, bei denen keine Verbindung zustande kommt, nicht erforderlich.

Artikel 4

Zugang zu Daten

Die Mitgliedstaaten erlassen Maßnahmen, um sicherzustellen, dass die gemäß dieser Richtlinie auf Vorrat gespeicherten Daten nur in bestimmten Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden weitergegeben werden. Jeder Mitgliedstaat legt in seinem innerstaatlichen Recht unter Berücksichtigung der einschlägigen Bestimmungen des Rechts der Europäischen Union oder des Völkerrechts, insbesondere der EMRK in der Auslegung durch den Europäischen Gerichtshof für Menschenrechte, das Verfahren und die Bedingungen fest, die für den Zugang zu auf Vorrat gespeicherten Daten gemäß den Anforderungen der Notwendigkeit und der Verhältnismäßigkeit einzuhalten sind.

Artikel 5

Kategorien von auf Vorrat zu speichernden Daten

(1) Die Mitgliedstaaten stellen sicher, dass gemäß dieser Richtlinie die folgenden Datenkategorien auf Vorrat gespeichert werden:

a) zur Rückverfolgung und Identifizierung der Quelle einer Nachricht benötigte Daten:

1. betreffend Telefonfestnetz und Mobilfunk:

i) die Rufnummer des anrufenden Anschlusses,

ii) der Name und die Anschrift des Teilnehmers oder registrierten Benutzers;

2. betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:

i) die zugewiesene(n) Benutzerkennung(en),

ii) die Benutzerkennung und die Rufnummer, die jeder Nachricht im öffentlichen Telefonnetz zugewiesen werden,

iii) der Name und die Anschrift des Teilnehmers bzw. registrierten Benutzers, dem eine Internetprotokoll-Adresse (IP-Adresse), Benutzerkennung oder Rufnummer zum Zeitpunkt der Nachricht zugewiesen war;

b) zur Identifizierung des Adressaten einer Nachricht benötigte Daten:

1. betreffend Telefonfestnetz und Mobilfunk:

i) die angewählte(n) Nummer(n) (die Rufnummer(n) des angerufenen Anschlusses) und bei Zusatzdiensten wie Rufweiterleitung oder Rufumleitung die Nummer(n), an die der Anruf geleitet wird,

ii) die Namen und Anschriften der Teilnehmer oder registrierten Benutzer;

2. betreffend Internet-E-Mail und Internet-Telefonie:

i) die Benutzerkennung oder Rufnummer des
vorgesehenen Empfängers eines Anrufs mittels Internet-Telefonie,

ii) die Namen und Anschriften der Teilnehmer oder registrierten Benutzer und die Benutzerkennung des vorgesehenen Empfängers einer Nachricht;

c) zur Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung benötigte Daten:

1. betreffend Telefonfestnetz und Mobilfunk: Datum und Uhrzeit des Beginns und Endes eines Kommunikationsvorgangs;

2. betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:

i) Datum und Uhrzeit der An- und Abmeldung beim Internetzugangsdienst auf der Grundlage einer bestimmten Zeitzone, zusammen mit der vom Internetzugangsanbieter einer Verbindung zugewiesenen dynamischen oder statischen IP-Adresse und die Benutzerkennung des Teilnehmers oder des registrierten Benutzers,

ii) Datum und Uhrzeit der An- und Abmeldung beim Internet-E-Mail-Dienst oder Internet-Telefonie-Dienst auf der Grundlage einer bestimmten Zeitzone;

d) zur Bestimmung der Art einer Nachrichtenübermittlung benötigte Daten:

1. betreffend Telefonfestnetz und Mobilfunk: der in Anspruch genommene Telefondienst;

2. betreffend Internet-E-Mail und Internet-Telefonie:
der in Anspruch genommene Internetdienst;

e) zur Bestimmung der Endeinrichtung oder der vorgeblichen Endeinrichtung von Benutzern benötigte Daten:

1. betreffend Telefonfestnetz: die Rufnummern des anrufenden und des angerufenen Anschlusses;

2. betreffend Mobilfunk:

i) die Rufnummern des anrufenden und des angerufenen Anschlusses,

ii) die internationale Mobilteilnehmerkennung (IMSI) des anrufenden Anschlusses,

iii) die internationale Mobilfunkgerätekennung (IMEI) des anrufenden Anschlusses,

iv) die IMSI des angerufenen Anschlusses,

v) die IMEI des angerufenen Anschlusses,

vi) im Falle vorbezahlter anonymer Dienste: Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Kennung des Standorts (Cell-ID), an dem der Dienst aktiviert wurde;

3. betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:

i) die Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluss,

ii) der digitale Teilnehmeranschluss (DSL) oder ein anderer Endpunkt des Urhebers des Kommunikationsvorgangs;

f) zur Bestimmung des Standorts mobiler Geräte

benötigte Daten:

1. die Standortkennung (Cell-ID) bei Beginn der Verbindung,

2. Daten zur geografischen Ortung von Funkzellen

durch Bezugnahme auf ihre Standortkennung (Cell-ID) während des Zeitraums, in dem die Vorratsspeicherung der Kommunikationsdaten erfolgt.

(2) Nach dieser Richtlinie dürfen keinerlei Daten, die Aufschluss über den Inhalt einer Kommunikation geben, auf Vorrat gespeichert werden.

Artikel 6

Speicherungsfristen

Die Mitgliedstaaten sorgen dafür, dass die in Artikel 5 angegebenen Datenkategorien für einen Zeitraum von mindestens sechs Monaten und höchstens zwei Jahren ab dem Zeitpunkt der Kommunikation auf Vorrat gespeichert werden.

Artikel 7

Datenschutz und Datensicherheit

Unbeschadet der zur Umsetzung der Richtlinien 95/46/EG und 2002/58/EG erlassenen Vorschriften stellt jeder Mitgliedstaat sicher, dass Anbieter von öffentlich zugänglichen elektronischen Kommunikationsdiensten bzw. Betreiber eines öffentlichen Kommunikationsnetzes in Bezug auf die nach Maßgabe der vorliegenden Richtlinie auf Vorrat gespeicherten Daten zumindest die folgenden Grundsätze der Datensicherheit einhalten:

a) Die auf Vorrat gespeicherten Daten sind von der gleichen Qualität und unterliegen der gleichen Sicherheit und dem gleichen Schutz wie die im Netz vorhandenen Daten,

b) in Bezug auf die Daten werden geeignete technische und organisatorische Maßnahmen getroffen, um die Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust oder zufällige Änderung, unberechtigte oder unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung zu schützen,

c) in Bezug auf die Daten werden geeignete technische und organisatorische Maßnahmen getroffen, um sicherzustellen, dass der Zugang zu den Daten ausschließlich besonders ermächtigten Personen vorbehalten ist,

und

d) die Daten werden am Ende der Vorratsspeicherungsfrist vernichtet, mit Ausnahme jener Daten, die abgerufen und gesichert worden sind.

Artikel 8

Anforderungen an die Vorratsdatenspeicherung

Die Mitgliedstaaten stellen sicher, dass die in Artikel 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.

Artikel 9

Kontrollstelle

(1) Jeder Mitgliedstaat benennt eine oder mehrere öffentliche Stellen, die für die Kontrolle der Anwendung der von den Mitgliedstaaten zur Umsetzung von Artikel 7 erlassenen Vorschriften bezüglich der Sicherheit der auf Vorrat gespeicherten Daten in seinem Hoheitsgebiet zuständig ist/sind. Diese Stellen können dieselben Stellen sein, auf die in Artikel 28 der Richtlinie 95/46/EG Bezug genommen wird.

(2) Die in Absatz 1 genannten Stellen nehmen die dort genannte Kontrolle in völliger Unabhängigkeit wahr.

Artikel 10

Statistik

(1) Die Mitgliedstaaten sorgen dafür, dass der Kommission jährlich eine Statistik über die Vorratsspeicherung von in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder eines öffentlichen Kommunikationsnetzes erzeugten oder verarbeiteten Daten übermittelt wird. Aus dieser Statistik muss hervorgehen:

- in welchen Fällen im Einklang mit dem innerstaatlichen Recht Daten an die zuständigen Behörden weitergegeben worden sind;

- wie viel Zeit zwischen dem Zeitpunkt der Vorratsspeicherung der Daten und dem Zeitpunkt, zu dem sie von der zuständigen Behörde angefordert wurden, vergangen ist

und

- in welchen Fällen die Anfragen nach Daten ergebnislos geblieben sind.

(2) Die Statistik darf keine personenbezogenen Daten enthalten.

Artikel 11

Änderung der Richtlinie 2002/58/EG

In Artikel 15 der Richtlinie 2002/58/EG wird folgender Absatz eingefügt:

'(1a) Absatz 1 gilt nicht für Daten, für die in der 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, eine Vorratsspeicherung zu den in Artikel 1 Absatz 1 der genannten Richtlinie aufgeführten Zwecken ausdrücklich vorgeschrieben ist.'

Artikel 12

Zukünftige Maßnahmen

(1) Ein Mitgliedstaat, in dem besondere Umstände die Verlängerung der maximalen Speicherungsfrist nach Artikel 6 für einen begrenzten Zeitraum rechtfertigen, kann die notwendigen Maßnahmen ergreifen. Der Mitgliedstaat setzt die Kommission hiervon unverzüglich in Kenntnis und unterrichtet die anderen Mitgliedstaaten über die gemäß dem vorliegenden Artikel ergriffenen Maßnahmen und gibt die Gründe für ihre Einführung an.

(2) Binnen eines Zeitraums von sechs Monaten nach der Mitteilung nach Absatz 1 billigt die Kommission die betreffenden einzelstaatlichen Maßnahmen oder lehnt diese ab, nachdem sie geprüft hat, ob sie ein Mittel zur willkürlichen Diskriminierung oder eine verschleierte Beschränkung des Handels zwischen den Mitgliedstaaten darstellen und ob sie das Funktionieren des Binnenmarktes behindern. Trifft die Kommission innerhalb dieses Zeitraums keine Entscheidung, so gelten die einzelstaatlichen Maßnahmen als gebilligt.

(3) Werden die von den Bestimmungen dieser Richtlinie abweichenden einzelstaatlichen Maßnahmen eines Mitgliedstaats nach Absatz 2 gebilligt, so kann die Kommission prüfen, ob sie eine Änderung dieser Richtlinie vorschlägt.

Artikel 13

Rechtsbehelfe, Haftung und Sanktionen

(1) Jeder Mitgliedstaat ergreift die erforderlichen Maßnahmen, um sicherzustellen, dass die einzelstaatlichen Maßnahmen zur Umsetzung von Kapitel III der Richtlinie 95/46/EG über Rechtsbehelfe, Haftung und Sanktionen im Hinblick auf die Datenverarbeitung gemäß der vorliegenden Richtlinie in vollem Umfang umgesetzt werden.

(2) Jeder Mitgliedstaat ergreift insbesondere die erforderlichen Maßnahmen, um sicherzustellen, dass der vorsätzliche Zugang zu oder die vorsätzliche Übermittlung von gemäß dieser Richtlinie auf Vorrat gespeicherten Daten, der bzw. die nach den zur Umsetzung dieser Richtlinie erlassenen nationalen Rechtsvorschriften nicht zulässig ist, mit Sanktionen, einschließlich verwaltungsrechtlicher und strafrechtlicher Sanktionen, belegt wird, die wirksam, verhältnismäßig und abschreckend sind.

Artikel 14

Bewertung

(1) Die Kommission legt dem Europäischen Parlament und dem Rat spätestens am 15. September 2010 eine Bewertung der Anwendung dieser Richtlinie sowie ihrer Auswirkungen auf die Wirtschaftsbeteiligten und die Verbraucher vor, um festzustellen, ob die Bestimmungen dieser Richtlinie, insbesondere die Liste von Daten in Artikel 5 und die in Artikel 6 vorgesehenen Speicherungsfristen, gegebenenfalls geändert werden müssen; hierbei berücksichtigt sie die Weiterentwicklung der Technologie der elektronischen Kommunikation und die ihr gemäß Artikel 10 zur Verfügung gestellte Statistik. Die Ergebnisse dieser Bewertung werden öffentlich gemacht.

(2) Die Kommission prüft zu diesem Zweck sämtliche Kommentare, die ihr von den Mitgliedstaaten oder der gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzten Datenschutzgruppe übermittelt werden.

Artikel 15

Umsetzung

(1) Die Mitgliedstaaten setzen die Rechts- und Verwaltungsvorschriften in Kraft, die erforderlich sind, um dieser Richtlinie bis spätestens 15. September 2007 nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis.

Wenn die Mitgliedstaaten diese Vorschriften erlassen, nehmen sie in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten der Bezugnahme.

(2) Die Mitgliedstaaten teilen der Kommission den Wortlaut der wichtigsten innerstaatlichen Rechtsvorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

(3) Bis 15. März 2009 kann jeder Mitgliedstaat die Anwendung dieser Richtlinie auf die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail aufschieben. Beabsichtigt ein Mitgliedstaat, den vorliegenden Absatz in Anspruch zu nehmen, so unterrichtet er den Rat und die Kommission hiervon mittels einer Erklärung bei der Annahme dieser Richtlinie. Die Erklärung wird im Amtsblatt der Europäischen Union veröffentlicht.

Artikel 16

Inkrafttreten

Diese Richtlinie tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

Artikel 17

Adressaten

Diese Richtlinie ist an die Mitgliedstaaten

gerichtet."

2. §102a TKG 2003, der Anbietern von öffentlichen Kommunikationsdiensten die Verpflichtung zur Speicherung ausdrücklich aufgezählter Daten vorschreibt, hat folgenden Wortlaut:

"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 Abs2 bis 4 Daten ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation zu speichern. Die Speicherung erfolgt ausschließlich zur Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach §135 Abs2a StPO rechtfertigt.

(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 zugrunde liegenden Zeitzone zugewiesen war;

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

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

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

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

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

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;

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

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

6. Bei Mobilfunknetzen zudem

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

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

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

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

(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;

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;

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;

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

(5) Die Speicherpflicht nach Abs1 besteht nur für

jene Daten gemäß Abs2 bis 4, die im Zuge der Bereitstellung der betreffenden Kommunikationsdienste erzeugt oder verarbeitet werden. Im Zusammenhang mit erfolglosen Anrufversuchen besteht die Speicherpflicht nach Abs1 nur, soweit diese Daten im Zuge der Bereitstellung des betreffenden Kommunikationsdienstes erzeugt oder verarbeitet und gespeichert oder protokolliert werden.

(6) Die Speicherpflicht nach Abs1 besteht nicht für solche Anbieter, deren Unternehmen nicht der Verpflichtung zur Entrichtung des Finanzierungsbeitrages gemäß §34 KommAustriaG unterliegen.

(7) Der Inhalt der Kommunikation und insbesondere

Daten über im Internet aufgerufene Adressen dürfen auf Grund dieser Vorschrift nicht gespeichert werden.

(8) Die nach Abs1 zu speichernden Daten sind nach

Ablauf der Speicherfrist unbeschadet des §99 Abs2 unverzüglich, spätestens jedoch einen Monat nach Ablauf der Speicherfrist, zu löschen. Die Erteilung einer Auskunft nach Ablauf der Speicherfrist ist unzulässig.

(9) 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."

Gemäß §102b TKG 2003 ist eine Auskunft über

Vorratsdaten ausschließlich auf Grund einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft zur Aufklärung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach §135 Abs2a Strafprozessordnung 1975 (Zulässigkeit der Auskunft über Vorratsdaten unter näher genannten Voraussetzungen, wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als sechs Monaten bzw. mehr als einem Jahr bedroht ist, gefördert werden kann, bzw. wenn auf Grund bestimmter Tatsachen zu erwarten ist, dass dadurch der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer mit mehr als einjähriger Freiheitsstrafe bedrohten vorsätzlich begangenen strafbaren Handlung dringend verdächtig ist, ermittelt werden kann) rechtfertigt, zulässig. Die Speicherung hat so zu erfolgen, dass die Daten unverzüglich an die nach den Bestimmungen der Strafprozessordnung für die Erteilung einer Auskunft über Daten einer Nachrichtenübermittlung zuständigen Behörden übermittelt werden können. Die Übermittlung der Daten hat "in angemessen geschützter Form" nach Maßgabe der in §94 Abs4 TKG 2003 vorzusehenden technischen Einrichtungen zu erfolgen.

§102c TKG 2003 enthält Bestimmungen über die Datensicherheit, Protokollierung und Statistik. So ist etwa durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den Vorratsdaten ausschließlich dazu ermächtigten Personen unter Einhaltung des Vier-Augen-Prinzips vorbehalten ist. Die Protokolldaten, die von zur Speicherung verpflichteten Anbietern über jeden Zugriff auf Vorratsdaten sowie über jede Anfrage oder Auskunft über Vorratsdaten zu führen sind, sind für drei Jahre ab Ende der Speicherfrist für das betreffende Vorratsdatum zu speichern. Die Kontrolle der Einhaltung dieser Verpflichtungen obliegt der Datenschutzkommission.

§109 Z22 bis 26 TKG 2003 enthält eine Strafbestimmung, nach der eine Verwaltungsübertretung begeht und mit Geldstrafe bis zu € 37.000,-- zu bestrafen ist, wer gegen die Bestimmungen der §§102a bis 102c leg.cit. verstößt.

3. §135 Strafprozessordnung, BGBl. 631/1975 idF BGBl. I 33/2011, lautet:

"Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Auskunft über Vorratsdaten sowie Überwachung von Nachrichten

§135. (1) Beschlagnahme von Briefen ist zulässig,

wenn sie zur Aufklärung einer vorsätzlich begangenen Straftat, die mit mehr als einjähriger Freiheitsstrafe bedroht ist, erforderlich ist und sich der Beschuldigte wegen einer solchen Tat in Haft befindet oder seine Vorführung oder Festnahme deswegen angeordnet wurde.

(2) Auskunft über Daten einer Nachrichtenübermittlung ist zulässig,

1. wenn und solange der dringende Verdacht besteht, dass eine von der Auskunft betroffene Person eine andere entführt oder sich sonst ihrer bemächtigt hat, und sich die Auskunft auf Daten einer solchen Nachricht beschränkt, von der anzunehmen ist, dass sie zur Zeit der Freiheitsentziehung vom Beschuldigten übermittelt, empfangen oder gesendet wird,

2. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann und der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft ausdrücklich zustimmt, oder

3. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, gefördert werden kann und auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können.

4. wenn auf Grund bestimmter Tatsachen zu erwarten ist, dass dadurch der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig ist, ermittelt werden kann.

(2a) Auskunft über Vorratsdaten (§§102a und 102b TKG) ist in den Fällen des Abs2 Z2 bis 4 zulässig.

(3) Überwachung von Nachrichten ist zulässig,

1. in den Fällen des Abs2 Z1,

2. in den Fällen des Abs2 Z2, sofern der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Überwachung zustimmt,

3. wenn dies zur Aufklärung einer vorsätzlich

begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, erforderlich erscheint oder die Aufklärung oder Verhinderung von im Rahmen einer kriminellen oder terroristischen Vereinigung oder einer kriminellen Organisation (§§278 bis 278b StGB) begangenen oder geplanten strafbaren Handlungen ansonsten wesentlich erschwert wäre und

a) der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, oder einer Straftat gemäß §§278 bis 278b StGB dringend verdächtig ist, oder

b) auf Grund bestimmter Tatsachen anzunehmen ist,

dass eine der Tat (lita) dringend verdächtige Person die technische Einrichtung benützen oder mit ihr eine Verbindung herstellen werde;

4. in den Fällen des Abs2 Z4."

4. Der im Verfassungsrang stehende §1 des Bundesgesetzes über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000), BGBl. I 165/1999 idF BGBl. I 112/2011, lautet:

"(Verfassungsbestimmung)

Grundrecht auf Datenschutz

§1. (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art8 Abs2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

(3) Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh. ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen

1. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;

2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.

(4) Beschränkungen der Rechte nach Abs3 sind nur

unter den in Abs2 genannten Voraussetzungen zulässig.

(5) Gegen Rechtsträger, die in Formen des Privatrechts eingerichtet sind, ist, soweit sie nicht in Vollziehung der Gesetze tätig werden, das Grundrecht auf Datenschutz mit Ausnahme des Rechtes auf Auskunft auf dem Zivilrechtsweg geltend zu machen. In allen übrigen Fällen ist die Datenschutzkommission zur Entscheidung zuständig, es sei denn, daß Akte der Gesetzgebung oder der Gerichtsbarkeit betroffen sind."

III.

1. In den beim Verfassungsgerichtshof anhängigen Anträgen wird mit unterschiedlicher Begründung nicht nur geltend gemacht, dass §102a TKG 2003 das Grundrecht auf Datenschutz (§1 Abs1 DSG 2000, Art8 EMRK, Art8 Grundrechte-Charta) verletze, sondern auch, dass die Vorratsdatenspeicherungsrichtlinie gegen Art8 Grundrechte-Charta verstoße. Während die antragstellende Landesregierung behauptet, dass die Vorratsdatenspeicherungsrichtlinie nicht im Einklang mit Art8 Grundrechte-Charta stünde, rügt der Antragsteller im Verfahren zu G59/12, dass die Vorratsdatenspeicherungsrichtlinie überhaupt gegen die Art7, 8, 11 und 20 Grundrechte-Charta verstoßen würde.

1.1. Antrag zu G47/12:

Nach Ansicht der antragstellenden Landesregierung

stelle die in den zur Umsetzung der Vorratsdatenspeicherungsrichtlinie ergangenen Bestimmungen des TKG 2003 vorgesehene verdachtsunabhängige Speicherung von Kommunikationsdaten einen massiven Eingriff in näher bezeichnete Grundrechte dar. Die antragstellende Landesregierung vermeint insbesondere, dass durch die pauschale Speicherung aller Verkehrs- und Standortdaten bei Kenntnis der Adressaten sowie der Häufigkeit und des Zeitpunktes der Kontakte vielfach Rückschlüsse auf Inhalte der Kommunikation gezogen werden könnten und dass bereits das Wissen um die Protokollierung der Daten ausreiche, um das Kommunikationsverhalten zu verändern. Darüber hinaus seien die Regelungen angesichts der unzuverlässigen Aussagekraft der aus den Daten abgeleiteten Informationen und der leichten Umgehungsmöglichkeit (etwa durch Nutzung von "prepaid"-Wertkarten für Mobiltelefone) im Hinblick auf den durch die Vorratsdatenspeicherungsrichtlinie angestrebten Zweck der Ermittlung, Feststellung und Verfolgung schwerer Straftaten nur in sehr geringem Maße geeignet und

der Grundrechtseingriff daher unverhältnismäßig. Die antragstellende Landesregierung macht ferner einen Verstoß gegen Art8 Grundrechte-Charta geltend. Aus der Formulierung des Rechts ergebe sich insbesondere, dass jeder einzelne ein Recht auf Datenschutz auch gegenüber der Union habe. Im Hinblick auf den Grundsatz der Verhältnismäßigkeit wird gerügt, dass weder im Vorfeld noch im Zuge der Beschlussfassung über die Vorratsdatenspeicherungsrichtlinie Ermittlungen zur Notwendigkeit bzw. hinsichtlich des zu erwartenden Erfolges einer solchen Maßnahme im Zusammenhang mit der Ermittlung, Feststellung und Verfolgung von schweren Straftaten durchgeführt worden seien.

1.2. Antrag zu G59/12:

Auch in dem Individualantrag zu G59/12 wird

vorgebracht, dass durch die vorgegebene Verpflichtung zur Speicherung der Daten Rückschlüsse auf Verhalten, Gewohnheiten und Aufenthaltsorte der Nutzer von Kommunikationsdiensten und damit die Erstellung von sogenannten "Bewegungsprofilen" ermöglicht würden. Der Antragsteller rügt, dass nach der Vorratsdatenspeicherungsrichtlinie Betreiber von nicht-öffentlichen Kommunikationsdiensten und -netzen (wie etwa Firmennetzwerken) nicht der Verpflichtung zur Vorratsdatenspeicherung unterliegen würden und es - weiterhin - möglich sei, dass Betreiber von öffentlichen Internet-Zugangsdiensten eine anonyme Nutzung ermöglichen und Betreiber von öffentlichen Telefondiensten ("prepaid") Wertkarten anbieten könnten, ohne dass die Daten der Nutzer aufgenommen werden müssten. Der Antragsteller bringt vor, dass die Vorratsdatenspeicherungsrichtlinie auf Grund eines Verstoßes gegen Art7, 8, 11 und 20 Grundrechte-Charta nicht rechtmäßig sei bzw. keine Rechtswirkungen entfalte, den österreichischen Gesetzgeber daher keine Verpflichtung zur Umsetzung treffe und kein Anwendungsvorrang der Regelungen vor dem österreichischen Verfassungsrecht anzunehmen sei. Der Antragsteller regt daher an, der Verfassungsgerichtshof möge gemäß Art267 AEUV ein Ersuchen um Vorabentscheidung an den Gerichtshof der Europäischen Union richten, und zwar mit der Frage, ob die Vorratsdatenspeicherungsrichtlinie gültig sei.

1.3. Antrag zu G62,70,71/12:

Die Antragsteller weisen zunächst darauf hin, dass zwar schon bisher nach der österreichischen Rechtslage vielfältig personenbezogene Daten ermittelt und verarbeitet worden seien, diese Datenanwendungen jedoch in aller Regel entweder zur individuellen Aufklärung und Verfolgung begangener Straftaten, zur Erfüllung eines Vertrages oder aber mit dem Ziel, der Gesellschaft die unterschiedlichsten Leistungen der öffentlichen Daseinsvorsorge zur Verfügung zu stellen, erfolgt seien. Durch die Umsetzung der Vorratsdatenspeicherungsrichtlinie erfolge die Datenspeicherung und -verarbeitung demgegenüber präventiv zum Zwecke der Ermittlung, Feststellung und Verfolgung von Straftaten ohne irgendeinen konkreten Tatverdacht. Dies stelle "im Ergebnis einen Paradigmenwechsel dar, der aus grundrechtlicher Sicht nicht zu rechtfertigen" sei. Die Antragsteller zu G62,70,71/12 bringen vor, dass sie die Umsetzung der Vorratsdatenspeicherungsrichtlinie durch den Verlust des "Gefühl[s], frei, selbstbestimmt und unbeobachtet leben zu können und nicht behelligt zu werden, wenn, soweit und solange man die Gesetze des Staates achte und befolge und nicht delinquent werde", beeinträchtige. Die Antragsteller behaupten u.a. einen Verstoß gegen Art7 und 8 Grundrechte-Charta sowie gegen §1 DSG 2000, den sie im Wesentlichen mit der zu Art8 EMRK ergangenen Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte begründen. Nach Ansicht der Antragsteller sei der durch die Speicherungsverpflichtung bewirkte Eingriff insbesondere auch angesichts der mangelnden Rechtsschutzmöglichkeiten nicht verhältnismäßig.

IV.

Der Verfassungsgerichtshof hat über die in

sinngemäßer Anwendung des §187 ZPO iVm §35 VfGG zur gemeinsamen Beratung verbundenen Anträge erwogen:

1. Der Verfassungsgerichtshof ist zur Entscheidung über die an ihn herangetragenen Gesetzesprüfungsanträge zuständig.

Gemäß Art140 Abs1 zweiter und vierter Satz B-VG hat der Verfassungsgerichtshof über die Verfassungswidrigkeit eines Bundesgesetzes unter anderem auf Antrag einer Landesregierung oder auf Antrag einer Person, die unmittelbar durch diese Verfassungswidrigkeit in ihren Rechten verletzt zu sein behauptet (Individualantrag), sofern das Gesetz ohne Fällung einer gerichtlichen Entscheidung oder ohne Erlassung eines Bescheides für diese Person wirksam geworden ist, zu entscheiden.

1.1. Der Verfassungsgerichtshof geht - für die Zwecke des Gesetzesprüfungsverfahrens: vorläufig - davon aus, dass der Antrag der Kärntner Landesregierung zu G47/12 und die Individualanträge zu G59/12 und zu G62,70,71/12 zulässig sind.

1.2. Nach der Rechtsprechung des Verfassungsgerichtshofes bilden die von der Grundrechte-Charta garantierten Rechte im Anwendungsbereich der Grundrechte-Charta (Art51 Abs1 Grundrechte-Charta) einen Prüfungsmaßstab in Verfahren der Normenkontrolle, insbesondere in Verfahren nach Art139 und 140 B-VG. Dies gilt jedenfalls dann, wenn die betreffende Garantie der Grundrechte-Charta in ihrer Formulierung und Bestimmtheit verfassungsgesetzlich gewährleisteten Rechten der österreichischen Bundesverfassung gleicht (vgl. VfGH 14.3.2012, U466/11 ua.).

Der Verfassungsgerichtshof hat daher - wie schon

bisher (vgl. VfSlg. 15.450/1999, 16.050/2000, 16.100/2001) - dann eine Frage dem Gerichtshof der Europäischen Union zur Vorabentscheidung vorzulegen, wenn er Zweifel an der Auslegung einer unionsrechtlichen Vorschrift, dh. auch der Grundrechte-Charta, oder Zweifel an der Gültigkeit einer Vorschrift des Sekundärrechts hat.

Der Verfassungsgerichtshof ist sohin nicht nur in Fragen der Auslegung der Grundrechte-Charta vorlageverpflichtetes Gericht im Sinne des Art267 Abs3 AEUV (vgl. VfGH 14.3.2012, U466/11 ua.), sondern auch in Fällen, in denen in einem bei ihm anhängigen Verfahren die Vereinbarkeit von Sekundärrecht mit der Grundrechte-Charta und damit dessen Gültigkeit in Frage steht.

2. Den Verfassungsgerichtshof bestimmen sowohl

Zweifel über die Auslegung der Grundrechte-Charta als auch Bedenken ob der Gültigkeit der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung dazu, ein Ersuchen um Vorabentscheidung an den Gerichtshof der Europäischen Union zu richten.

3. Voraussetzung der Zulässigkeit eines Vorabentscheidungsersuchens nach Art267 AEUV ist, dass das vorlegende Gericht die Entscheidung der Gültigkeitsfrage für erforderlich, dh. für entscheidungserheblich hält. Darüber hat das vorlegende Gericht in eigener Zuständigkeit zu entscheiden (EuGH 27.6.1991, Rs. C-348/89, Mecanarte, Slg. 1991, I-3277 [Rz 47]).

Sowohl die Frage nach der Gültigkeit der Vorratsdatenspeicherungsrichtlinie als auch die Fragen nach der Auslegung des Art8 Grundrechte-Charta sind entscheidungserheblich:

3.1. §102a TKG 2003 ist ausweislich des Umsetzungshinweises und der Gesetzesmaterialien in Umsetzung der Vorratsdatenspeicherungsrichtlinie ergangen. Die gesetzliche Regelung setzt demgemäß im Wesentlichen alle Inhalte der Richtlinie um. §102a Abs1 leg.cit. normiert in Umsetzung des Art3 Vorratsdatenspeicherungsrichtlinie die grundsätzliche Speicherungsverpflichtung und sieht unter Heranziehung der Mindestfrist des Art6 Vorratsdatenspeicherungsrichtlinie eine Speicherungsfrist von sechs Monaten vor. Abs2 und 3 definieren in Umsetzung von Art5 Vorratsdatenspeicherungsrichtlinie die zu speichernden Daten.

Diese Regelung trifft in der österreichischen Rechtsordnung auf spezifische verfassungsrechtliche Anforderungen. Das Bundesverfassungsrecht enthält ein selbständiges von Art8 EMRK verschiedenes Grundrecht auf Datenschutz. Die Verfassungsbestimmung des §1 DSG 2000 räumt jeder natürlichen und juristischen Person einen Anspruch auf Geheimhaltung der sie betreffenden personenbezogenen Daten ein, soweit ein schutzwürdiges Interesse daran besteht (§1 Abs1 DSG 2000, siehe oben II.4.).

§1 Abs2 DSG 2000 enthält einen materiellen Gesetzesvorbehalt, der die Grenzen für Eingriffe in das Grundrecht enger zieht, als dies Art8 Abs2 EMRK tut. Abgesehen von der Verwendung von personenbezogenen Daten im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art8 Abs2 EMRK genannten Gründen notwendig sind.

Für die gesetzliche Grundlage verlangt §1 Abs2

DSG 2000 über Art8 Abs2 EMRK hinausgehend, dass die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorgesehen werden darf und dass gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen gesetzlich festgelegt werden. Explizit ordnet diese Bestimmung schließlich an, dass auch im Falle zulässiger Beschränkungen der Eingriff in das Grundrecht "jeweils nur in der gelindesten, zum Ziel führenden Art"

vorgenommen werden darf. Nach der Rechtsprechung des Verfassungsgerichtshofes folgt aus dieser Regelung, dass an die Verhältnismäßigkeit des Eingriffs in das Datenschutzgrundrecht ein strengerer Maßstab angelegt werden muss, als er sich bereits aus Art8 EMRK ergibt (VfSlg. 16.369/2001, 18.643/2008).

3.2. In den Anträgen wird die Verhältnismäßigkeit der in der Vorratsdatenspeicherungsrichtlinie vorgesehenen Speicherungspflichten von mindestens sechs Monaten mit Blick auf Art8 Grundrechte-Charta bestritten.

Wenn diese Bedenken gegen die Pflicht zur Speicherung an sich zutreffen sollten, dann würde das Unionsrecht die Umsetzung einer Richtlinie fordern, die als Bestandteil des Sekundärrechts Vorrang (auch) gegenüber dem Verfassungsrecht (VfSlg. 15.427/1999) und damit gegenüber dem Grundrecht nach §1 DSG 2000 genösse, sofern der österreichische Gesetzgeber die Richtlinie nur in einer das Grundrecht verletzenden Weise umsetzen könnte. Da der Gesetzgeber aber in einem solchen Fall insoweit keinen Spielraum zu einer verfassungskonformen Umsetzung der Richtlinie hätte, wäre dem Verfassungsgerichtshof wegen des Vorrangs der Richtlinie vor dem innerstaatlichen Datenschutzgrundrecht eine Prüfung des §102a TKG 2003 am Maßstab des §1 DSG 2000 verwehrt.

3.3. Aber auch der Inhalt des Grundrechts des Art8 Grundrechte-Charta, der ebenfalls zum Prüfungsmaßstab des Verfassungsgerichtshofes gehört, hängt nicht nur vom Inhalt der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, sondern insofern auch von der Gültigkeit der Vorratsdatenspeicherungsrichtlinie ab, als die Richtlinie im Sinne des Art52 Abs3 letzter Satz Grundrechte-Charta mitbestimmend dafür ist, ob das Recht der Union weitergehenden Schutz gewährleistet, der bei der Bestimmung von Bedeutung und Tragweite des Grundrechts auf Datenschutz zu berücksichtigen wäre. Dass die Beantwortung der Auslegungsfragen zu Art8 Grundrechte-Charta unmittelbare Auswirkungen auf die Entscheidung des Verfassungsgerichtshofes hat, bedarf keiner weiteren Begründung.

3.4. Die Vereinbarkeit der Richtlinie mit der Grundrechte-Charta und die Fragen der Auslegung des Art8 Grundrechte-Charta sind auch noch nicht durch die Rechtsprechung des Gerichtshofes der Europäischen Union geklärt. Dieser hatte zwar bereits über die Gültigkeit der Vorratsdatenspeicherungsrichtlinie zu entscheiden. Die entsprechende Klage bezog sich jedoch nur auf die Wahl der Rechtsgrundlage und nicht auf eine eventuelle Verletzung der Grundrechte in Zusammenhang mit der Vorratsdatenspeicherungsrichtlinie (EuGH 10.2.2009, Rs. C-301/06, Irland/Europäisches Parlament u. Rat, Slg. 2009, I-00593).

4. Folgende Überlegungen haben den Verfassungsgerichtshof dazu bewogen, ein Vorabentscheidungsersuchen an den Gerichtshof der Europäischen Union zu richten:

4.1. Nach Art8 Abs1 Grundrechte-Charta hat jede

Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Diese Daten dürfen gem. Abs2 leg.cit. 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. Soweit die Grundrechte-Charta Rechte enthält, die den durch die EMRK garantierten Rechten entsprechen, haben sie gem. Art52 Abs3 Grundrechte-Charta die gleiche Bedeutung und Tragweite, wie sie ihnen in der EMRK verliehen wird.

Der Verfassungsgerichtshof verkennt nicht die Bedeutung und das Gewicht der mit der Vorratsdatenspeicherungsrichtlinie verfolgten Ziele der Harmonisierung der Pflichten der Diensteanbieter bzw. Netzbetreiber im Zusammenhang mit der Vorratsdatenspeicherung bestimmter Daten und der Gewährleistung, dass diese Daten zum Zweck der Ermittlung, Feststellung und Verfolgung von schweren Straftaten zur Verfügung stehen. Auch verweist der Verfassungsgerichtshof darauf, dass die Mitgliedstaaten in Art4 Vorratsdatenspeicherungsrichtlinie verpflichtet werden, unter Berücksichtigung u.a. der EMRK das Verfahren und die Bedingungen festzulegen.

4.2. Ungeachtet dessen bestehen Bedenken hinsichtlich der Pflicht zur - anlasslosen - Vorratsdatenspeicherung an sich und der mit ihr notwendig verbundenen Folgen. Die Bedenken der Antragsteller gründen sich vor allem auf die hohe Eingriffsintensität der Vorratsdatenspeicherung. Diese wird durch mehrere Faktoren bestimmt. Zunächst enthält die Richtlinie einen zeitlichen Rahmen für die Speicherungsfristen, der von sechs Monaten bis zu zwei Jahren reicht. Diese Frist ist unter Berücksichtigung des Umfangs der zu speichernden Daten zu beurteilen. Nach vorläufiger Auffassung des Verfassungsgerichtshofes begegnet die Speicherungsfrist erheblichen Bedenken.

4.3. Sodann begründet der Umfang der Vorratsdatenspeicherung Bedenken, ob diese mit der Grundrechte-Charta konform geht. Die Richtlinie ermöglicht die massenhafte Sammlung von Daten sowohl in Bezug auf den Kreis der Daten, mögen sie auch auf einen Katalog von Verkehrsdaten begrenzt sein, als auch in Bezug auf den nicht eingeschränkten Personenkreis sowie im Zusammenhang mit den staatlichen Aufgaben, für die sie angeordnet wird. Die "Streubreite" des Eingriffs übertrifft damit jene der bisher in der Rechtsprechung des Verfassungsgerichtshofes zu beurteilenden Eingriffe in das Grundrecht auf Datenschutz, wobei auch die Möglichkeiten der Verknüpfung von in unterschiedlichen Zusammenhängen ermittelten Daten zu berücksichtigen sind (Berka, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, Gutachten,

18. Österreichischer Juristentag, 2012, 76 und 111 f.).

4.4. Die Vorratsdatenspeicherung erfasst darüber

hinaus fast ausschließlich Personen, die keinerlei Anlass für die Datenspeicherung gegeben haben. Gleichzeitig werden sie - unabhängig von einer konkreten Ausgestaltung der Datenverwendung - durch den nationalen Gesetzgeber - notwendigerweise - einem erhöhten Risiko ausgesetzt sein, nämlich dass Behörden ihre Daten ermitteln, ihren Inhalt zur Kenntnis nehmen und sich damit über privates Verhalten solcher Personen informieren und diese Daten für andere Zwecke weiterverwenden (etwa als Folge der zufälligen Anwesenheit in einer bestimmten Funkzelle zu einem Zeitpunkt, der für Ermittlungen der Behörde relevant ist).

4.5. Hinzu kommt das erhöhte Risiko des Missbrauchs. In diesem Zusammenhang ist insbesondere zu beachten, dass die in der Vorratsdatenspeicherungsrichtlinie - und damit auch in dem in Umsetzung der Vorratsdatenspeicherungsrichtlinie ergangenen §102a TKG 2003 - vorgesehene Verpflichtung zur Speicherung von personenbezogenen Daten über die bisherige, im Zusammenhang mit der Verrechnung von Endkunden- oder Vorleistungsentgelten vorgesehene Erlaubnis zur Speicherung von Verkehrsdaten hinausgeht. Angesichts der Vielzahl der Anbieter von Telekommunikationsdienstleistungen und damit von Speicherungsverpflichteten hat ein nicht überblickbarer Kreis von Personen Zugriff auf gemäß der Vorratsdatenspeicherungsrichtlinie auf Vorrat für mindestens sechs Monate zu speichernde Verkehrsdaten. Die Sicherung vor Missbrauch dürfte ungeachtet der Anstrengungen des nationalen Gesetzgebers vor allem deshalb auf "strukturelle Grenzen" stoßen, weil auch kleinere Diensteanbieter erfasst werden, die im Hinblick auf Sicherungen vor Missbrauch schon allein wegen ihrer geringeren Größe nur begrenzt leistungsfähig sind (explizit BVerfG, 2.3.2010, 1 BvR 256/08 ua., Rz 212).

Nicht zuletzt auch im Hinblick auf Zweifel an der Eignung zur Zielerreichung erscheint der damit verbundene Eingriff unverhältnismäßig.

5. Der Verfassungsgerichtshof sieht sich durch die Ausgangsverfahren veranlasst, auch Fragen zur Auslegung des Art8 der Grundrechte-Charta an den Gerichtshof der Europäischen Union zu richten (vgl. VfGH 14.3.2012, U466/12 ua.). Sie betreffen das Verhältnis des Grundrechts zum Unionsrecht einschließlich des Sekundärrechts, zur EMRK und zu den Verfassungen der Mitgliedstaaten.

5.1. Art52 Abs7 Grundrechte-Charta ordnet an, dass die Erläuterungen auch von den Gerichten der Union zu berücksichtigen sind. In den Erläuterungen zu Art8 Grundrechte-Charta heißt es, dass dieser sich auf Art286 EGV und auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr sowie auf Art8 EMRK und das Übereinkommen des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, das von allen Mitgliedstaaten ratifiziert wurde, stützte und dass nunmehr Art286 EGV durch Art16 AEUV und Art39 EUV ersetzt werde. Ferner wird auf die Verordnung (EG) Nr. 45/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr verwiesen. Die Richtlinie und die Verordnung enthalten Bedingungen und Beschränkungen für die Wahrnehmung des Rechts auf den Schutz personenbezogener Daten (vgl. Erläuterungen zur Grundrechte-Charta, ABl. 2007 C 303, 20).

Es erscheint dem Verfassungsgerichtshof vorderhand nicht geklärt, in welchem Verhältnis das in den Erläuterungen ausdrücklich verwiesene Sekundärrecht zu den in den Art8 Abs2 und Art52 Abs1 und 3 Grundrechte-Charta enthaltenen Schranken (Frage 2.1.) bzw. zu Richtlinien im selben Regelungsbereich (Fragen 2.2. und 2.3.) steht.

5.2. Das österreichische Bundesverfassungsrecht

enthält - ebenso wie Verfassungen anderer Mitgliedstaaten - eine eigene grundrechtliche Gewährleistung für den Datenschutz in §1 DSG 2000. Nach Art53 Grundrechte-Charta wird das Schutzniveau nach der Grundrechte-Charta u.a. auch von den Verfassungen der Mitgliedstaaten mitbestimmt. Mit der Frage 2.4. soll geklärt werden,

ob diese Rechte für den Fall, dass sie weitergehenden Schutz gewähren als Art8 Grundrechte-Charta, bei der Beurteilung von Handlungen der Mitgliedstaaten in Durchführung von Unionsrecht bzw. der Gültigkeit von Sekundärrecht den Schranken vorgehen, die sich aus der Grundrechte-Charta selbst ergeben. Der Verfassungsgerichtshof geht davon aus, dass im Anwendungsbereich der Grundrechte-Charta zwar nicht ein einzelnes Grundrecht der Verfassung eines einzigen Mitgliedstaates maßgeblich sein und die uneingeschränkte Anwendbarkeit des Charta-Grundrechts beseitigen kann (vgl. SA Bot, 2.10.2012, Rs. C-399/11, Melloni, Rz 96 ff.). Wohl aber kann ein höheres Schutzniveau als jenes nach der Grundrechte-Charta, das sich aus einem wertenden Rechtsvergleich der Verfassungen der Mitgliedstaaten ergibt, maßgeblich sein und dazu zwingen, die einschlägige Garantie der Grundrechte-Charta so auszulegen, dass der Grundrechtsstandard der mitgliedstaatlichen Verfassungen nicht unterschritten wird.

Diese Ansicht wird letztlich auch dadurch gestützt, dass Art52 Abs4 Grundrechte-Charta ausdrücklich anordnet, dass Grundrechte, die in der Charta anerkannt werden und sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ergeben, im Einklang mit diesen Überlieferungen auszulegen sind (vgl. im Übrigen auch Art6 Abs3 EUV). Auch wenn nicht jede mitgliedstaatliche Verfassung ein eigenes Datenschutzgrundrecht enthält, so ist dennoch - nicht zuletzt im Hinblick auf die Rechtsprechung der Verfassungsgerichte der Mitgliedstaaten - davon auszugehen, dass das Grundrecht auf Datenschutz nicht nur in den Verfassungsüberlieferungen der Mitgliedstaaten enthalten ist, sondern auch zu den Menschenrechten und Grundrechten iSd Art53 Grundrechte-Charta gehört, die durch die Verfassungen der Mitgliedstaaten anerkannt werden (siehe beispielhaft neben §1 DSG 2000 den Art51 Abs2 Polnische Verfassung oder das aus Art2 Abs1 des deutschen Grundgesetzes abgeleitete Recht auf informationelle Selbstbestimmung).

5.3. Die letzte Frage des Verfassungsgerichtshofes (Frage 2.5.) ist auf die Klärung der Bedeutung der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte zu Art8 EMRK gerichtet. Diese enthält auch zahlreiche Urteile zu Fragen des Datenschutzes. Die Erläuterungen zu Art8 Grundrechte-Charta enthalten jedoch keinen Bezug auf Art8 EMRK. Vielmehr wird in den Erläuterungen zu Art7 Grundrechte-Charta ("Achtung des Privat- und Familienlebens") erklärt, dass dieser dem Art8 EMRK entspreche. Gemäß Art52 Abs7 Grundrechte-Charta sind die Erläuterungen zur Charta als Anleitung für die Auslegung von den Gerichten gebührend zu berücksichtigen. Abs5 der Präambel nimmt nicht nur auf die Erläuterungen des Präsidiums des Europäischen Konvents, sondern auch auf die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte ausdrücklich Bezug. Angesichts dessen erscheint es klärungsbedürftig, inwieweit die Rechtsprechung zu Art8 EMRK bei der Auslegung nicht nur des Art7, sondern auch des Art8 Grundrechte-Charta zu berücksichtigen ist.

V.

1. Aus diesen Gründen fasst der Verfassungsgerichtshof den Beschluss, die Frage nach der Gültigkeit der Art3 bis 9 Vorratsdatenspeicherungsrichtlinie sowie die im Spruch genannten Fragen zur Auslegung des Art8 Grundrechte-Charta dem Gerichtshof der Europäischen Union zur Vorabentscheidung vorzulegen.

2. Die Verfahren werden - mit Ausnahme von

Handlungen, Entscheidungen und Verfügungen gem. §19a Abs1 VfGG - nach Vorliegen der Entscheidung des Gerichtshofs der Europäischen Union fortgesetzt werden.

3. Dies konnte gemäß §19 Abs4 erster Satz VfGG ohne mündliche Verhandlung in nichtöffentlicher Sitzung beschlossen werden.