G 47/2012-49, G 59/2012-38, G 62/2012-46,
G 70/2012-40, G 71/2012-36
27. Juni 2014

IM NAMEN DER REPUBLIK!

Der Verfassungsgerichtshof hat unter dem Vorsitz des Präsidenten
Dr. Gerhart HOLZINGER,

in Anwesenheit der Vizepräsidentin
Dr. Brigitte BIERLEIN

und der Mitglieder
Dr. Sieglinde GAHLEITNER,
DDr. Christoph GRABENWARTER,
Dr. Christoph HERBST,
Dr. Michael HOLOUBEK,
Dr. Helmut HÖRTENHUBER,
Dr. Claudia KAHR,
Dr. Georg LIENBACHER,
Dr. Rudolf MÜLLER,
Dr. Johannes SCHNIZER und
Dr. Ingrid SIESS-SCHERZ

als Stimmführer, im Beisein des Schriftführers
Mag. Christian SIMON,

über die Anträge 1. der KÄRNTNER LANDESREGIERUNG auf Aufhebung näher bezeichneter Bestimmungen des Telekommunikationsgesetzes 2003, BGBl. I 70/2003 idF BGBl. I 27/2011 (protokolliert zu G 47/2012), 2. des Mag. Michael SEITLINGER, LL.M., (…) , vertreten durch die Brauneis Klauser Prändl Rechtsanwälte GmbH, Bauernmarkt 2, 1010 Wien, auf Aufhebung näher bezeichneter Bestimmungen des Telekommunikationsgesetzes 2003, BGBl. I 70/2003 idF BGBl. I 102/2011, in eventu auch Bestimmungen der Strafprozeßordnung 1975, BGBl. 631 idF BGBl. I 35/2012, und des Sicherheitspolizeigesetzes, BGBl. 566/1991 idF BGBl. I 13/2012 (protokolliert zu G 59/2012), und 3. des Ing. Dr. Christof TSCHOHL, (…) , vertreten durch die Scheucher Rechtsanwalt GmbH, Lindengasse 39, 1070 Wien, auf Aufhebung näher bezeichneter Bestimmungen des Telekommunikationsgesetzes 2003, BGBl. I 70/2003 idF BGBl. I 102/2011, der Strafprozeßordnung 1975, BGBl. 631 idF BGBl. I 53/2012, und des Sicherheitspolizeigesetzes, BGBl. 566/1991 idF BGBl. I 13/2012 (protokolliert zu G 62,70,71/2012), als verfassungswidrig, nach Vorlage von Fragen an den Gerichtshof der Europäischen Union zur Vorabentscheidung gemäß Art. 267 AEUV, nach der am 12. Juni 2014 durchgeführten öffentlichen mündlichen Verhandlung, nach Anhörung des Vortrages des Berichterstatters und der Ausführungen des Vertreters der antragstellenden Landesregierung Dr. Edmund Primosch, des Zweitantragstellers Mag. Michael Seitlinger, LL.M., und seines Vertreters Rechtsanwalt Dr. Gerald Otto, LL.M., des Drittantragstellers Ing. Dr. Christof Tschohl und seines Vertreters Rechtsanwalt Mag. Ewald Scheucher sowie der Vertreter der Bundesregierung, SC Dr. Gerhard Hesse, SC Mag. Christian Pilnacek, MR Dr. Christian Singer und OR Mag. Verena Weiss, gemäß Art. 140 B-VG zu Recht erkannt und am heutigen Tage verkündet:

I. Im Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 – TKG 2003), BGBl. I Nr. 70/2003 in der Fassung BGBl. I Nr. 27/2011, werden folgende Bestimmungen als verfassungswidrig aufgehoben:

   – § 92 Abs. 3 Z 6b;

– in § 93 Abs. 3 die Wortfolge "einschließlich Vorratsdaten";

– in § 94 Abs. 1 die Wortfolge "einschließlich der Auskunft über Vorratsdaten";

– in § 94 Abs. 2 die Wortfolge "einschließlich der Auskunft über Vorratsdaten";

– in § 94 Abs. 4 die Wortfolgen "einschließlich der Übermittlung von Vorratsdaten," und "sowie die näheren Bestimmungen betreffend die Speicherung der gemäß § 102c angefertigten Protokolle";

– in § 98 Abs. 2 die Wortfolge ", auch wenn hiefür ein Zugriff auf gemäß § 102a Abs. 3 Z 6 lit. d gespeicherte Vorratsdaten erforderlich ist";

– in § 99 Abs. 5 Z 2 die Wortfolge ", auch wenn diese als Vorratsdaten gemäß § 102a Abs. 2 Z 1, Abs. 3 Z 6 lit. a und b oder § 102a Abs. 4 Z 1, 2, 3 und 5 längstens sechs Monate vor der Anfrage gespeichert wurden,";

– in § 99 Abs. 5 Z 3 die Wortfolge ", auch wenn hiefür ein Zugriff auf gemäß § 102a Abs. 3 Z 6 lit. d gespeicherte Vorratsdaten erforderlich ist";

– in § 99 Abs. 5 Z 4 die Wortfolgen "auch" und "als Vorratsdaten gemäß § 102a Abs. 2 Z 1 oder § 102a Abs. 4 Z 1, 2, 3 und 5";

– § 102a;

– § 102b;

– § 102c Abs. 2, 3 und 6;

– in § 109 Abs. 3 die Z 22, 23, 24, 25 und 26.

II. § 134 Z 2a und § 135 Abs. 2a der Strafprozeßordnung 1975 (StPO), BGBl. Nr. 631, in der Fassung BGBl. I Nr. 33/2011, werden als verfassungswidrig aufgehoben.

III. Im Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz – SPG), BGBl. Nr. 566/1991, werden folgende Bestimmungen aufgehoben:

– In § 53 Abs. 3a Z 3 in der Fassung BGBl. I Nr. 33/2011, die Wortfolge "auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 4 iVm § 102a TKG 2003 erforderlich ist,";

– in § 53 Abs. 3b in der Fassung BGBl. I Nr. 13/2012, die Wortfolge ", auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 iVm § 102a TKG 2003 erforderlich ist,";

IV. Frühere gesetzliche Bestimmungen treten nicht wieder in Kraft.

V. Der Bundeskanzler ist zur unverzüglichen Kundmachung dieser Aussprüche im Bundesgesetzblatt I verpflichtet.

VI. Der Antrag der KÄRNTNER LANDESREGIERUNG zu G 47/2012 wird zurückgewiesen.

VII. Der Antrag des Mag. Michael SEITLINGER, LL.M., zu G 59/2012 wird zurückgewiesen, soweit er sich gegen § 1 Abs. 4 Z 7 des Bundesgesetzeses, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 – TKG 2003), BGBl. I Nr. 70/2003, in der Fassung BGBl. I Nr. 102/2011, und gegen § 102c Abs. 1, 4 und 5 des Bundesgesetzes, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 – TKG 2003), BGBl. I Nr. 70/2003 in der Fassung BGBl. I Nr. 27/2011, richtet.

VIII. Der Antrag des Ing. Dr. Christof TSCHOHL zu G 62,70,71/2012 wird zurückgewiesen, soweit er sich gegen § 102c Abs. 1, 4 und 5 des Bundesgesetzes, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 – TKG 2003), BGBl. I Nr. 70/2003 in der Fassung BGBl. I Nr. 27/2011, richtet.

IX. Im Übrigen werden die Anträge abgewiesen.

X. Der Bund (Bundesministerin für Verkehr, Innovation und Technologie) ist schuldig, dem Antragsteller zu G 59/2012 zuhanden seines Rechtsvertreters die mit € 3.697,76 bestimmten Prozesskosten binnen 14 Tagen bei sonstiger Exekution zu ersetzen und dem Antragsteller zu G 62,70,71/2012 zuhanden seines Rechtsvertreters die mit € 2.620,-- bestimmten Prozesskosten binnen 14 Tagen bei sonstiger Exekution zu ersetzen.

Entscheidungsgründe

I. Anträge und Vorverfahren

1. Der Antrag zu G 47/2012: 1

1.1. Die Kärntner Landesregierung (in der Folge: die antragstellende Landesregierung) stellt auf Grund ihres Beschlusses vom 27. März 2012 gemäß Art. 140 Abs. 1 B-VG iVm §§ 62 ff. VfGG den Antrag, 2

"[d]ie Bestimmungen der […]
§ 90 Abs. 6, Abs. 7 bis 8,
§ 92 Abs. 3 Z 2a bis 2b, Abs. 3 Z 3 lit. a bis c, Abs. 3 Z 6a bis 6b, Abs. 3 Z 8, Abs. 3 Z 8a,
§ 93 Abs. 5,
§ 94 Abs. 1 bis 2, Abs. 3, Abs. 4,
§ 98 Abs. 2,
§ 99 Abs. 1, Abs. 5 Z 1 bis 4,
§ 102a Abs. 1 bis 7, Abs. 8,
§ 102b Abs. 1, Abs. 2, Abs. 3,
§ 102c Abs. 1, Abs. 2
TKG 2003 idF BGBl. I 2011/27 zur Gänze aufzuheben."

1.2. Begründend führt die antragstellende Landesregierung im Wesentlichen aus, dass der Nationalrat die Novellierung des Telekommunikationsgesetzes 2003 (TKG 2003) beschlossen habe und diese Novelle am 18. Mai 2011 durch das BGBl. I 27/2011 kundgemacht worden sei. Die Novelle habe der Umsetzung der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt und verarbeitet werden, und zur 3

Änderung der Richtlinie 2002/58/EG (im Folgenden: Vorratsdatenspeicherungsrichtlinie) gedient. Durch die Novelle werde eine flächendeckende und verdachtsunabhängige Vorratsdatenspeicherung für das gesamte Bundesgebiet vorgesehen. Ziel der Vorratsdatenspeicherungsrichtlinie sei – ausweislich der Erwägungsgründe 5 bis 9 der Richtlinie – die verdachtsunabhängige Speicherung des Telefon- und Internetverkehrs sowie von Standortdaten über jede einzelne "telekommunikative" Verbindung. Ausgehend davon seien die bekämpften Bestimmungen aus den im Folgenden näher angeführten Gründen verfassungswidrig:

1.3. Neben einem "Verstoß gegen Bauprinzipien der Verfassung", der sich aus dem Umstand ergebe, dass die bekämpften Rechtsvorschriften "in ihrer Gesamtheit gegen den Baustil eines modernen Staates" verstießen, macht die antragstellende Landesregierung einen "massiven Eingriff in die Grundrechte, insbesondere das Gebot der Achtung der Privatsphäre des Art. 8 EMRK, das Grundrecht auf Datenschutz des [§] 1 DSG, das Fernmeldegeheimnis des Art. 10a StGG, das Kommunikationsgeheimnis des § 93 TKG, das Recht auf freie Meinungsäußerung der Art. 10 EMRK und Art. 13 StGG, die Unschuldsvermutung des Art. 6 Abs. 2 EMRK" geltend. Die Speicherung von Kommunikationsdaten greife in grob unverhältnismäßiger Weise in diese Grundrechte ein. Die "Verletzung der Grundrechte" entstehe nicht erst durch die Nutzung der gespeicherten Daten, sondern bereits durch die gesetzliche Anordnung der fortwährenden und pauschalen Speicherung von Kommunikationsdaten. 4

1.4. Unter "Kritikpunkte an einzelnen Paragraphen des TKG" werden im Antrag die §§ 90 Abs. 6 bis Abs. 8, 92 Abs. 3 Z 2a bis Z 3 lit. c, Z 6a und Z 6b, Z 8a und Z 8b, 93 Abs. 5, 94, 98 Abs. 2, 99 Abs. 1, 99 Abs. 5, 102a, 102b und 102c TKG 2003 mit umfangreichen Anmerkungen versehen. Mehrfach wird vorgebracht, bestimmte in den angeführten Bestimmungen verwendete Begriffe seien "unklar und unpräzise" (so zB zum Begriff der Standortkennung in § 90 Abs. 8 TKG 2003), "widersprüchlich und unpräzise" (zu § 92 Abs. 3 Z 3 lit. a bis c TKG 2003) oder "unbestimmt, unpräzise" (zu §§ 92 Abs. 3 Z 6b, 94 Abs. 3 TKG 2003). Durch die angeführten Bestimmungen ergäben sich "massive" bzw. "gravierende Eingriffe" (zB im Falle der §§ 90 Abs. 6 bis 8, 92 Abs. 3 Z 8, 93 5

Abs. 5, 94 Abs. 3 und 4, 99 Abs. 1, 102b Abs. 3 TKG 2003) in Grundrechte. Auch die übrigen der angeführten Bestimmungen seien grundrechtswidrig bzw. verstießen gegen das Bestimmtheitsgebot des Art. 18 B-VG.

1.5. Im Rahmen der Ausführungen zu § 102a TKG 2003 wird vorgebracht, dass die Daten, deren Speicherung durch § 102a Abs. 3 Z 3 bis 5 TKG 2003 angeordnet werde, jedenfalls personenbezogene Daten iSd § 1 DSG 2000 darstellten. Diese dürften, da jedermann einen Anspruch auf Geheimhaltung dieser Daten habe, nicht gespeichert werden. 6

Die in § 102a Abs. 2 bis 4 TKG 2003 vorgesehene Speicherung von Daten sei nicht das gelindeste, zum Ziel führende Mittel iSd § 1 Abs. 2 DSG 2000. Zusammengefasst stehe § 102a TKG 2003 in Widerspruch zur Verfassungsbestimmung des § 1 DSG 2000. Überdies werde dadurch, dass die Identität der Gesprächspartner, die Dauer der Gespräche, die Uhrzeit und dergleichen aufgezeichnet und gespeichert würden, in das in Art. 8 EMRK verankerte Grundrecht auf Achtung des Privat- und Familienlebens eingegriffen. Dieser Eingriff sei untauglich, nicht erforderlich und unverhältnismäßig. 7

2. Die Bundesregierung erstattete eine Äußerung zum Antrag der Kärntner Landesregierung, in der den im Antrag erhobenen Bedenken entgegengetreten wird: 8

2.1. Im Rahmen eines abstrakten Gesetzesprüfungsverfahrens nach Art. 140 B-VG habe der Antrag die gegen die Verfassungsmäßigkeit des Gesetzes sprechenden Bedenken im Einzelnen darzulegen (§ 62 Abs. 1 VfGG). Dies sei im Antrag oftmals nicht der Fall. An vielen Stellen des Antrags werde zwar die Behauptung einer Verfassungswidrigkeit aufgestellt, diese erfolge jedoch zumeist ohne nähere Begründung oder Darlegung. Es sei Sache der antragstellenden Landesregierung, die jeweiligen Bedenken den verschiedenen Aufhebungsbegehren zuzuordnen. Es könne nicht Aufgabe des Verfassungsgerichtshofes sein, pauschal vorgetragene Bedenken einzelnen Bestimmungen zuzuordnen. 9

2.2. In weiterer Folge weist die Bundesregierung darauf hin, dass die Regelungen des TKG 2003 gemeinsam mit korrespondierenden Bestimmungen über die Vorrausetzungen der Datenverwendung und Datenanfrage der Strafprozeßord- 10

nung 1975 (StPO) aber auch des Sicherheitspolizeigesetzes (SPG) zu sehen seien. Eine gesonderte Betrachtung der Bestimmungen des TKG 2003 greife zu kurz, um die Rechtmäßigkeit des jeweiligen Grundrechtseingriffs zu beurteilen. Des Weiteren orientiere sich der Antrag offenbar ausschließlich am Text jenes Bundesgesetzblattes, mit dem die Novelle des TKG 2003 zur Einführung der Vorratsdatenspeicherung kundgemacht wurde (BGBl. I 27/2011). Dies stelle nur einen kleinen Teil des gesamten TKG 2003 dar und könne isoliert nur schwer sinnerfassend gelesen werden. Der Antrag ignoriere an einigen Stellen, dass für die Beurteilung der Verfassungskonformität einer Rechtsvorschrift der Gesamtzusammenhang heranzuziehen sei und dass einige kritisierte Aspekte bereits in vorherigen Fassungen des TKG 2003 (wie etwa die Ausführungen zu § 92 Abs. 3 Z 3 TKG 2003) und nicht im novellierten Text geregelt gewesen seien.

Die Bundesregierung gelangt zur Auffassung, dass im Antrag der Kärntner Landesregierung die Gründe der behaupteten Verfassungswidrigkeiten nicht präzise genug umschrieben und viele der dargelegten Bedenken nicht schlüssig bzw. überprüfbar seien. Aus dem Antrag lasse sich nicht mit hinreichender Deutlichkeit entnehmen, zu welchen Rechtsvorschriften die zur Aufhebung beantragten Normen in Widerspruch stünden bzw. welche Gründe für diese Thesen sprächen. Vor diesem Hintergrund sei der Antrag nach Auffassung der Bundesregierung zurückzuweisen. 11

2.3. Für den Fall der Zulässigkeit des Antrags erwidert die Bundesregierung in der Sache zunächst, dass im Antrag offenbar davon ausgegangen werde, dass jede behauptete Ungenauigkeit oder Unzweckmäßigkeit, jedes Ermessen oder jeder sonstige behauptete Mangel die Verletzung von Verfassungsbestimmungen bewirke. Auch werde jede Beschränkung eines Grundrechts bzw. jeder Eingriff in ein Grundrecht mit einer Verletzung desselben gleichgesetzt. Diese Auffassung der antragstellenden Landesregierung sei unrichtig. 12

Die in der Folge relevanten Ausführungen der Bundesregierung werden wörtlich wiedergegeben: 13

"3.1. Zur behaupteten Verletzung des Grundrechtes auf Achtung der Privatsphäre

Die Antragstellerin ortet in der im TKG 2003 vorgesehenen Vorratsdatenspeicherung einen Verstoß gegen das in Art. 8 EMRK verbriefte Recht auf Achtung des Privatlebens. Diesem Vorbringen sind folgende Argumente entgegen zu halten:

Das Recht auf Achtung des Privatlebens soll dem Einzelnen einen privaten Bereich sichern, in dem er seine Persönlichkeit frei entwickeln und entfalten kann. Es gewährleistet einen umfassenden Schutz der unmittelbaren Persönlichkeitssphäre: Hieraus folgt, dass u.a. auch der Schutz von persönlichen Daten zu einem wichtigen Teilbereich der Gewährleistungen des Art. 8 EMRK zählt.

Im Fall der gegenständlichen Vorratsdatenspeicherung liegt durch das systematische Sammeln bzw. Speichern von Informationen (genauer gesagt Verkehrs- und Standortdaten) zweifelsfrei ein Eingriff in Art. 8 EMRK vor. Allerdings ist dieser Eingriff gerechtfertigt: Denn der gesetzlich vorgesehene Eingriff stellt eine Maßnahme dar, die nach Art. 8 Abs. 2 EMRK 'in einer demokratischen Gesellschaft für (...) die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen notwendig ist.' Überdies werden die vom Europäischen Gerichtshof für Menschenrechte (EGMR) etwa im Fall Rotaru (vgl. EGMR, Urteil vom 4. Mai 2000, Rotaru/Rumänien, Nr. 28341/95, Z. 57 et seq.) aufgestellten 'Voraussetzungen' für eine ordnungsgemäße Datenspeicherung bzw. -verarbeitung – was in der Rechtssache Rotaru nicht der Fall war – allesamt erfüllt […]:

1. Die vorhandene gesetzliche Grundlage im TKG 2003 ist ausreichend, da die Grenzen der Befugnisse der Telekommunikationsbetreiber zur Informationssammlung und -verarbeitung, etwa durch genaue Definitionen der auf Vorrat zu speichernden Daten (vgl. hierzu die Erläuterungen - Allgemeiner Teil, RV 1074 BlgNR XXIV. GP) festgelegt sind.

2. Im TKG 2003 wird geregelt, welche Informationen gesammelt und aufbewahrt werden können sowie unter welchen Voraussetzungen und nach welchen Verfahren dies erfolgen kann (vgl. etwa § 99 Abs. 5 TKG 2003, der die Zulässigkeit der Verarbeitung von Verkehrsdaten zu Auskunftszwecken regelt).

3. Die zulässige Dauer der Aufbewahrung ist (auf sechs Monate) befristet.

4. Ein Verfahren zur Sicherung der Rechte des Betroffenen und zur Kontrolle der Behörden ist vorhanden (vgl. etwa § 102c Abs. 1 TKG 2003).

Ferner wird bemerkt, dass bei der Verpflichtung zur Speicherung von Telekommunikationsverkehrsdaten durch private Diensteanbieter keine Erstellung von Personenprofilen oder gar die Sichtbarmachung von sozialen Geflechten, priva-

ten und beruflichen Kontakten erfolgt. Es wird lediglich eine Pflicht für diese Anbieter zur Aufbewahrung bestimmter Daten mit dem Ziel statuiert, einen späteren justiziellen oder sicherheitspolizeilichen Zugriff darauf zu ermöglichen. Die Daten werden somit für ein halbes Jahr einem Löschungsanspruch der Betroffenen entzogen. Kommunikationsinhalte sind in diesem Zusammenhang von der Speicherung nicht betroffen. Der Vollständigkeit halber sei erwähnt, dass selbst diese Daten (Inhalte), deren Speicherung und Verwendung wohl einen ungleich größeren Grundrechtseingriff darstellt, etwa gemäß § 135 Abs. 3 StPO unter bestimmten Voraussetzungen gespeichert werden dürfen.

Die bloße Speicherverpflichtung von Verkehrs- und Standortdaten stellt damit vor dem Hintergrund der möglichen Inhaltsüberwachung keinen massiven Eingriff in Art. 8 EMRK dar und ist auch im Hinblick auf den angestrebten Zweck der [Vorratsdatenspeicherungsrichtlinie], nämlich die Ermittlung, Feststellung und Verfolgung von schweren Straftaten, nicht unverhältnismäßig (vgl. etwa Art. 1 Abs. 1 der [Vorratsdatenspeicherungsrichtlinie]). Die bloße Möglichkeit der Umgehung von Telefonie- oder Internetkommunikation im Zuge von kriminellen Aktivitäten indiziert ebenso wenig die Unangemessenheit der Maßnahme, weil die überwiegende Mehrzahl der Kommunikationsvorgänge auch weiterhin über konventionelle, das heißt von der Speicherpflicht erfasste Wege erfolgt. Auch die Ausnahme von der Speicherpflicht für Unternehmen, die unter einer bestimmten Umsatzschwelle liegen, ändert daran nichts, da auch in diesem Fall Verhältnismäßigkeitsüberlegungen vorzunehmen waren […].

Des Weiteren sei festgehalten, dass die Auswertung von Verkehrsdaten für die Strafverfolgung unverzichtbar ist. Insbesondere können daraus Anhaltspunkte zu Tatzeitpunkt, zu Aufenthalten von Verdächtigen in Tatortnähe, zum Vor- und Nachtatverhalten von Tatverdächtigen, zu Verbindungen der Tatverdächtigen untereinander, zum Verlauf von Fluchtwegen und zur Ermittlung weiterer Tatverdächtiger gewonnen werden. Verkehrsdaten kommt darüber hinaus bei der Verifizierung von Beschuldigtenverantwortungen oder bei der Ermittlung des Aufenthaltsorts von Beschuldigten Bedeutung zu. So kann zB die Aufklärung der Verbreitung kinderpornografischer Darstellungen im Internet praktisch nur anhand von Verkehrsdaten erfolgen. Bei banden- oder gewerbsmäßig begangenen Straftaten ist die Kenntnis des Kommunikationsverhaltens für die Aufklärung von Organisationsstrukturen und Serientaten unerlässlich. Nicht zuletzt hat ein Gutachten des Max-Planck-Institutes zum Thema 'Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten' als eine Art Bestandaufnahme der Situation im Bereich der Verkehrsdatenabfrage seit dem Urteil des deutschen Bundesverfassungsgerichtes vom 2. März 2010 zur Vorratsdatenspeicherung in einer Gesamtschau nicht ausgeschlossen […], dass in komplexen Verfahren und bei Kapitaldelikten Verkehrsdaten wichtige Beweismittel darstellen oder zusätzliche

Ermittlungsansätze schaffen. Zudem ist die Dauer von sechs Monaten in Anbetracht komplexer krimineller Strukturen und oftmals nötiger umfangreicher Ermittlungen ohnehin ein sehr niedriger Ansatz. Gerade für den Bereich des Internets, wo durch die zunehmende Verbreitung von 'Flatrates' und dem damit weggefallenen betrieblichen Speicherungszweck von Verkehrsdaten ein Schlupfloch für Kriminalität aller Art entstehen kann, kann dieser Entwicklung durch die Verpflichtung zur Vorratsdatenspeicherung begegnet werden.

[…]

3.5. Zu den Bedenken in Hinblick auf die Missbrauchsgefahr der Datenverwendung

Nach Auffassung der Antragstellerin führt die Vorratsdatenspeicherung zu einer Erhöhung der Gefahr missbräuchlicher Datenverwendung. Dem tritt die Bundesregierung wie folgt entgegen:

Der Antrag behauptet fest, dass das Vorhandensein von Daten die Gefahr 'neuer Begehrlichkeiten' weckt. Dabei wird jedoch übersehen, dass die Daten auch vor Einführung der Vorratsdatenspeicherung beim Betreiber tatsächlich vorhanden und im Gegensatz zur neuen Rechtslage wesentlich weniger geschützt waren.

Es ist denkunmöglich, einen Kommunikationsdienst zu erbringen, ohne dass Kommunikationsdaten anfallen. Werden diese nun länger, als dies für Verrechnung und Betrieb notwendig ist, gespeichert, ist es erforderlich, die […] dargelegte Abwägung einander widerstreitender Interessen – einerseits das öffentliche Interesse an der Strafverfolgung sowie der ersten allgemeinen Hilfeleistung, andererseits das berechtigte Interesse des Einzelnen auf Geheimhaltung seiner personenbezogenen Daten – vorzunehmen. Angesichts der Zweckbindung der Daten und der mit der Datenspeicherung verbundenen strengen Datenschutzvorkehrungen ist der Eingriff ins Grundrecht auf Datenschutz verhältnismäßig gering und wohl gerechtfertigt.

Dass gerade in der Übersendung von Protokolldaten an die Datenschutzkommission, bzw. an den Bundesminister für Justiz – diesem obliegt eine Berichterstattungspflicht gegenüber der Europäischen Kommission und dem Nationalrat – als eine Missbrauchsquelle gesehen wird, ist nicht nachvollziehbar. Denn sowohl die Datenschutzkommission als auch der Bundesminister für Justiz dienen der nachprüfenden Kontrolle der Vorratsdatenspeicherung.

Darüber hinaus verkennt die Antragstellerin, dass Protokolldaten iSd § 102c Abs. 1 TKG 2003 jedenfalls von jenen Daten, die nach § 102a TKG 2003 zu speichern sind, zu unterscheiden sind. Die Protokolldaten dienen einerseits dazu, dass Betroffene ihre Rechte nach dem DSG 2000 wahrnehmen können, und sind

andererseits notwendig, um der Verpflichtung nach Art. 10 der [Vorratsdaten-speicherungsrichtlinie] nachkommen zu können.

[…]

4. Zu den Kritikpunkten an einzelnen Bestimmungen des TKG 2003

[…]

4.3.4. Zu § 92 Abs. 3 Z 6b TKG 2003

[Im Antrag] wird vorgebracht, dass unklar sei, ob Daten, die schon bisher zu Verrechnungszwecken gespeichert wurden, Vorratsdaten sind oder nicht. Dabei wird die Systematik der Stamm-, Rechnungs-, Verkehrs- und Vorratsdaten verkannt.

Die Beschwerdeführerin moniert, dass die Bestimmungen der §§ 92 Abs. 3 Z 6b und 102a TKG 2003 bezüglich der Vorratsdaten nicht dem Determinierungsgebot entsprechen. Dazu ist Folgendes auszuführen: Die Definition des Vorratsdatums nach § 92 Abs. 3 Z 6b TKG 2003 ('die ausschließlich aufgrund der Speicherverpflichtung nach § 102a TKG gespeichert werden') ist im Zusammenhang mit § 102a TKG 2003 zu sehen. Vorratsdaten sind ab dem Zeitpunkt der Erzeugung oder Verarbeitung für maximal sechs Monate zur Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs. 2a StPO (Auskunft über Vorratsdaten) rechtfertigt, zu speichern wobei diese Speichermöglichkeit über die Berechtigung zur Datenspeicherung oder Datenverarbeitung nach den §§ 96, 97, 99, 101 und 102 TKG 2003 hinausgeht: Daher liegt ein Vorratsdatum vor, wenn keine Berechtigung zur Datenspeicherung oder Datenverarbeitung nach den genannten Bestimmungen (mehr) gegeben ist, und die Daten auf Grund der Speicherverpflichtung ausschließlich für Zwecke des § 135 Abs. 2a StPO zu speichern sind.

[…]

4.6. Zu § 94 Abs. 3 und 4 TKG 2003

§ 94 Abs. 3 TKG 2003 entspricht im Wesentlichen der vor der Novelle geltenden Rechtslage, die mit der noch geltenden Überwachungsverordnung, BGBl. II Nr. 418/2011 näher konkretisiert wurde. Abgesehen davon, dass § 94 Abs. 3 TKG 2003 selbst nur die technischen Voraussetzungen für die Datenverwendung regelt und die Verwendung an anderer Stelle zu normieren ist, geht der Antrag

offenbar (fälschlich) davon aus, dass ein einfachgesetzlicher Eingriff in ein Grundrecht per se schon verfassungsrechtlich bedenklich ist.

Ferner wird an dieser Stelle unrichtigerweise das Fehlen näherer Bestimmungen für die technischen Einrichtungen gerügt. § 94 Abs. 3 TKG 2003 legt fest, dass diese Bestimmungen dem jeweiligen Stand der Technik zu entsprechen haben. Damit wird ein Gesetzesbegriff gewählt, der jederzeit einer objektiven Auslegung zugänglich ist. Dementsprechend schreibt die Überwachungsverordnung in § 4 auch den vom European Telecommunications Standardisation Institute (ETSI) erarbeiteten Europäischen Standard ES 201 671 Version 2.1.1. vor. Damit ist ein Standard zitiert, der dem Stand der Technik entspricht.

Auch die Gesetzesbegriffe in § 94 Abs. 4 TKG 2003 lassen sich eindeutig auslegen. Der Verordnungsgeber hat eine nähere Spezifizierung mit der DSVO [Datensicherheitsverordnung] erlassen.

4.7. Zu § 98 Abs. 2 TKG 2003

Der Inhalt des § 98 Abs. 2 TKG 2003 – insbesondere was unter einem 'gefährdeten Menschen' zu verstehen ist […] – ist einer eindeutigen Auslegung zugänglich: So wird die Wortfolge 'gefährdeter Mensch' etwa bereits durch § 98 Abs. 1 TKG 2003 näher umschrieben, der u.a. auf das Bestehen eines Notfalles, der nur durch Bekanntgabe von Stamm- und Standortdaten abgewehrt werden kann, abstellt. Ziel des § 98 Abs. 2 TKG 2003 ist in einem konkreten Notfall das Auffinden eines 'gefährdeten Menschen' – dieser könnte etwa vermisst sein – durch Bekanntgabe der Standortdaten seines Mobiltelefons zu erleichtern.

Der Zulässigkeit der Auskunft über Standortdaten an Betreiber von Notrufdiensten gemäß § 98 TKG 2003 liegt eine Interessensabwägung zu Grunde, die aufgrund der bestehenden Gefährdungssituation für einen Menschen zugunsten der Übermittlung (und damit des Eingriffs) ausfällt.

[…]

4.9. Zu § 99 Abs. 5 TKG 2003

§ 99 Abs. 5 TKG 2003 stellt die Verarbeitungsermächtigung für den Anbieter von Verkehrsdaten zur Beauskunftung von bestimmten Datenkategorien nach den in den korrespondierenden spezifischen gesetzlichen Voraussetzungen der StPO bzw. des SPG dar. Z 2 leg. cit. beschränkt die Verarbeitungsermächtigung dabei zeitlich und zwar soweit die dort genannten Vorratsdaten längstens sechs Monate vor Anfrage gespeichert wurden. Die Löschungsverpflichtung für Vorratsdaten nach Ablauf der Frist iSd § 102a Abs. 8 TKG 2003 bleibt unbeschadet aufrecht und entkräftet damit auch jegliches Argument, dass für bestimmte Kategorien

von Daten keine Löschungsverpflichtung statuiert wäre. Die Ausführungen des Antrages zu einem behaupteten Eingriff in verfassungsgesetzlich gewährleistete Rechte durch diese Bestimmungen erscheinen daher unbegründet.

4.10. Zu § 102a TKG 2003

Die Ausführungen der Antragstellerin zu § 102a TKG 2003 beschäftigen sich mit dem darin enthaltenen Datenartenkatalog und den damit verbundenen behaupteten Verletzungen verfassungsgesetzlich gewährleisteter Rechte. Vorauszuschicken ist, dass der Datenartenkatalog des § 102a Abs. 2 TKG 2003 von der [Vorratsdatenspeicherungsrichtlinie] vorgegeben ist.

§ 102a Abs. 1 TKG 2003 sieht die Speicherverpflichtung für in Abs. 2 bis 4 genannte Datenkategorien zu Zwecken der Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs. 2a StPO rechtfertigen vor. Der Speicherzweck stellt nicht – wie von der Antragstellerin […] irrtümlich angenommen – auf die Schwere der Anordnung, sondern auf [die] spezifische, die Zulässigkeitsvoraussetzungen determinierende, Schwere von Straftaten nach § 135 Abs. 2a StPO ab.

Dass die konkrete Speicherung der Daten ohne Gerichtsbeschluss erfolgt, entspricht dem Wesen der Vorratsdatenspeicherung. Im Hinblick darauf, dass der Zugriff jedoch an Kriterien gebunden ist, die primär in der StPO und im SPG geregelt sind, ist sichergestellt, dass die Daten nur verfassungskonform verwendet werden.

Die im Antrag […] zu dieser Regelung vorgebrachten Argumente vermischen zwei verschiedene Sachverhalte, deren unterschiedliche Behandlung in Zusammenhang mit dem Gleichheitsgrundsatz gebracht wird.

Einerseits normiert § 102a Abs. 6 TKG 2003 eine Ausnahme von der generellen Speicherpflicht für kleine Unternehmen. Damit wird sichergestellt, dass kleine Unternehmen nicht vor dem Hintergrund ihrer Umsätze wirtschaftlich unverhältnismäßige Investitionen tätigen müssen. Angesichts der bei solchen Unternehmen geringen Kundenanzahl ist diese Ausnahme sachlich gerechtfertigt, da sie nur einen Bruchteil aller Kommunikationsvorgänge umfasst.

Im Übrigen darf auf eine ähnliche Bestimmung in § 27 Abs. 6 DSG 2000 verwiesen werden, die ebenfalls das System einer 'logischen Löschung' aus Gründen der Wirtschaftlichkeit kennt.

Auch die seitens der Antragstellerin behauptete unsachliche Differenzierung der Speicherung von Daten zum Zweck der Verrechnung liegt eben wegen des Erfordernisses dieser Daten für die Verrechnung, somit für einen gänzlich verschiedenen Zweck, nicht vor.

4.12. Zu § 102b Abs. 1 TKG 2003

Die im Antrag monierten Unklarheiten hinsichtlich der Anordnung einer Auskunft bestehen insofern nicht, als die Anlassfälle und die Form der Auskunft nicht im TKG 2003 sondern in der StPO (vgl. §§ 135 StPO ff.) zu regeln sind.

4.13. Zu § 102b Abs. 2 TKG 2003

[Der Antrag] setzt sich mit der Frage auseinander, was die Verpflichtung zur Speicherung der Daten in einer solchen Form, dass sie unverzüglich weitergegeben werden können, bedeutet. Dabei wird von der Antragstellerin eine Überprüfung, offenbar durch eine zusätzliche Behörde oder den Betreiber, angedacht. Das Prinzip des TKG 2003 besteht jedoch in der Anknüpfung an die Voraussetzungen der StPO und geht daher richtigerweise auch von der vollen Verantwortung der Staatsanwaltschaft für die Zulässigkeit der Anordnung aus.

Ein direkter Zugriff der Behörden auf die Daten ist jedenfalls nicht vorgesehen. Bereits die Formulierung 'dass die Daten übermittelt werden können' legt klar, dass eine selbständige Abrufbarkeit der Daten nicht vorgesehen ist. Die DSVO richtet folgerichtig auch eine 'Durchlaufstelle' ein, über die die Daten anzufordern und zu übermitteln sind. Ein direkter Zugriff auf die Daten ist damit auch tatsächlich unmöglich.

4.14. Zu § 102b Abs. 3 TKG 2003

Durch den in § 102b Abs. 3 TKG 2003 zu findenden Verweis auf die Regelung des § 94 Abs. 4 TKG 2003 ist klar, dass die gerügte Unbestimmtheit der Formulierung – die Übermittlung der Daten habe 'in angemessener geschützter Form' zu erfolgen – nicht vorliegt. Auf die Ausführungen zu § 94 Abs. 4 TKG 2003 […] wird daher verwiesen.

4.15. Zu § 102c Abs. 2 TKG 2003

An dieser Stelle wird nochmals die Protokollierung der Datenverwendung gerügt. Auf die diesbezüglichen Ausführungen in […] dieser Stellungnahme wird verwiesen.

[…]" (Zitat ohne die im Original enthaltenen Hervorhebungen)

2.4. Die Bundesregierung beantragt, den Antrag als unzulässig zurückzuweisen, in eventu als unbegründet abzuweisen. 14

3. Der Antrag zu G 59/2012: 15

3.1. Der Antragsteller zu G 59/2012 (in der Folge: der Zweitantragsteller) stellt gemäß Art. 140 Abs. 1 B-VG iVm §§ 62 ff. VfGG den Antrag, Bestimmungen des TKG 2003 idF BGBl. I 102/2011 als verfassungswidrig aufzuheben. § 102a TKG 2003 sei wegen Verletzung des verfassungsgesetzlich gewährleisteten Rechts auf Achtung des Privat- und Familienlebens, auf den Schutz personenbezogener Daten, auf Kommunikationsfreiheit und Gleichheit aller Staatsbürger vor dem Gesetz aufzuheben. Die § 1 Abs. 4 Z 5 (gemeint wohl § 1 Abs. 4 Z 7), § 92 Abs. 3 Z 6b, in § 93 Abs. 3 die Wortfolge "einschließlich Vorratsdaten", in § 94 Abs. 1 die Wortfolge "einschließlich der Auskunft über Vorratsdaten", § 94 Abs. 4, § 99 Abs. 5 Z 2, 3, und 4, § 102b, § 102c, § 109 Abs. 3 Z 22 bis 26 TKG 2003 stünden mit § 102a TKG 2003 in untrennbarem Zusammenhang und seien deshalb ebenfalls aufzuheben. Hinsichtlich des § 94 Abs. 4 und des § 99 Abs. 5 Z 2, 3 und 4 TKG 2003 beantragt der Zweitantragsteller auch, bestimmte Wortfolgen "in eventu" als verfassungswidrig aufzuheben. Ebenso beantragt der Zweitantragsteller, eventualiter die Bestimmungen des § 53 Abs. 3a sowie 3b SPG bzw. – wiederum "in eventu" – bestimmte Wortfolgen aus diesen Bestimmungen wegen untrennbaren Zusammenhangs mit § 102a TKG 2003 sowie aus demselben Grund § 134 Z 2a StPO und § 135 Abs. 2a StPO als verfassungswidrig aufzuheben. 16

3.2. Im Hinblick auf die Zulässigkeit seines Antrags führt der Zweitantragsteller aus, auf seinen Namen liefen mehrere Verträge betreffend mobile und feste Sprachtelefoniedienste sowie mobile und feste Internet-Zugangsdienste einschließlich E-Mail-Dienste. Er nutze diese näher genannten Anschlüsse sowohl privat als auch beruflich. Die Endgeräte, über die der Zweitantragsteller diese Dienste in Anspruch nehme, würden regelmäßig auch von Dritten (zB von Familienangehörigen und Freunden) zur Nutzung von Kommunikationsdiensten verwendet werden. Desgleichen nutze auch der Zweitantragsteller regelmäßig Endgeräte Dritter, denen zum Teil dem Zweitantragsteller nicht bekannte Ver- 17

tragsverhältnisse mit Anbietern von Kommunikationsdienstleistungen zugrunde liegen würden.

Anbieter von öffentlichen Kommunikationsdiensten seien seit 1. April 2012 nach § 102a TKG 2003 zur Speicherung der in § 102a Abs. 2 bis 4 TKG 2003 genannten Daten verpflichtet. Eine Ausnahme von dieser Speicherpflicht bestehe nach § 102a Abs. 6 TKG 2003 lediglich für Anbieter, deren Unternehmen nicht der Verpflichtung zur Entrichtung des Finanzierungsbeitrags nach § 34 KOG (Komm-Austria-Gesetz, BGBl. I 32/2001) unterliege. Jener Anbieter, dessen öffentliche Kommunikationsdienste der Zweitantragsteller nutze, falle nicht unter die Ausnahmebestimmung des § 102a Abs. 6 TKG 2003. 18

Für den Zweitantragsteller sei ein Wechsel zu einem anderen, nicht der Beitragspflicht nach § 34 KOG und damit nicht der Speicherpflicht nach § 102a TKG 2003 unterliegenden Anbieter von Kommunikationsdiensten im Übrigen weder möglich noch zumutbar, weil für ihn die Qualität der von seinem derzeitigen Anbieter erbrachten Dienste von wesentlicher Bedeutung sei. Überdies sei der Zweitantragsteller bei diesem Anbieter als Dienstnehmer beschäftigt. Er müsse davon ausgehen, dass sein Dienstgeber Vertragsverhältnisse zwischen dem Zweitantragsteller und dritten Anbietern nicht goutieren würde. Eine Kündigung sämtlicher Vertragsverhältnisse und die Substitution dieser durch ein anonymes System von Wertkarten (beim derzeitigen oder einem anderen Anbieter) sei dem Zweitantragsteller ebenfalls nicht zumutbar, weil ihm dies teurer kommen würde. Zum anderen könne dies auch kein vollständiger "Ausweg" aus den durch § 102a TKG 2003 bedingten Eingriffen in die Rechte des Zweitantragstellers sein, insbesondere weil ein fester Telefonanschluss ohne ein Vertragsverhältnis am Markt nicht angeboten werde. 19

Da die in § 102a Abs. 2 bis 4 TKG 2003 genannten Daten seit 1. April 2012 ohne (der Sphäre des Zweitantragstellers zuzuordnenden) Anlass, unabhängig von einer technischen Notwendigkeit, unabhängig von Verrechnungszwecken und unabhängig vom Willen des Zweitantragstellers, in concreto sogar gegen den Willen des Zweitantragstellers, gespeichert werden, sei der Zweitantragsteller durch § 102a Abs. 1 TKG 2003 unmittelbar und aktuell in seinen Rechten betroffen. 20

Für den Zweitantragsteller bestünden keine anderen Möglichkeiten, als durch den vorliegenden, auf Art. 140 B-VG gestützten Antrag, die Unterlassung der Speicherung der von § 102a TKG 2003 umfassten Daten bzw. deren Löschung durchzusetzen. Auch wenn derartige Möglichkeiten bestünden, wäre es ihm nicht zumutbar, gegen seinen Dienstgeber, der gleichzeitig der von ihm gewählte Anbieter öffentlicher Kommunikationsdienste ist, vorzugehen. 21

3.3. Die in § 102a TKG 2003 vorgesehene Speicherverpflichtung verletze den Zweitantragsteller in seinem verfassungsgesetzlich gewährleisteten Recht auf Achtung des Privat- und Familienlebens nach Art. 8 EMRK und Art. 7 GRC. Nach der Judikatur des Europäischen Gerichtshofes für Menschenrechte sei das Fernmeldegeheimnis vom Anwendungsbereich des Art. 8 EMRK erfasst. Die verpflichtende Speicherung der in § 102a Abs. 2 bis 4 TKG 2003 genannten Daten stelle per se einen Eingriff in das Fernmeldegeheimnis dar. Der Zweitantragsteller lebe mit dem ständigen Unbehagen, dass seine Lebensweise und seine Kommunikationsvorgänge überwacht werden. Gleichzeitig lebe der Zweitantragsteller in der ständigen Sorge, dass die gespeicherten Daten, zB auf Grund eines unberechtigten Zugriffs Dritter, missbraucht werden könnten. Der Zweitantragsteller sei daher geneigt, seine Nutzung der Kommunikationsdienste einzuschränken. 22

Nach dem Vorbringen des Zweitantragstellers sei der von der Vorratsdatenspeicherungsrichtlinie vorgegebenen Speicherpflicht nach § 102a TKG 2003 die Verfolgung eines berechtigten Ziels abzusprechen. Ausweislich der Erwägungsgründe 8 bis 10 der Vorratsdatenspeicherungsrichtlinie sei der Kampf gegen den Terrorismus das erklärte Ziel dieser Richtlinie. Dieses werde aber nicht erreicht. Vielmehr bewirke die Speicherpflicht eine Einschränkung der über die letzten Jahrhunderte erkämpften Freiheiten in der Gesellschaft. Die Speicherpflicht unterstütze daher weniger den Kampf gegen den Terrorismus, "als sie vielmehr einer Submission vor dem Terrorismus" gleichkomme. 23

Die in der Vorratsdatenspeicherungsrichtlinie und in § 102a TKG 2003 enthaltenen Regelungen seien überdies weder notwendig noch verhältnismäßig iSd EMRK. Die mangelnde Notwendigkeit und Eignung des Eingriffs ergebe sich aus dem Umstand, dass der Nutzer eines Kommunikationsdienstes der Darstellung 24

des Zweitantragstellers zufolge die Speicherung seiner Daten im Rahmen der Vorratsdatenspeicherungsrichtlinie und des § 102a TKG 2003 insofern verhindern könne, als er nur Kommunikationsdienste nutze, die keiner Speicherpflicht unterliegen. Dies seien in Österreich jene Unternehmen, die unter die Ausnahmebestimmung des § 102a Abs. 6 TKG 2003 fallen.

Darüber hinaus unterlägen Anbieter von Diensten der Informationsgesellschaft im Sinne von § 1 Abs. 2 Z 2 des Notifikationsgesetzes, BGBl. I 183/1999, die nicht ganz oder überwiegend in der Übertragung von Signalen oder Kommunikationsnetzen bestehen, nicht der Speicherpflicht, da ein derartiger Dienst schon kein "Kommunikationsdienst" iSd Legaldefinition des § 3 Z 9 TKG 2003 sei. Zur Speicherung von Daten nach § 102a TKG 2003 seien aber nur Anbieter öffentlicher Kommunikationsdienste verpflichtet. 25

Ebenso seien sogenannte "reine" Internet-Telefoniedienste, dh. Telefoniedienste, die mittels des Internet Protocol (IP) operieren und keinen Zugang zum "herkömmlichen" Telefonnetz ermöglichen, nicht von der Speicherungspflicht des § 102a TKG 2003 erfasst, da sie keine "Kommunikationsdienste" iSd § 3 Z 9 TKG 2003 seien. 26

Des Weiteren könnten in Österreich, beispielsweise durch die Nutzung öffentlicher Internetzugänge, durch den Besuch sogenannter "Call-Shops" oder "Internet-Cafes", durch die Nutzung sogenannter "prepaid-Wertkarten" oder durch die Nutzung öffentlicher Telefonzellen, öffentliche Kommunikationsdienste dergestalt genutzt werden, dass der jeweilige Endnutzer anonym bleibe. 27

Kriminelle würden daher der Darstellung des Zweitantragstellers zufolge wohl bevorzugt Kommunikationsmittel verwenden, die entweder von der Speicherpflicht nach § 102a TKG 2003 nicht erfasst seien, oder bei deren Benutzung aus den gespeicherten Daten keine für eine Strafverfolgung verwertbaren Rückschlüsse zu ziehen seien. In erster Linie würden daher die Daten unbescholtener Bürger – wie jene des Zweitantragstellers – von der Vorratsdatenspeicherung betroffen sein. Die so gespeicherten Daten dienten aber gerade nicht zur Aufklärung, Verfolgung oder zur Ermittlung schwerer Straftaten. 28

Es sei auszuschließen, dass ein zielgerichtetes und effektives Durchsuchen der enormen gespeicherten Datenmengen überhaupt möglich sei, ohne bereits auf "traditionelle Weise" die notwendigen Anhaltspunkte zur Feststellung der Straftäter oder Straftaten erlangt zu haben. 29

Dass die von der Vorratsdatenspeicherungsrichtlinie vorgegebene Speicherpflicht nach § 102a TKG 2003 weder notwendig noch geeignet iSd Art. 8 EMRK sei, zeige auch ein Vergleich mit jenen Mitgliedstaaten, in denen die Vorgaben der Richtlinie schon länger umgesetzt sind. In der überwiegenden Mehrzahl von Mitgliedstaaten sei es nämlich zu keinen signifikanten Änderungen der Aufklärungsquote gekommen. 30

Der Eingriff in die durch Art. 8 EMRK gewährleisteten Rechte sei auch unverhältnismäßig. Es fehle jegliche Differenzierung zwischen den von der Vorratsdatenspeicherung Betroffenen. Es bestehe im konkreten Fall kein Anlass zur Speicherung der Daten des Zweitantragstellers. Die potentielle Möglichkeit der Verhinderung, Aufklärung oder Verfolgung von im Verhältnis zur Gesamtbevölkerung sehr wenigen schweren Straftaten, die von sehr wenigen Straftätern begangen würden, stehe in keinem Verhältnis zu dem von der Vorratsdatenspeicherungsrichtlinie vorgegebenen und mit § 102a TKG 2003 innerstaatlich normierten Eingriff "in die Rechte des den Deckmantel der Anonymität nicht suchenden und damit überwiegenden Großteils von Teilnehmern und Nutzern von Kommunikationsdiensten, die ihrerseits […] mit schweren Straftaten nie in Berührung kommen, sowie des unbescholtenen [Zweitantragstellers]." 31

Darüber hinaus kämen gelindere Mittel als die von der Vorratsdatenspeicherungsrichtlinie vorgegebene Speicherpflicht in Betracht, mit denen das proklamierte Ziel der Feststellung, Ermittlung und Verfolgung von schweren Straftaten ebenso gut erreicht werden kann. 32

Durch die Vorratsdatenspeicherung steige auch das Risiko eines jeden Nutzers, Ermittlungen ausgesetzt zu werden, ohne selbst Anlass dazu gegeben zu haben. Es reiche aus, zB zur falschen Zeit am falschen Ort (dh. in einer bestimmten Funkzelle eingeloggt) gewesen oder von einer bestimmten Person (eventuell 33

auch versehentlich) kontaktiert worden zu sein. Es sei unwürdig, anlasslos als Bürger unter einen Generalverdacht gestellt zu werden, der durch die Speicherpflicht bewirkt werde.

3.4. Im Hinblick auf § 102c TKG 2003, wonach die gespeicherten Vorratsdaten durch geeignete technische und organisatorische Maßnahmen vor unrechtmäßiger Zerstörung, zufälligem Verlust oder unrechtmäßiger Speicherung, Verarbeitung, Zugänglichmachung und Verbreitung zu schützen sind, bringt der Zweitantragsteller vor, dass diese Bestimmung nicht den Anforderungen der EMRK an die angemessene und wirksame Sicherung von Daten gegen Missbrauch, wie sie in der Judikatur des Europäischen Gerichtshofes für Menschenrechte entwickelt worden wären, entspreche. Nach Ansicht des Zweitantragstellers sei es überhaupt nicht möglich, die gemäß § 102a TKG 2003 auf Vorrat gespeicherten Daten in einer Art und Weise zu sichern, wie sie die exzessive Datensammlung und die erheblichen Konsequenzen eines Missbrauchs erforderten. Jedenfalls müssten sich die technischen und organisatorischen Maßnahmen zur Absicherung immer am höchsten Stand der Technik bewegen und nicht bloß für den Regelfall "geeignet" sein. 34

3.5. Des Weiteren bringt der Zweitantragsteller vor, dass der Kreis der in § 102a Abs. 1 TKG 2003 in Bezug genommenen Straftaten ("Straftaten, deren Schwere eine Anordnung nach § 135 Abs. 2a StPO rechtfertigt"), zu weit gezogen sei. Er umfasse nämlich auch "niederschwellige" Straftaten, die jedenfalls keine schweren Straftaten iSd Vorratsdatenspeicherungsrichtlinie seien, wie beispielsweise den Straftatbestand des § 138 StGB (Schwerer Eingriff in fremdes Jagd- und Fischereirecht). 35

3.6. Selbst unter der Annahme, dass die Vorratsdatenspeicherung nicht gegen Art. 8 EMRK verstieße, liege ein Verstoß gegen § 1 DSG 2000 vor, weil diese Bestimmung eine zusätzliche Verdeutlichung des Verhältnismäßigkeitsprinzips für die Zulässigkeit gesetzlich vorgesehener Eingriffe bringe. Nach dem letzten Satz des § 1 Abs. 2 DSG 2000 sei nämlich für den Fall an sich gesetzlich zugelassener Beschränkungen der konkrete Eingriff in das Grundrecht unzulässig, wenn er nicht in der jeweils "gelindesten, zum Ziel führenden Art" vorgenommen wird. Zum Ziel führe § 102a TKG 2003 jedenfalls nicht, weil eben gerade jene Dienste, die den Deckmantel der Anonymität böten, weiterhin zulässig seien. Im Hinblick 36

auf die vielfältigen Möglichkeiten der "herkömmlichen" Ermittlungsarbeit sowie die Möglichkeit der Implementierung des sogenannten "Quick-Freeze-Verfahrens" sei die von der Vorratsdatenspeicherungsrichtlinie vorgegebene Speicherpflicht jedenfalls nicht das gelindeste Mittel zur Erreichung des proklamierten Ziels der Ermittlung, Feststellung und Verfolgung schwerer Straftaten.

4. Die Bundesregierung erstattete eine Äußerung zum Antrag zu G 59/2012, in der den im Antrag erhobenen Bedenken wie folgt entgegengetreten wird: 37

4.1. Der Antrag sei unzulässig, da sich keine der angefochtenen Bestimmungen direkt auf den Zweitantragsteller beziehe. Er sei von den bekämpften Bestimmungen nicht aktuell rechtlich betroffen, da sich diese an Betreiber öffentlicher Telekommunikationsdienste und nicht an Endkunden richteten. Überdies stehe dem Zweitantragsteller ein zumutbarer Weg zur Geltendmachung der behaupteten Verfassungswidrigkeiten zur Verfügung, der die Antragslegitimation des Zweitantragstellers ausschließe. 38

Einerseits könne der Zweitantragsteller die in § 31 Abs. 1 und 7 DSG 2000 vorgesehene Möglichkeit der Beschwerde an die (seinerzeitige) Datenschutzkommission unter Behauptung einer Verletzung des Auskunftsrechts nach § 26 DSG 2000 nutzen und so einen abweisenden (§ 31 Abs. 7 DSG 2000) Bescheid erwirken, der beim Verfassungsgerichtshof bekämpft werden könne. Andererseits erachte es die Bundesregierung für zumutbar, dass der Zweitantragsteller im Zivilrechtsweg (§ 32 Abs. 1 DSG 2000) gegen jenen Anbieter, dessen öffentliche Kommunikationsdienste er nutzt und der gleichzeitig sein Arbeitgeber ist, vorgeht. 39

4.2. Für den Fall, dass der Verfassungsgerichtshof den Antrag des Zweitantragstellers nicht zurückweise, verweist die Bundesregierung auf ihre – oben (siehe insbesondere 2.3) teils wörtlich wiedergegebene – Äußerung zum Antrag der Kärntner Landesregierung. 40

4.3. Im Hinblick auf die Behauptung des Zweitantragstellers, der Kreis der durch § 102a Abs. 1 TKG 2003 in Bezug genommenen Straftaten sei überschießend, verweist die Bundesregierung auf die schon vor dem 1. April 2012 geltende 41

Zulässigkeitsvoraussetzung zur Auskunft über Daten einer Nachrichtenübermittlung und zur Überwachung von Nachrichten, wie sie in § 135 StPO in der bis zum Ablauf des 31. März 2012 anzuwendenden Fassung vorgesehen gewesen sei. Der seit 1. April 2012 in Kraft stehende § 135 Abs. 2a StPO idF BGBl. I 33/2011 ergänze die bisherigen Bestimmungen unter Berücksichtigung der bestehenden Systematik und der engen grundrechtlichen Vorgaben. Es sei unklar, wie eine insofern richtlinienkonforme Anknüpfung an nationales Recht zu einem verfassungswidrigen Ergebnis führen könne.

Zusammenfassend sei die Bundesregierung der Ansicht, dass es sich bei den vom Zweitantragsteller angefochtenen Bestimmungen um im öffentlichen Interesse gelegene, sachlich gerechtfertigte und nicht unverhältnismäßige Regelungen handle, die keinen verfassungsrechtlichen Bedenken begegneten. Der Gesetzgeber habe sich lediglich an dem in der Vorratsdatenspeicherungsrichtlinie vorgesehenen "Regelungsminimum" orientiert. 42

4.4. Die Bundesregierung beantragt, den Antrag des Zweitantragstellers als unzulässig zurückzuweisen, in eventu den Antrag als unbegründet abzuweisen. 43

5. Der Antrag zu G 62,70,71/2012: 44

5.1. In einem als "Sammel-Individualantrag" bezeichneten und auf Art. 140 Abs. 1 B-VG gestützten Antrag an den Verfassungsgerichtshof begehren der Drittantragsteller und 11.129 weitere Personen, der Verfassungsgerichtshof möge Bestimmungen des TKG 2003 idF BGBl. I 102/2011, des SPG idF BGBl. I 13/2012 und der StPO idF BGBl. I 53/2012 als verfassungswidrig aufheben. Der Antrag der 11.129 weiteren Personen wurde mit Beschluss des Verfassungsgerichtshofes vom 10. Juni 2014 zurückgewiesen (G 62/2012-36, G 70/2012-30, G 71/2012-26). 45

Beantragt wird, § 102a TKG 2003 sowie des Weiteren wegen untrennbaren Zusammenhangs mit dieser Bestimmung § 102b, § 102c, in § 99 Abs. 5 Z 2 die Wortfolge "auch wenn diese als Vorratsdaten gemäß § 102a Abs. 2 Z 1, Abs. 3 Z 6 lit. a und b oder § 102a Abs. 4 Z 1, 2, 3 und 5 längstens sechs Monate vor der Anfrage gespeichert wurden,", in § 99 Abs. 5 Z 3 die Wortfolge ", auch wenn hiefür ein Zugriff auf gemäß § 102a Abs. 3 Z 6 lit. d gespeicherte Vorratsdaten 46

erforderlich ist", in § 99 Abs. 5 Z 4 die Wortfolgen "auch" und "als Vorratsdaten gemäß § 102a Abs. 2 Z 1 oder § 102a Abs. 4 Z 1, 2, 3 und 5", § 92 Abs. 3 Z 6 lit. b zur Gänze, in § 93 Abs. 3 die Wortfolge "einschließlich Vorratsdaten", in § 94 Abs. 1 die Wortfolge "einschließlich der Auskunft über Vorratsdaten", in § 94 Abs. 2 die Wortfolge "einschließlich der Auskunft über Vorratsdaten", in § 94 Abs. 4 die Wortfolgen "einschließlich der Auskunft über Vorratsdaten" und "sowie die näheren Bestimmungen betreffend die Speicherung der gemäß § 102c angefertigten Protokolle", in § 98 Abs. 2 die Wortfolge ", auch wenn hiefür ein Zugriff auf gemäß § 102a Abs. 3 Z 6 lit. d gespeicherte Vorratsdaten erforderlich ist" und die Z 22, 23, 24, 25 und 26 des § 109 Abs. 3 TKG 2003 wegen Verletzung des Rechts auf Privat- und Familienleben und Schutz der Korrespondenz gemäß Art. 8 EMRK bzw. Art. 7 GRC, des Rechts auf Datenschutz gemäß § 1 DSG 2000 bzw. Art. 8 GRC, des Rechts auf Meinungs- und Informationsfreiheit gemäß Art. 10 EMRK bzw. Art. 11 GRC, des Rechts auf Versammlungs- und Vereinigungsfreiheit gemäß Art. 11 EMRK bzw. Art. 12 GRC, des Rechts auf Schutz des Fernmeldegeheimnisses gemäß Art. 10a StGG sowie des Rechts auf die Unschuldsvermutung im Strafverfahren gemäß Art. 6 EMRK bzw. Art. 48 GRC aufzuheben.

Aus denselben Gründen begehrt der Drittantragsteller, § 135 Abs. 2a und § 134 StPO Z 2a StPO als verfassungswidrig aufzuheben. Schließlich beantragt er die Aufhebung der Wortfolge "auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 4 iVm § 102a TKG 2003 erforderlich ist," in § 53 Abs. 3a Z 3 SPG und der Wortfolge "auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 iVm § 102a TKG 2003 erforderlich ist," in § 53 Abs. 3b SPG. Dem Hauptbegehren des Drittantragstellers folgen umfangreiche Eventualbegehren. 47

Der Drittantragsteller regt überdies an, dass der Verfassungsgerichtshof beim Gerichtshof der Europäischen Union eine Vorabentscheidung betreffend die Vereinbarkeit der Vorratsdatenspeicherungsrichtlinie mit Rechten der GRC einholen möge. 48

5.2. Zur Antragslegitimation wird ausgeführt, dass schon die nach Ansicht des Drittantragstellers überschießende und nicht gerechtfertigte Speicherung von 49

Daten auf Vorrat Rechte aus § 1 DSG 2000 und Art. 8 EMRK verletze. Der Drittantragsteller sei durch jene Rechtsvorschriften, die die Verwendungszwecke der auf Vorrat gespeicherten Daten begrenzten, unmittelbar und aktuell betroffen, selbst wenn eine tatsächliche weitere Verwendung von personenbezogenen Daten erst später durch Anwendung der StPO- und SPG-Bestimmungen aktualisiert werde: Der Grundrechtseingriff und damit die rechtliche Betroffenheit iSd Zulässigkeitsvoraussetzungen für einen Individualantrag nach Art. 140 B-VG würden primär durch die Speicherung bewirkt, der Sitz der Verfassungswidrigkeit und die nachteilige Betroffenheit seien aber auch in der – in Relation zur Schwere des Grundrechtseingriffs unverhältnismäßigen – Zweckbestimmung der zu speichernden Daten zu sehen. Obwohl § 102a TKG 2003 unmittelbar nur die Anbieter elektronischer Kommunikationsdienste adressiere, sei der Drittantragsteller aber dennoch unmittelbar in seiner Rechtssphäre betroffen. Es sei nämlich gerade der Zweck der Vorratsdatenspeicherung, die personenbezogenen Daten der Nutzer elektronischer Kommunikationsdienste zu erfassen und für sechs Monate zu speichern. Unter Verweis auf das Erkenntnis VfSlg. 13.038/1992 (unmittelbare Betroffenheit von Arbeitnehmerinnen durch ein an die Arbeitgeber gerichtetes Nachtarbeitsverbot für Frauen) führt der Drittantragsteller aus, dass die Eigenschaft als Normadressat keine unbedingte Voraussetzung für die unmittelbare Betroffenheit in der Rechtssphäre sei. Unmittelbar betroffen von der Vorratsdatenspeicherung seien alle natürlichen und juristischen Personen, die bei einem speicherpflichtigen Anbieter im Sinne des § 102a TKG 2003 einen Vertrag zur Nutzung eines oder mehrerer der in § 102a Abs. 2 bis 4 TKG 2003 aufgezählten Dienste abgeschlossen hätten und daher mit ihren Teilnehmerdaten ("Stammdaten") und den jeweiligen Verkehrsdaten von der Vorratsdatenspeicherung erfasst würden.

Zum Nachweis der aktuellen und unmittelbaren rechtlichen Betroffenheit des Drittantragstellers wurden eine Mobilfunkrechnung (betreffend die Nutzung von Mobiltelefon, Internet und E-Mail) inklusive Einzelgesprächsnachweis vom 12. Juni 2012, eine Auftragsbestätigung und eine Rechnung betreffend die Nutzung von Internet, Festnetztelefonie und Internettelefonie vom 2. Mai 2012 bis zum 11. Juni 2012 durch den Drittantragsteller vorgelegt. 50

Dass der Drittantragsteller durch die Vorratsdatenspeicherung in seiner Rechtssphäre betroffen sei, zeige sich nicht zuletzt daran, dass ohne die Speicherver- 51

pflichtung des § 102a TKG 2003 personenbezogene Verbindungsdaten in viel geringerem Umfang und regelmäßig für kürzere Zeit als sechs Monate gespeichert werden würden. Die unmittelbarsten Auswirkungen zeigten sich dabei im Bereich der E-Mail-Dienste, weil keiner der seit 1. April 2012 speicherpflichtigen Anbieter bisher E-Mail-Verbindungsdaten für betriebliche Zwecke zu speichern gehabt habe. Das Risiko einer rechtswidrigen Datenverwendung und damit das Ausmaß des weiteren Grundrechtseingriffs wäre ohne Vorratsdatenspeicherung deutlich geringer.

Dem Drittantragsteller sei die Erlangung eines anfechtbaren Verwaltungsaktes, den er letztlich vor dem Verfassungsgerichtshof in Beschwerde ziehen könnte, nicht zumutbar bzw. unmöglich. So müssten insbesondere Auskunftsbegehren nach § 26 DSG 2000 und entsprechende Beschwerden (§ 31 DSG 2000) wiederkehrend und betreffend alle möglichen Anbieter öffentlicher Kommunikationsdienste gestellt bzw. erhoben werden, die aber letztlich gar nicht zielführend wären, weil das Rechtsschutzbegehren des Drittantragstellers nicht auf Auskunft über die auf Vorrat gespeicherten Daten, sondern auf deren Löschung gerichtet sein müsse. Ein Begehren auf Löschung dieser Daten sei theoretisch nur im Zivilrechtsweg (§ 27 iVm § 32 DSG 2000) zulässig. Es würde aber ebenso wenig zur Erreichung des Rechtsschutzziels des Drittantragstellers führen, da einem Löschungsbegehren im Hinblick auf die auf Vorrat gespeicherten Daten gerade auf Grund des § 102a TKG 2003 nicht stattzugeben sei. Dem Drittantragsteller sei es deshalb nicht zumutbar, ein von vornherein aussichtsloses Zivilverfahren nur zu dem Zweck zu führen, die damit befassten Gerichte allenfalls dazu zu bewegen, einen Antrag auf Aufhebung der Vorschriften betreffend die Vorratsdatenspeicherung nach Art. 89 Abs. 2 B-VG an den Verfassungsgerichtshof zu stellen. 52

5.2.1. Nach der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte (EGMR 6.6.2006, Fall *Segerstedt-Wilberg ua.*, Appl. 62.332/00, NL 2006, 129) verletze allein schon die überschießende oder nicht gerechtfertigte Speicherung von Daten einerseits Art. 8 EMRK, andererseits auch Art. 10 und 11 EMRK. Daher bewirke die in § 102a TKG 2003 normierte Speicherverpflichtung einen Eingriff in Art. 8 EMRK, Art. 7 GRC, § 1 DSG 2000, Art. 8 GRC, Art. 10 EMRK und Art. 11 GRC. Die darüber hinaus angefochtenen Bestimmungen (§§ 102b, 99 53

Abs. 5 TKG 2003, § 135 Abs. 2a StPO sowie § 53 Abs. 3a und 3b SPG) regelten die Verwendungszwecke der gemäß § 102a TKG 2003 gespeicherten personenbezogenen Verkehrsdaten. Weil die Speicheranordnung nicht isoliert von ihrer Zweckbestimmung beurteilt werden könne, "perpetuierten" diese Bestimmungen die geltend gemachten Grundrechtseingriffe. Darüber hinaus bewirkten sie auch einen Eingriff in das Fernmeldegeheimnis gemäß Art. 10a StGG.

Die durch die Vorratsdatenspeicherungsrichtlinie als Ziel vorgegebene Bekämpfung schwerer Kriminalität werde durch die bekämpften Vorschriften nicht merkbar gefördert. Ein "Umgehen" der Bestimmungen über die Vorratsdatenspeicherung oder das Ergreifen von entsprechenden Gegenmaßnahmen sei für Kriminelle ein Leichtes. 54

Überdies würden die bekämpften Vorschriften selbst dort, wo durch sie in Einzelfällen der vorgegebene Zweck erfüllt werden könne, nicht das schonendste Mittel zur Erreichung dieses Zwecks darstellen. In den meisten Fällen würden schon Daten, die bei den Anbietern öffentlicher Kommunikationsdienste aus betrieblichen Notwendigkeiten vorlägen, ausreichen, um den in der Vorratsdatenspeicherungsrichtlinie vorgegebenen Zweck zu erfüllen. In den übrigen Fällen reiche ein abgekürztes Verfahren, bei dem ein Gericht bei entsprechender Verdachtslage anordnen könne, bestimmte Daten von Telekommunikationsteilnehmern einzufrieren (sogenanntes "Quick-Freeze-Verfahren"). 55

Selbst wenn man aber davon ausgehe, dass mit der Vorratsdatenspeicherung den staatlichen Stellen das gelindeste und zum intendierten Ziel führende Mittel an die Hand gegeben werde, stünden die Vorschriften in keinem angemessenen Verhältnis zu dem sich aus ihnen ergebenden Nachteil für den Einzelnen und die Gesellschaft. Auf Grund des Umstands, dass Eignung und Erforderlichkeit nach Ansicht des Drittantragstellers fragwürdig erschienen, müssten besonders hohe Anforderungen an die Verhältnismäßigkeit der durch die bekämpften Bestimmungen bewirkten Grundrechtseingriffe gestellt werden. Nur in wenigen Einzelfällen wirke sich die Vorratsdatenspeicherung positiv aus. Dem stehe allerdings ein schwerer Eingriff in die Privatsphäre praktisch der gesamten Bevölkerung gegenüber. Die Verwendungszwecke der auf Vorrat gespeicherten Daten seien viel zu weit gefasst und es stünden keine ausreichenden Rechtschutzmöglichkeiten zur Verfügung, was ebenfalls zur Unverhältnismäßigkeit beitrage. 56

Die Bestimmungen, die die Verwendung der auf Vorrat gespeicherten Daten festlegen, räumten eine überschießende Verwendungsmöglichkeit ein und seien auch aus diesen Gründen unverhältnismäßig. Das Bestimmtheitsgebot gehe in Datenschutzangelegenheiten über den allgemeinen Maßstab des Art. 18 B-VG hinaus. Die Bindung der Verwaltung sei im Hinblick auf Überwachungsmaßnahmen besonders wichtig, da der Betroffene von solchen Maßnahmen naturgemäß keine Kenntnis erlange und daher auch keine Möglichkeit habe, in einem vorgeschalteten Verfahren Einfluss auf das eingreifende Verhalten der Behörde zu nehmen. Insbesondere bei Überwachungsmaßnahmen in Phasen, in denen sich (noch) kein konkreter Straftatbestand abzeichne, bestehe das Risiko, dass der Eingriff lediglich an ein noch schwer fassbares Geschehen anknüpfe. Die Antragsteller führen in der Folge unter Hinweis auf ein Urteil des Bundesverfassungsgerichts (BVerfGE 110, 33) und unter wörtlicher Wiedergabe von Teilen eines Erkenntnisses des Verfassungsgerichtshofes (VfSlg. 16.369/2001) aus, dass Handlungen, auf Grund deren Vorratsdaten verwendet werden können, vorhersehbar und kontrollierbar sein müssten. Insbesondere die § 99 Abs. 5 Z 3 und 4 TKG 2003 iVm § 53 Abs. 3a und 3b SPG seien in diesem Sinne zu unbestimmt, da Auskünfte keiner Einschränkung im Hinblick auf den Schutz höherrangiger Güter unterlägen, sondern schon zur Abwehr gefährlicher Angriffe iSd § 16 SPG zulässig seien. Trotz Richtervorbehalts sei auch die Grundregel zur Verwendung von Vorratsdaten in § 102b TKG 2003 iVm § 135 Abs. 2a StPO zu weitgehend, weil die Delikte, für deren Aufklärung eine Auskunft zulässig ist, lediglich eine Höchststrafdrohung von mehr als einem Jahr Freiheitsstrafe beinhalten müssten. 57

5.3. Abschließend zieht der Drittantragsteller aus der "Praxis der Vorratsdatenspeicherung" Schlüsse, die seines Erachtens auch die Verfassungswidrigkeit der bekämpften Vorschriften belegen könnten. Insbesondere dürften IP-Adressen nicht als "harmlose Zugangsdaten" behandelt werden, da staatliche Stellen an IP-Adressen, die von Individuen verwendet werden, nur herankommen würden, wenn sie vorher den Inhalt einer Kommunikation (zB den Inhalt einer besuchten Website) kennen würden. Aus dem Umstand, dass auch dynamische IP-Adressen oftmals über einen längeren Zeitraum ein und demselben Nutzer zugewiesen blieben, könne die Polizei "Registraturen" mit IP-Adressen für die Zukunft aufbauen, da es keine klaren Bestimmungen betreffend die Löschung ermittelter IP- 58

Adressen gäbe. Betreffend Standortdaten iSd § 53 Abs. 3b SPG bestehe kein effektiver Rechtsschutz, mittels dessen sichergestellt werden könne, dass eine Abfrage tatsächlich zur Erfüllung einer der in dieser Vorschrift bestimmten Zwecke erfolgte. Die Praxis der Vorratsdatenspeicherung führe des Weiteren zu einer "Verletzung materieller Grundrechte", insbesondere des § 1 DSG 2000 und des Art. 8 EMRK. Durch die Verknüpfung von Vorratsdaten mit anderen Datensammlungen könnten neue Informationen "erzeugt" und Schlüsse gezogen werden, die sowohl die grundrechtlich geschützten Geheimhaltungsinteressen der Betroffenen beeinträchtigten, als auch anschließende Eingriffe in die Privatsphäre nach sich zögen. Die schiere "Menge" der auf Vorrat gespeicherten Daten führe zu einem gesteigerten Gefährdungspotential. Überdies ergäben sich aus der anlasslosen Speicherung Einschüchterungseffekte, die zu Beeinträchtigungen bei der Ausübung von Grundrechten führen könnten. Die Unbefangenheit des Verhaltens werde insbesondere gefährdet, da die Streubreite von Ermittlungsmaßnahmen dazu beitrage, dass Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens entstünden. Unter Verweis auf die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte hält der Drittantragsteller des Weiteren fest, dass seiner Meinung nach "jede Form einer groß angelegten, allgemeinen oder sondierenden elektronischen Überwachung unzulässig [sei], insbesondere, wenn nicht wegen einer bestimmten Tat oder Gefahr ermittelt […], sondern nach möglichen Taten oder Gefährdungen gesucht [werde]." Die Ermächtigung zur Speicherung und in der Folge zur Überwachung der Telekommunikation zwecks Vorsorge für die Verfolgung und die Verhütung der in Bezug genommenen Straftaten genüge den Anforderungen der Verhältnismäßigkeit im engeren Sinne nicht. Die durch die angefochtenen Bestimmungen vorgesehenen Eingriffe in die vom Drittantragsteller näher bezeichneten verfassungsgesetzlich gewährleisteten Rechte seien daher im engeren Sinne nicht verhältnismäßig.

6. Die Bundesregierung erstattete eine Äußerung zum Antrag zu G 62,70,71/2012. Sie erachte ihn für unzulässig, da 11.130 Antragsteller nicht aktuell rechtlich betroffen seien und ihnen überdies ein "zumutbarer Umweg" offen stehe. Die Argumentation der Bundesregierung war diesbezüglich im Wesentlichen gleichlautend mit jener, die schon oben unter 4.1 wiedergegeben wurde. 59

6.1. Für den Fall, dass der Verfassungsgerichtshof den Antrag als zulässig erachte, verwies die Bundesregierung auf ihre Äußerungen zum Antrag der Kärntner Landesregierung sowie zum Antrag zu G 59/2012 (siehe dazu oben 2.3 und 4.2 f.). 60

6.2. Den Bedenken, die die Antragsteller im Hinblick auf die behauptete Unverhältnismäßigkeit auf Grund überschießender, über die Abwehr einer konkreten Gefahr oder die Aufklärung einer konkreten Straftat hinausgehender Verwendungsmöglichkeiten von auf Vorrat gespeicherten Daten und den mangelnden diesbezüglichen Rechtsschutz geltend gemacht hatten, entgegnet die Bundesregierung, dass insbesondere weder § 53 Abs. 3a Z 3 SPG noch § 53 Abs. 3b SPG eine Rechtsgrundlage für eine allgemeine oder sondierende Überwachung der Bevölkerung, im Zuge derer nicht wegen einer bestimmten Tat oder Gefahr ermittelt wird, sondern nach möglichen Taten oder Gefährdungen gesucht werden soll, bilde. Dies sei vom Verfassungsgerichtshof im Erkenntnis VfSlg. 19.657/2012 bestätigt worden. Das Gleiche gelte für die relevanten Bestimmungen der StPO, insbesondere § 135 Abs. 2a StPO. Sofern die Antragsteller geltend machten, der Zweck der Speicherpflicht nach § 102a TKG 2003 habe einen präventiven Charakter, übersähen sie, "dass die Bestimmung zur Speicherverpflichtung nur gemeinsam mit jenen Bestimmungen, die die Zulässigkeit der Anfrage regeln (vgl. § 53 Abs. 3a Z 2 und 3 SPG, § 53 Abs. 3b SPG sowie § 135 Abs. 2a StPO), in einer Gesamtschau zu beurteilen [sei]." Die Eingriffsermächtigungen des § 53 Abs. 3a und 3b SPG im Bereich der ersten allgemeinen Hilfeleistungspflicht unterlägen sehr wohl einer Einschränkung auf die Rechtsgüter Leben, Gesundheit und Freiheit eines Menschen. Soweit die Eingriffsbefugnis der Abwehr eines gefährlichen Angriffs diene, ergebe sich eine Einschränkung auf bestimmte Rechtsgüter durch die Strafrechtsakzessorietät des § 16 SPG. Daraus folge, dass Auskünfte zur Abwehr eines gefährlichen Angriffs nach § 53 Abs. 3a und 3b SPG grundsätzlich nur zum Schutz solcher Rechtsgüter rechtlich zulässig seien, die vom Gesetzgeber im Rahmen der in § 16 Abs. 2 Z 1 bis 5 SPG angeführten Straftatbestände als schützenswert erachtet würden. Die Verhältnismäßigkeit von Eingriffen gemäß § 53 Abs. 3a Z 2 bis 4 und § 53 Abs. 3b SPG unterliege der nachprüfenden kommissarischen Kontrolle des beim Bundesminister für Inneres eingerichteten Rechtsschutzbeauftragten (§§ 91a ff. SPG). Neben dem 61

kommissarischen Rechtsschutz durch den Rechtsschutzbeauftragten stehe Personen, die den konkreten Verdacht hegten, dass ihre Daten auf Grund der angefochtenen Bestimmungen des SPG ermittelt wurden, das Auskunftsrecht gemäß § 26 DSG 2000, das Löschungsrecht gemäß § 27 DSG 2000, das Beschwerderecht gemäß § 31 DSG 2000 iVm § 90 SPG, aber auch die Eingabe an die (seinerzeitige) Datenschutzkommission gemäß § 30 Abs. 1 DSG 2000, die im Fall eines begründeten Verdachtes zu einer Systemprüfung gemäß § 30 Abs. 2 DSG 2000 führen könne, zur Verfügung. In diesem Zusammenhang sei auch auf die ausdrückliche Löschungsverpflichtung des § 63 SPG zu verweisen. Auch im Anwendungsbereich der StPO stünden dem Betroffenen eine Reihe von Rechtsschutzmöglichkeiten zur Verfügung. So gewährten etwa die §§ 87, 106, 138 Abs. 5 sowie § 139 StPO unter Einbeziehung des Rechtsschutzbeauftragten der Justiz in allen Fällen der Auskunft über Vorratsdaten (vgl. § 147 Abs. 1 StPO) einen umfassenden Schutz für den Einzelnen.

6.3. Die Bundesregierung beantragt, den Antrag zu G 62,70,71/2012 als unzulässig zurückzuweisen, in eventu den Antrag als unbegründet abzuweisen. 62

7. Der Verfassungsgerichtshof verband in sinngemäßer Anwendung des § 187 ZPO iVm § 35 VfGG die Anträge zur gemeinsamen Beratung. 63

8. Mit Beschluss vom 28. November 2012, G 47/12-11, G 59/12-10, G 62,70,71/12-11 (= VfSlg. 19.702/2012), setzte der Verfassungsgerichtshof die Gesetzesprüfungsverfahren aus und legte dem Gerichtshof der Europäischen Union gemäß Art. 267 AEUV folgende Fragen zur Vorabentscheidung vor: 64

"1. Zur Gültigkeit von Handlungen von Organen der Union:

Sind die Art. 3 bis 9 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, und zur Änderung der Richtlinie 2002/58/EG mit Art. 7, 8 und 11 der Charta der Grundrechte der Europäischen Union vereinbar?

2. Zur Auslegung der Verträge:

2.1. Sind im Lichte der Erläuterungen zu Art. 8 der Charta, die gemäß Art. 52 Abs. 7 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 Art. 8 Abs. 2 und Art. 52 Abs. 1 der Charta zu berücksichtigen?

2.2. In welchem Verhältnis steht das in Art. 52 Abs. 3 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 Art. 8 der Charta zu berücksichtigen?

2.4. Hat unter Berücksichtigung des Art. 52 Abs. 4 der Charta der Grundsatz der Wahrung höherer Schutzniveaus in Art. 53 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 Art. 52 Abs. 3 der Charta, Abs. 5 der Präambel und die Erläuterungen zu Art. 7 der Charta, wonach die darin garantierten Rechte den Rechten nach Art. 8 EMRK entsprechen, aus der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte zu Art. 8 EMRK Gesichtspunkte für die Auslegung des Art. 8 der Charta ergeben, die die Auslegung des zuletzt genannten Artikels beeinflussen?" (Zitat ohne die Hervorhebungen im Original)

9. Der Gerichtshof der Europäischen Union verband das Vorabentscheidungsersuchen des Verfassungsgerichtshofes mit einem entsprechenden Ersuchen des irischen High Courts. Mit Urteil der Großen Kammer in den verbundenen Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland und Seitlinger ua.*, vom 8. April 2014 erkannte der Gerichtshof der Europäischen Union, dass die Vorratsdatenspeicherungsrichtlinie ungültig ist. 65

9.1. Die erste Vorlagefrage des Verfassungsgerichtshofes beantwortete der Gerichtshof der Europäischen Union in seinem Urteil vom 8. April 2014 auf das Wesentlichste zusammengefasst wie folgt: 66

Die Gültigkeit der Richtlinie sei anhand der Art. 7 und 8 GRC zu prüfen (EuGH 8.4.2014 [GK], verb. Rs. C-293/12, C-594/12, *Digital Rights Ireland und Seitlinger ua.* [Rz 31]). Die den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste und den Betreibern eines öffentlichen Kommunikationsnetzes durch die Vorratsdatenspeicherungsrichtlinie auferlegte Pflicht, Daten über das Privatleben einer Person und ihre Kommunikationsvorgänge während eines bestimmten Zeitraums auf Vorrat zu speichern, stelle als solche einen Eingriff in die durch Art. 7 GRC garantierten Rechte dar (EuGH, *Digital Rights Ireland und Seitlinger ua.*, Rz 34). Zudem stelle der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten einen zusätzlichen Eingriff in dieses Grundrecht dar (EuGH, *Digital Rights Ireland und Seitlinger ua.*, Rz 35 mit Nachweisen aus der Rechtsprechung des EGMR). Desgleichen greife die Vorratsdatenspeicherungsrichtlinie in das durch Art. 8 GRC garantierte Grundrecht auf den Schutz personenbezogener Daten ein, da sie eine Verarbeitung personenbezogener Daten vorsehe (EuGH, *Digital Rights Ireland und Seitlinger ua.*, Rz 36). Der mit der Vorratsdatenspeicherungsrichtlinie verbundene Eingriff in die in Art. 7 und Art. 8 GRC verankerten Grundrechte sei von großem Ausmaß und als besonders schwerwiegend anzusehen. 67

In weiterer Folge prüfte der Gerichtshof der Europäischen Union, ob der Eingriff in die durch Art. 7 und Art. 8 GRC garantierten Rechte gerechtfertigt sei (EuGH, *Digital Rights Ireland und Seitlinger ua.*, Rz 38 ff.). In diesem Zusammenhang hielt er fest, dass die Vorratsdatenspeicherungsrichtlinie klare und präzise Regeln für die Tragweite und die Anwendung der fraglichen Maßnahme vorsehen und Mindestanforderungen aufstellen müsse, sodass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügten, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichten (EuGH, *Digital Rights Ireland und Seitlinger ua.*, Rz 54 unter Hinweis auf die Rechtsprechung des EGMR). 68

Der Gerichtshof der Europäischen Union setzte sich in seinem Urteil vom 8. April 2014 in der Folge detailliert mit der Frage auseinander, ob die Vorratsdatenspeicherungsrichtlinie den in der Rz 54 des Urteils aufgestellten Anforderungen genügt (EuGH, *Digital Rights Ireland und Seitlinger ua.*, Rz 56 ff.). Er kam letztlich zum Schluss, dass der Unionsgesetzgeber beim Erlass der Richtlinie die Grenzen überschritten habe, die er zur Wahrung des Grundsatzes der Verhältnismäßigkeit im Hinblick auf die Art. 7, 8 und 52 Abs. 1 GRC einhalten musste (EuGH, *Digital Rights Ireland und Seitlinger ua.*, Rz 69). Die erste Vorlagefrage des Verfassungsgerichtshofes beantwortete der Gerichtshof der Europäischen Union daher dahingehend, dass die Vorratsdatenspeicherungsrichtlinie ungültig sei (EuGH, *Digital Rights Ireland und Seitlinger ua.*, Rz 71). 69

9.2. Aus den Ausführungen zur ersten Vorlagefrage des Verfassungsgerichtshofes folge, dass dessen "zweite Vorlagefrage nicht zu beantworten" sei (EuGH, *Digital Rights Ireland und Seitlinger ua.*, Rz 72). 70

10. In der Folge stellte es der Verfassungsgerichtshof den Parteien des verfassungsgerichtlichen Verfahrens frei, zu den Auswirkungen dieses Urteils auf das verfassungsgerichtliche Verfahren Stellung zu nehmen. Hievon machten die antragstellende Landesregierung, die Antragsteller zu G 59/2012 und zu G 62,70,71/2012 sowie die Bundesregierung Gebrauch. 71

10.1. Die antragstellende Landesregierung bringt in der auf Grund ihres Beschlusses vom 6. Mai 2014 erstatteten Äußerung vor, dass dem Urteil des Europäischen Gerichtshofes in der Rs. *Digital Rights Ireland und Seitlinger ua.* im Ausgangsverfahren Bindung inter partes und über das Ausgangsverfahren die uneingeschränkte Wirkung erga omnes zukomme. Der Verfassungsgerichtshof habe im Ausgangsverfahren die für ungültig erklärte Richtlinie "vom Zeitpunkt ihres In-Kraft-Tretens an – also rückwirkend – außer Anwendung zu lassen […]". 72

10.2. Der Zweitantragsteller macht in seiner Äußerung zum Urteil geltend, dass aus dem Umstand, dass die Vorratsdatenspeicherungsrichtlinie nunmehr nicht mehr "Teil des Unionsrechts" sei, die angefochtenen Rechtsvorschriften ausschließlich am Maßstab des höherrangigen staatlichen Rechts zu prüfen seien. Da 73

die für das Urteil in der Rs. *Digital Rights Ireland und Seitlinger ua.* relevanten Bestimmungen der GRC den "parallelen Bestimmungen der EMRK" glichen und diese in Österreich in Verfassungsrang stünden, könnten die Feststellungen des Gerichtshofes der Europäischen Union auch für die Prüfung der bekämpften Vorschriften nach nationalem Recht herangezogen werden.

Die Schlussfolgerungen in den Rz 56 ff. des Urteils, in denen die mangelnde Verhältnismäßigkeit der Grundrechtseingriffe durch die Vorratsdatenspeicherungsrichtlinie festgestellt wird, seien am wichtigsten für die Prüfung der Verhältnismäßigkeit einer Speicherung von Daten auf Vorrat. Im Ergebnis führten sie zu einer Absage an eine anlasslose, flächendeckende und undifferenzierte Speicherung von Daten. 74

Im Hinblick auf die Ausführungen in Rz 60 des Urteils, wonach die Vorratsdatenspeicherungsrichtlinie kein objektives Kriterium vorsehe, das es ermögliche, den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung zwecks Verhütung, Feststellung oder strafrechtlicher Verfolgung auf Straftaten zu beschränken, die im Hinblick auf das Ausmaß und die Schwere des Eingriffs in die in Art. 7 und Art. 8 GRC verankerten Grundrechte als hinreichend schwer angesehen werden könnten, um einen solchen Eingriff zu rechtfertigen, führt der Zweitantragsteller aus, dass dies auch auf die angefochtenen Bestimmungen im Besonderen zutreffe. Die in § 102a TKG 2003 angeordnete Speicherpflicht zur "Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs. 2a StPO rechtfertige", nehme keine Straftaten in Bezug, die im Hinblick auf das Ausmaß und die Schwere des Eingriffs in die Grundrechte durch die angefochtenen Normen einen Eingriff rechtfertigten. 75

Der in der Rz 67 des Urteils aufgegriffene Umstand, dass die Vorratsdatenspeicherungsrichtlinie nicht vorsehe, dass Daten nach Ablauf der Speicherungsfrist unwiderruflich vernichtet werden, treffe auch auf die angefochtenen Bestimmungen zu. § 102a Abs. 8 TKG 2003 bestimme lediglich, dass die Daten nach Ablauf der Speicherfrist "zu löschen" seien. Aus technischer Sicht seien Daten bei einer "reinen Löschung" relativ leicht wiederherzustellen, da sie auf dem entsprechenden Datenträger verblieben und lediglich "ausgeblendet" seien. 76

Der Zweitantragsteller hält seinen im Individualantrag zu G 59/2012 gestellten Antrag weiterhin aufrecht und begehrt, ihm Kosten in näher bezeichneter Höhe zuzusprechen. 77

Schließlich stellt der Zweitantragsteller "aus prozessualer Vorsicht" zu seinem im Individualantrag enthaltenen Aufhebungsbegehren einen Eventualantrag. Er begehrt eventualiter nunmehr, näher bezeichnete Wortfolgen in § 53 Abs. 3a Z 3 und § 53 Abs. 3b SPG sowie § 135 Abs. 2a und § 134 Z 2a StPO jeweils als verfassungswidrig aufzuheben, weil diese mit § 102a TKG 2003 in untrennbarem Zusammenhang stünden. 78

10.3. Der Drittantragsteller bringt vor, dass das Urteil des Gerichthofes der Europäischen Union in der Rs. *Digital Rights Ireland und Seitlinger ua.* eine Aufhebung des § 102a TKG 2003 gebiete, der die Vorratsdatenspeicherung vorschreibe und daher die "zentrale Norm" zur österreichischen Umsetzung der Vorratsdatenspeicherung bilde. Auch die "tendenziell eher zurückhaltende Umsetzung" der Vorratsdatenspeicherungsrichtlinie in Österreich erfolgte "innerhalb der Determinanten dieser Richtlinie". Da die Vorratsdatenspeicherungsrichtlinie "in vielen verschiedenen Aspekten als unverhältnismäßig erkannt wurde", indiziere dies, "dass jede Umsetzung innerhalb dieser Determinanten ebenso überschießend und damit grundrechtswidrig [sei]". 79

Wie der Zweitantragsteller (siehe oben 10.2) macht der Drittantragsteller im Hinblick auf die Rz 60 des Urteils geltend, dass es in Zweifel zu ziehen sei, dass die durch § 135 Abs. 2a StPO in Bezug genommenen Straftaten als "hinreichend schwer" anzusehen seien. 80

Im Hinblick auf die Zugriffsbefugnisse nach § 76a Abs. 2 StPO sowie § 53 Abs. 3a SPG sei auch für die nationale Umsetzung die "Kritik des EuGH" gültig, dass "der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterläge, deren Entscheidung den Zugang zu den Daten und ihre Nutzung auf das zur Erreichung des verfolgten Ziels absolut Notwendige beschränken soll und im Anschluss an einen mit Gründen versehenen Antrag der 81

genannten Behörden im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten ergeht" (EuGH, *Digital Rights Ireland und Seitlinger ua.*, Rz 62).

Der Drittantragsteller hält seine Anträge vollinhaltlich aufrecht. Er modifiziert seinen Antrag auf Kostenzuspruch und begehrt nunmehr – unter Anführung näherer Gründe und Vorlage eines Kostenverzeichnisses – einen Kostenzuspruch in der Höhe von € 55.064,40. 82

10.4. Schließlich erstattete die Bundesregierung eine Äußerung. Sie verweist darauf, dass hinsichtlich des Zugangs zu Vorratsdaten die österreichische Rechtslage eine differenzierte und verhältnismäßige Regelung aufweise, die über den Regelungsgehalt der Vorratsdatenspeicherungsrichtlinie hinausgehe. Vor dem Hintergrund des differenziert geregelten Zuganges zu den Vorratsdaten sei die anlasslose Speicherung der Vorratsdaten im konkreten Verfahren "nicht relevant". 83

Zu den Bedenken, dass "keinerlei Zugangsbeschränkungen" für die nationalen Behörden bestünden und dass der Begriff der "schweren Straftaten" nicht definiert sei, weist die Bundesregierung darauf hin, dass nach § 135 Abs. 2a iVm Abs. 2 Z 3 und 4 StPO die Auskunft über Vorratsdaten gegen den Willen des Überwachten erst ab einer Strafdrohung von mehr als einem Jahr Freiheitsstrafe zulässig sei. Soweit der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Überwachung sein wird, dieser zustimmt, werde bereits eine Strafdrohung von mehr als sechs Monaten als ausreichend vom Gesetz angesehen (§ 135 Abs. 2a iVm Abs. 2 Z 2 StPO); dies nicht zuletzt, um den Opfern von beharrlicher Verfolgung nach § 107a StGB ("Stalking") eine Möglichkeit der wirksamen Verfolgung von Tätern zu bieten. Insofern bestehe im innerstaatlichen Recht eine Zugangsbeschränkung für nationale Behörden. Festzuhalten sei, dass die Strafverfolgungsbehörden "nach wie vor" einen maßhaltenden Umgang mit der Auskunftserteilung über Vorratsdaten übten. Dies ergebe sich insbesondere aus dem Bericht des stellvertretenden Rechtsschutzbeauftragten (§ 47a StPO), den die Bundesregierung betreffend das Jahr 2013 dem Verfassungsgerichtshof vorlegte. 84

Im Hinblick auf die Risiken eines unberechtigten Zugangs zu Vorratsdaten und des Missbrauchs von Vorratsdaten sei die Bundesregierung der Ansicht, dass für sämtliche Stadien des Verfahrens ausreichende Vorkehrungen getroffen wurden, um diese soweit wie möglich zu minimieren. 85

Die Bundesregierung hält die in ihren bisherigen Äußerungen erstatteten Ausführungen vollinhaltlich aufrecht. 86

11. Der Verfassungsgerichtshof führte am 12. Juni 2014 eine öffentliche mündliche Verhandlung durch, in der die antragstellende Landesregierung, die Zweit- und Drittantragsteller bzw. deren Vertreter und die Vertreter der Bundesregierung insbesondere zu Fragen der technischen Umsetzung der Vorratsdatenspeicherungspflicht, des Kreises der betroffenen Dienste und des Kreises der Delikte, für die in der Praxis Auskunftsersuchen an Betreiber gerichtet werden, Stellung nahmen. In der mündlichen Verhandlung wurde auch die Frage erörtert, inwieweit ein untrennbarer Zusammenhang zwischen den angefochtenen Bestimmungen des TKG 2003 einerseits und den Bestimmungen der StPO sowie des SPG mit Bezug zur Vorratsdatenspeicherung andererseits besteht. 87

II. Rechtslage

1. Art. 15 der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. 2002 L 201, 37, zuletzt geändert durch die Richtlinie 2009/136/EG, ABl. 2009 L 337, 11, lautet – auszugsweise – wie folgt: 88

"Artikel 15

Anwendung einzelner Bestimmungen der Richtlinie 95/46/EG

(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokra-

tischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen.
[(1a) mit Art. 11 der Vorratsdatenspeicherungsrichtlinie eingefügt]
(1b) […]
(2) Die Bestimmungen des Kapitels III der Richtlinie 95/46/EG über Rechtsbehelfe, Haftung und Sanktionen gelten im Hinblick auf innerstaatliche Vorschriften, die nach der vorliegenden Richtlinie erlassen werden, und im Hinblick auf die aus dieser Richtlinie resultierenden individuellen Rechte.
(3) […]"

2. Art. 13 der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. 1995 L 281, 31, idF der Verordnung (EG) Nr. 1882/2003, ABl. 2003 L 284, 1, lautet – auszugsweise – wie folgt: 89

"ABSCHNITT VI
AUSNAHMEN UND EINSCHRÄNKUNGEN
Artikel 13
Ausnahmen und Einschränkungen
(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Pflichten und Rechte gemäß Artikel 6 Absatz 1, Artikel 10, Artikel 11 Absatz 1, Artikel 12 und Artikel 21 beschränken, sofern eine solche Beschränkung notwendig ist für
a) die Sicherheit des Staates;
b) die Landesverteidigung;
c) die öffentliche Sicherheit;
d) die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen;
e) ein wichtiges wirtschaftliches oder finanzielles Interesse eines Mitgliedstaats oder der Europäischen Union einschließlich Währungs-, Haushalts- und Steuerangelegenheiten;
f) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben c), d) und e) genannten Zwecke verbunden sind;
g) den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen.
(2) […]"

3. In den vorliegenden Anträgen wird u.a. die Aufhebung von Bestimmungen des Bundesgesetzes, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 – TKG 2003), BGBl. I 70/2003, begehrt. Die Anträge 90

richten sich teils gegen näher bezeichnete Bestimmungen des TKG 2003 idF BGBl. I 27/2011 (so der Antrag der Kärntner Landesregierung zu G 47/2012, siehe oben I.1.1), teils gegen näher bezeichnete Bestimmungen des TKG 2003 idF BGBl. I 102/2011 (so die Anträge zu G 59/2012, G 62,70,71/2012, siehe oben I.3.1 und I.5.1).

3.1. Die maßgeblichen Bestimmungen des TKG 2003, BGBl. I 70/2003 idF BGBl. I 27/2011, lauten – auszugsweise – wie folgt (die angefochtenen Gesetzesbestimmungen sind hervorgehoben): 91

"1. Abschnitt
Allgemeines
Zweck

§ 1. (1) Zweck dieses Bundesgesetzes ist es, durch Förderung des Wettbewerbes im Bereich der elektronischen Kommunikation die Versorgung der Bevölkerung und der Wirtschaft mit zuverlässigen, preiswerten, hochwertigen und innovativen Kommunikationsdienstleistungen zu gewährleisten.
(2)-(3) […]
(4) Durch dieses Bundesgesetz werden folgende Richtlinien der Europäischen Union umgesetzt:
1.-5. […]
6. Richtlinie 2006/24/EG 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, ABl. Nr. L 105 vom 13. April 2006, S 54.

[…]

Informationspflichten

§ 90 (1)-(5) […]
(6) Anbieter 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) Anbieter von Kommunikationsdiensten sind auf schriftliches Verlangen der zuständigen Gerichte, Staatsanwaltschaften oder der Kriminalpolizei (§ 76a Abs. 1 StPO) verpflichtet, diesen zur Aufklärung und Verfolgung des konkreten Verdachts einer Straftat Auskunft über Stammdaten (§ 92 Abs. 3 Z 3) von Teilnehmern zu geben. Dies gilt sinngemäß für Verlangen der Sicherheitsbehörden

nach Maßgabe des § 53 Abs. 3a Z 1 SPG. In dringenden Fällen können aber solche Ersuchen vorläufig mündlich übermittelt werden.
(8) Anbieter 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.

[…]

12. Abschnitt

Kommunikationsgeheimnis, Datenschutz Allgemeines

§ 92. (1) Soweit dieses Bundesgesetz nicht anderes bestimmt, sind auf die in diesem Bundesgesetz geregelten Sachverhalte die Bestimmungen des Datenschutzgesetzes 2000, BGBl. I Nr. 165/1999, anzuwenden.
(2) Die Bestimmungen der Strafprozessordnung bleiben durch die Bestimmungen dieses Abschnittes unberührt.
(3) In diesem Abschnitt bezeichnet unbeschadet des § 3 der Begriff
1. “Anbieter” Betreiber von öffentlichen Kommunikationsdiensten;
2. “Benutzer” eine natürliche Person, die einen öffentlichen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst zwangsläufig abonniert zu haben;
2a. „Teilnehmerkennung“ jene Kennung, welche die eindeutige Zuordnung eines Kommunikationsvorgangs zu einem Teilnehmer ermöglicht;
2b. „E-Mail-Adresse“ die eindeutige Kennung, die einem elektronischen Postfach von einem Internet-E-Mail-Anbieter zugewiesen wird;
3. „Stammdaten“ alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer 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),
d) Teilnehmernummer und sonstige Kontaktinformation für die Nachricht,
e) Information über Art und Inhalt des Vertragsverhältnisses,
f) Bonität;
4. “Verkehrsdaten” Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden;
4a. “Zugangsdaten” jene Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind;
5. “Inhaltsdaten” die Inhalte übertragener Nachrichten (Z 7);

6. “Standortdaten” Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben;
6a. „Standortkennung“ die Kennung einer Funkzelle, über welche eine Mobilfunkverbindung hergestellt wird (Cell-ID);
6b. „Vorratsdaten“ Daten, die ausschließlich aufgrund der Speicherverpflichtung gemäß § 102a gespeichert werden;
7. “Nachricht” jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht Informationen ein, die als Teil eines Rundfunkdienstes über ein Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Teilnehmer oder Nutzer, der sie erhält, in Verbindung gebracht werden können;
8. „Anruf“ eine über einen öffentlichen Telefondienst aufgebaute Verbindung, die eine zwei- oder mehrseitige Echtzeit-Kommunikation ermöglicht;
8a. „erfolgloser Anrufversuch“ einen Telefonanruf, bei dem die Verbindung erfolgreich aufgebaut wurde, der aber unbeantwortet bleibt oder bei dem das Netzwerkmanagement eingegriffen hat;
9.-16. […]

Kommunikationsgeheimnis

§ 93. (1) Dem Kommunikationsgeheimnis unterliegen die Inhaltsdaten, die Verkehrsdaten und die Standortdaten. Das Kommunikationsgeheimnis erstreckt sich auch auf die Daten erfolgloser Verbindungsversuche.
(2) Zur Wahrung des Kommunikationsgeheimnisses ist jeder Betreiber und alle Personen, die an der Tätigkeit des Betreibers mitwirken, verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.
(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 sowie für eine technische Speicherung, die für die Weiterleitung einer Nachricht erforderlich ist.
(4) […]
(5) Das Redaktionsgeheimnis (§ 31 Mediengesetz) sowie sonstige, in anderen Bundesgesetzen normierte Geheimhaltungsverpflichtungen sind nach Maßgabe des Schutzes der geistlichen Amtsverschwiegenheit und von Berufsgeheimnissen sowie das Verbot deren Umgehung gemäß §§ 144 und 157 Abs. 2 StPO zu beachten. Den Anbieter trifft keine entsprechende Prüfpflicht.

Technische Einrichtungen

§ 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. Für die Bereitstellung sind dem Anbieter 80% der Kosten (Personal- und Sachaufwendungen), die er aufwenden musste, um die gemäß den Abs. 3 und 4 erlassenen Verordnungen erforderlichen Funktionen in seinen Anlagen einzurichten, zu ersetzen. Der Bundesminister für Verkehr, Innovation und Technologie hat im Einvernehmen mit dem Bundesminister für Inneres, dem Bundesminister für Justiz und dem Bundesminister für Finanzen durch Verordnung die Bemessungsgrundlage für diesen Prozentsatz sowie die Modalitäten für die Geltendmachung dieses Ersatzanspruches festzusetzen. 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, sowie auf die Einfachheit und Kostengünstigkeit des Verfahrens Bedacht zu nehmen.

(2) Der Anbieter 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, sowie der öffentlichen Aufgabe der Rechtspflege Bedacht zu nehmen.

(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.

(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 Übertragungstechnologie, welche die Identifikation und Authentifizierung von Sender und Empfänger sowie die Datenintegrität sicherstellt, zu erfolgen. Die Daten sind unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie als “Comma-Separated Value (CSV)“ - Dateiformat zu übermitteln. Ausgenommen davon ist die Übermittlung von Daten

in den Fällen des § 98, von Daten in den Fällen von § 99 Abs. 5 Z 3 und 4 bei Gefahr in Verzug, von Standortdaten in den Fällen der Feststellung des aktuellen Standortes gemäß §§ 134 ff StPO sowie die Übermittlung von begleitenden Rufdaten im Rahmen einer Überwachung von Nachrichten. 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 Speicherung und Übermittlung der Daten sowie die näheren Bestimmungen betreffend die Speicherung der gemäß § 102c angefertigten Protokolle festsetzen. Nach Erlass der Verordnung ist unmittelbar dem Hauptausschuss des Nationalrates zu berichten.

[…]

Auskünfte an Betreiber von Notrufdiensten

§ 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 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.

(2) Ist eine aktuelle Standortfeststellung nicht möglich, darf die Standortkennung (Cell-ID) zum letzten Kommunikationsvorgang der Endeinrichtung des gefährdeten Menschen verarbeitet werden, auch wenn 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 frühestens nach 48 Stunden, jedoch spätestens nach 30 Tagen grundsätzlich durch Versand einer Kurzmitteilung (SMS), wenn dies nicht möglich ist schriftlich, zu informieren. Diese Information hat zu enthalten:

a) die Rechtsgrundlage,

b) die betroffene Daten,

c) das Datum und die Uhrzeit der Abfrage,

d) Angabe der Stelle, von der die Standortfeststellung in Auftrag gegeben wurde, sowie eine entsprechende Kontaktinformation.

Verkehrsdaten

§ 99. (1) Verkehrsdaten dürfen außer in den in diesem Gesetz geregelten Fällen nicht gespeichert oder übermittelt werden und sind vom Anbieter nach Beendi-

gung der Verbindung unverzüglich zu löschen oder zu anonymisieren. Die Zulässigkeit der weiteren Verwendung von Verkehrsdaten, die nach Abs. 5 übermittelt werden, richtet sich nach den Vorschriften der StPO sowie des SPG.
(2) Sofern dies für Zwecke der Verrechnung von Entgelten, einschließlich der Entgelte für Zusammenschaltungen, erforderlich ist, hat der Betreiber Verkehrsdaten bis zum Ablauf jener Frist zu speichern, innerhalb derer die Rechnung rechtlich angefochten werden oder der Anspruch auf Zahlung geltend gemacht werden kann. Diese Daten sind im Streitfall der entscheidenden Einrichtung sowie der Schlichtungsstelle unverkürzt zur Verfügung zu stellen. Wird ein Verfahren über die Höhe der Entgelte eingeleitet, dürfen die Daten bis zur endgültigen Entscheidung über die Höhe der Entgelte nicht gelöscht werden. Der Umfang der gespeicherten Verkehrsdaten ist auf das unbedingt notwendige Minimum zu beschränken.
(3)-(4) […]
(5) Eine Verarbeitung von Verkehrsdaten zu Auskunftszwecken ist zulässig zur Auskunft über
1. Daten einer Nachrichtenübermittlung gemäß § 134 Z 2 StPO;
2. Zugangsdaten, auch wenn diese als Vorratsdaten gemäß § 102a Abs. 2 Z 1, Abs. 3 Z 6 lit. a und b oder § 102a Abs. 4 Z 1, 2, 3 und 5 längstens sechs Monate vor der Anfrage gespeichert wurden, an Gerichte und Staatsanwaltschaften nach Maßgabe des § 76a Abs. 2 StPO.
3. Verkehrsdaten und Stammdaten, wenn hiefür die Verarbeitung von Verkehrsdaten erforderlich ist, sowie zur Auskunft über Standortdaten an nach dem SPG zuständige Sicherheitsbehörden nach Maßgabe des § 53 Abs. 3a und 3b SPG. Ist eine aktuelle Standortfeststellung nicht möglich, darf die Standortkennung (Cell-ID) zum letzten Kommunikationsvorgang der Endeinrichtung verarbeitet werden, auch wenn hiefür ein Zugriff auf gemäß § 102a Abs. 3 Z 6 lit. d gespeicherte Vorratsdaten erforderlich ist;
4. Zugangsdaten, auch wenn diese als Vorratsdaten gemäß § 102a Abs. 2 Z 1 oder § 102a Abs. 4 Z 1, 2, 3 und 5 längstens drei Monate vor der Anfrage gespeichert wurden, an nach dem SPG zuständige Sicherheitsbehörden nach Maßgabe des § 53 Abs. 3a Z 3 SPG.

[…]

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 zur Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a 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 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.
(6) Die Speicherpflicht nach Abs. 1 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 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. 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.

Auskunft über Vorratsdaten

§ 102b. (1) Eine Auskunft über Vorratsdaten ist ausschließlich aufgrund einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft zur Aufklärung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a StPO rechtfertigt, 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.
(3) Die Übermittlung der Daten hat in angemessen geschützter Form nach Maßgabe des § 94 Abs. 4 zu erfolgen.

Datensicherheit, Protokollierung und Statistik

§ 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 dazu ermächtigten Personen unter Einhaltung des Vier-Augen-Prinzips vorbehalten ist. Die Protokolldaten sind drei Jahre ab Ende der Speicherfrist für das betreffende Vorratsdatum zu speichern. Die Kontrolle über die Einhaltung dieser Vorschriften obliegt der für die Datenschutzkontrolle gemäß § 30 DSG 2000 zuständigen Datenschutzkommission. Eine nähere Beschreibung des Sorgfaltsmaßstabs zur Gewährleistung der Datensicherheit kann der Bundesminister für Verkehr, Innovation und Technologie per Verordnung festschreiben.

(2) Die gemäß § 102a zur Speicherung verpflichteten Anbieter haben zu gewährleisten, dass jeder Zugriff auf Vorratsdaten sowie jede Anfrage und jede Auskunft über Vorratsdaten nach § 102b revisionssicher protokolliert wird. Diese Protokollierung umfasst
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,
2. in den Fällen des § 99 Abs. 5 Z 3 und 4 die dem Anbieter mit dem Auskunftsbegehren bekannt gegebene Aktenzahl der Sicherheitsbehörde,
3. das Datum der Anfrage sowie das Datum und den genauen Zeitpunkt der erteilten Auskunft,
4. die nach Datum und Kategorien gemäß § 102a Abs. 2 bis 4 aufgeschlüsselte Anzahl der übermittelten Datensätze,
5. die Speicherdauer der übermittelten Daten zum Zeitpunkt der Anordnung der Übermittlung,
6. den Namen und die Anschrift des von der Auskunft über Vorratsdaten betroffenen Teilnehmers, soweit der Anbieter über diese Daten verfügt sowie
7. eine eindeutige Kennung, welche eine Zuordnung der Personen ermöglicht, die im Unternehmen des Anbieters auf Vorratsdaten zugegriffen haben.
(3) Die Speicherung der Protokolldaten hat so zu erfolgen, dass deren Unterscheidung von Vorratsdaten sowie von nach Maßgabe der §§ 96, 97, 99, 101 und 102 gespeicherter Daten möglich ist.
(4) Die gemäß § 102a zur Speicherung verpflichteten Anbieter haben
1. für Zwecke der Kontrolle des Datenschutzes und zur Gewährleistung der Datensicherheit die Protokolldaten gemäß Abs. 2 an die Datenschutzkommission und den Datenschutzrat sowie
2. zum Zweck der Berichterstattung an die Europäische Kommission und an den Nationalrat die Protokolldaten gemäß Abs. 2 Z 2 bis 4 an den Bundesminister für Justiz zu übermitteln.
(5) Die Übermittlung der Protokolldaten hat auf schriftliches Ersuchen der Datenschutzkommission bzw. des Bundesministers für Justiz zu erfolgen; die Übermittlung an den Bundesminister muss darüber hinaus jährlich bis zum 31. Jänner für das vorangegangene Kalenderjahr erfolgen.
(6) Über die Protokollierungspflichten nach Abs. 2 hinaus ist eine Speicherung der übermittelten Datensätze selbst unzulässig.

[…]

Verwaltungsstrafbestimmungen

§ 109. (1)-(2) […]
(3) Eine Verwaltungsübertretung begeht und ist mit einer Geldstrafe bis zu 37 000 Euro zu bestrafen, wer
1.-21. […]

22. 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;
23. entgegen § 102a Abs. 8 Daten nicht löscht;
24. entgegen § 102b Daten ohne Vorliegen einer gerichtlichen Bewilligung beauskunftet;
25. entgegen § 102b Daten in nicht verschlüsselter Form über ein Kommunikationsnetz übermittelt;
26. entgegen § 102c nicht protokolliert oder die notwendigen Auskünfte erteilt.
(4)-(9) […]

[…]

In-Kraft-Treten

§ 137. (1)-(3) […]
(4) §§ 94 Abs. 1 und 102a Abs. 1 in der Fassung des Bundesgesetzes BGBl. I Nr. 27/2011 treten am 1. April 2012 in Kraft."

3.2. § 1 Abs. 4 TKG 2003, BGBl. I 70/2003 idF BGBl. I 102/2011, lautet – auszugsweise – wie folgt (die angefochtene Gesetzesbestimmung ist hervorgehoben): 92

"(4) Durch dieses Bundesgesetz werden folgende Richtlinien der Europäischen Union umgesetzt:
1.-6. […]
7. Richtlinie 2006/24/EG 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, ABl. Nr. L 105 vom 13. April 2006, S 54."

3.3. Die übrigen der in den Anträgen zu G 59/2012 und G 62,70,71/2012 angefochtenen Bestimmungen des TKG 2003 hatten durch das Bundesgesetz, mit dem das Telekommunikationsgesetz 2003, das KommAustria-Gesetz sowie das Verbraucherbehörden-Kooperationsgesetz geändert werden (BGBl. I 102/2011), keine Änderung erfahren. Sie standen nach Inkrafttreten des letzteren Bundesgesetzes in der ihnen durch das Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird (BGBl. I 27/2011), gegebenen Fassung (siehe oben 3.1) in Geltung. 93

3.4. Mit 1. Jänner 2014 trat in § 102c Abs. 1, 4 und 5 TKG 2003 an die Stelle des Begriffs "Datenschutzkommission" der Begriff "Datenschutzbehörde" (Art. 2 des Bundesgesetzes, mit dem das Datenschutzgesetz 2000 geändert wird [DSG-Novelle 2014], BGBl. I 83/2013). 94

4. Das Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz – SPG), BGBl. 566/1991 idF BGBl. I 13/2012 lautet – auszugsweise – wie folgt (die angefochtenen Gesetzesbestimmungen sind hervorgehoben): 95

"2. Hauptstück
Ermittlungsdienst Aufgabenbezogenheit

§ 52. Personenbezogene Daten dürfen von den Sicherheitsbehörden gemäß diesem Hauptstück nur verwendet werden, soweit dies zur Erfüllung der ihnen übertragenen Aufgaben erforderlich ist. Ermächtigungen nach anderen Bundesgesetzen bleiben unberührt.

Zulässigkeit der Verarbeitung

§ 53. (1) Die Sicherheitsbehörden dürfen personenbezogene Daten ermitteln und weiterverarbeiten

1. für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht (§ 19);
2. für die Abwehr krimineller Verbindungen (§§ 16 Abs. 1 Z 2 und 21);
2a. für die erweiterte Gefahrenerforschung (§ 21 Abs. 3) unter den Voraussetzungen des § 91c Abs. 3;
3. für die Abwehr gefährlicher Angriffe (§§ 16 Abs. 2 und 3 sowie 21 Abs. 2); einschließlich der im Rahmen der Gefahrenabwehr notwendigen Gefahrenerforschung (§ 16 Abs. 4 und § 28a);
4. für die Vorbeugung wahrscheinlicher gefährlicher Angriffe gegen Leben, Gesundheit, Sittlichkeit, Freiheit, Vermögen oder Umwelt (§ 22 Abs. 2 und 3) oder für die Vorbeugung gefährlicher Angriffe mittels Kriminalitätsanalyse, wenn nach der Art des Angriffes eine wiederholte Begehung wahrscheinlich ist;
5. für Zwecke der Fahndung (§ 24);
6. um bei einem bestimmten Ereignis die öffentliche Ordnung aufrechterhalten zu können;
7. für die Analyse und Bewertung der Wahrscheinlichkeit einer Gefährdung der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit durch die Verwirklichung eines Tatbestandes nach dem Vierzehnten und Fünfzehnten Abschnitt des Strafgesetzbuches.

(2) Die Sicherheitsbehörden dürfen Daten, die sie in Vollziehung von Bundes- oder Landesgesetzen verarbeitet haben, für die Zwecke und unter den Voraussetzungen nach Abs. 1 ermitteln und weiterverarbeiten; ein automationsunterstützter Datenabgleich im Sinne des § 141 StPO ist ihnen jedoch untersagt. Bestehende Übermittlungsverbote bleiben unberührt.

(3) Die Sicherheitsbehörden sind berechtigt, von den Dienststellen der Gebietskörperschaften, den anderen Körperschaften des öffentlichen Rechtes und den von diesen betriebenen Anstalten Auskünfte zu verlangen, die sie für die Abwehr gefährlicher Angriffe, für die erweiterte Gefahrenerforschung unter den Voraussetzungen nach Abs. 1 oder für die Abwehr krimineller Verbindungen benötigen.

Eine Verweigerung der Auskunft ist nur zulässig, soweit andere öffentliche Interessen die Abwehrinteressen überwiegen oder eine über die Amtsverschwiegenheit (Art. 20 Abs. 3 B-VG) hinausgehende sonstige gesetzliche Verpflichtung zur Verschwiegenheit besteht.
(3a) Die Sicherheitsbehörden sind berechtigt, von Betreibern öffentlicher Telekommunikationsdienste (§ 92 Abs. 3 Z 1 Telekommunikationsgesetz 2003 - TKG 2003, BGBl. I Nr. 70) und sonstigen Diensteanbietern (§ 3 Z 2 E-Commerce-Gesetz - ECG, BGBl. I Nr. 152/2001) Auskünfte zu verlangen:
1. über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses wenn dies zur Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben erforderlich ist,
2. über die Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung, wenn sie diese Daten als wesentliche Voraussetzung zur Abwehr
a) einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht (§ 19),
b) eines gefährlichen Angriffs (§ 16 Abs. 1 Z 1) oder
c) einer kriminellen Verbindung (§ 16 Abs.1 Z 2) benötigen,
3. über Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, wenn sie diese Daten als wesentliche Voraussetzung zur Abwehr
a) einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht (§ 19),
b) eines gefährlichen Angriffs (§ 16 Abs. 1 Z 1) oder
c) einer kriminellen Verbindung (§ 16 Abs. 1 Z 2) benötigen,
auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 4 iVm § 102a TKG 2003 erforderlich ist,
4. über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer, wenn dies zur Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder zur Abwehr gefährlicher Angriffe erforderlich ist.
(3b) Ist auf Grund bestimmter Tatsachen anzunehmen, dass eine gegenwärtige Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen besteht, sind die Sicherheitsbehörden zur Hilfeleistung oder Abwehr dieser Gefahr berechtigt, von Betreibern öffentlicher Telekommunikationsdienste Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) der von dem gefährdeten oder diesen begleitenden Menschen mitgeführten Endeinrichtung zu verlangen, auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 iVm § 102a TKG 2003 erforderlich ist, sowie technische Mittel zur Lokalisierung der Endeinrichtung zum Einsatz zu bringen.
(3c) In den Fällen der Abs. 3a und 3b trifft die Sicherheitsbehörde die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens. Die ersuchte Stelle ist verpflichtet, die Auskünfte unverzüglich und im Fall des Abs. 3b gegen Ersatz der Kosten nach der Überwachungskostenverordnung – ÜKVO, BGBl. II Nr. 322/2004, zu erteilen. Im Falle des Abs. 3b hat die Sicherheitsbehörde dem Betreiber überdies unverzüglich, spätestens innerhalb von 24 Stunden eine

schriftliche Dokumentation nachzureichen. In den Fällen des Abs. 3a Z 3 sowie Abs. 3b ist die Sicherheitsbehörde verpflichtet, den Betroffenen darüber zu informieren, dass eine Auskunft zur Zuordnung seines Namens oder seiner Anschrift zu einer bestimmten IP-Adresse (§ 53 Abs. 3a Z 3) oder zur Standortbeauskunftung (§ 53 Abs. 3b) eingeholt wurde, sofern hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 oder 4 iVm § 102a TKG 2003 erforderlich war. Dabei sind dem Betroffenen nachweislich und ehestmöglich die Rechtsgrundlage sowie das Datum und die Uhrzeit der Anfrage bekannt zu geben. Die Information Betroffener kann aufgeschoben werden, solange durch sie der Ermittlungszweck gefährdet wäre, und kann unterbleiben, wenn der Betroffene bereits nachweislich Kenntnis erlangt hat oder die Information des Betroffenen unmöglich ist.

(3d) Die Sicherheitsbehörden sind zur Vorbeugung und Abwehr gefährlicher Angriffe gegen die Umwelt berechtigt, von Behörden des Bundes, der Länder und Gemeinden Auskünfte über von diesen genehmigte Anlagen und Einrichtungen zu verlangen, bei denen wegen der Verwendung von Maschinen oder Geräten, der Lagerung, Verwendung oder Produktion von Stoffen, der Betriebsweise, der Ausstattung oder aus anderen Gründen besonders zu befürchten ist, dass im Falle einer Abweichung der Anlage oder Einrichtung von dem der Rechtsordnung entsprechenden Zustand eine Gefahr für das Leben, die Gesundheit mehrerer Menschen oder in großem Ausmaß eine Gefahr für Eigentum oder Umwelt entsteht. Die ersuchte Behörde ist verpflichtet, die Auskunft zu erteilen.

(4) Abgesehen von den Fällen der Abs. 2 bis 3b und 3d sind die Sicherheitsbehörden für Zwecke des Abs. 1 berechtigt, personenbezogene Daten aus allen anderen verfügbaren Quellen durch Einsatz geeigneter Mittel, insbesondere durch Zugriff auf allgemein zugängliche Daten, zu ermitteln und weiterzuverarbeiten.

(5) Die Sicherheitsbehörden sind im Einzelfall und unter den Voraussetzungen des § 54 Abs. 3 ermächtigt, für die Abwehr gefährlicher Angriffe und krimineller Verbindungen, wenn bestimmte Tatsachen auf eine schwere Gefahr für die öffentliche Sicherheit schließen lassen, für die erweiterte Gefahrenerforschung (§ 21 Abs. 3) und zur Fahndung (§ 24) personenbezogene Bilddaten zu verwenden, die Rechtsträger des öffentlichen oder privaten Bereichs mittels Einsatz von Bild- und Tonaufzeichnungsgeräten rechtmäßig ermittelt und den Sicherheitsbehörden übermittelt haben. Dabei ist besonders darauf zu achten, dass Eingriffe in die Privatsphäre der Betroffenen die Verhältnismäßigkeit (§ 29) zum Anlass wahren. Nicht zulässig ist die Verwendung von Daten über nichtöffentliches Verhalten."

5. Die Strafprozeßordnung 1975 (StPO), BGBl. 631 idF BGBl. I 35/2012, lautet – auszugsweise – wie folgt (die angefochtenen Gesetzesbestimmungen sind hervorgehoben): 96

"5. Abschnitt

Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Auskunft über Vorratsdaten sowie Überwachung von Nachrichten und von Personen Definitionen

§ 134. Im Sinne dieses Bundesgesetzes ist

1. […]

2. Auskunft über Daten einer Nachrichtenübermittlung" die Erteilung einer Auskunft über Verkehrsdaten (§ 92 Abs. 3 Z 4 TKG), Zugangsdaten (§ 92 Abs. 3 Z 4a TKG), die nicht einer Anordnung gemäß § 76a Abs. 2 unterliegen, und Standortdaten (§ 92 Abs. 3 Z 6 TKG) eines Telekommunikationsdienstes oder eines Dienstes der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes),

2a. „Auskunft über Vorratsdaten" die Erteilung einer Auskunft über Daten, die Anbieter von öffentlichen Kommunikationsdiensten nach Maßgabe des § 102a Abs. 2 bis 4 TKG zu speichern haben und die nicht nach § 99 Abs. 2 TKG einer Auskunft nach Z 2 unterliegen,

3.-5. […]

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 Abs. 2 Z 2 bis 4 zulässig.

(3) Überwachung von Nachrichten ist zulässig,

1. in den Fällen des Abs. 2 Z 1,

2. in den Fällen des Abs. 2 Z 2, 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 (lit. a) dringend verdächtige Person die technische Einrichtung benützen oder mit ihr eine Verbindung herstellen werde;
4. in den Fällen des Abs. 2 Z 4."

5.1. Die vom Drittantragsteller angefochtenen Bestimmungen der StPO idF BGBl. I 53/2012 weichen von den dargestellten Bestimmungen nicht ab. 97

6. Die maßgeblichen Bestimmungen des Bundesgesetzes über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000), BGBl. I 165/1999 in der geltenden Fassung, BGBl. I 83/2013, lauten – auszugsweise – wie folgt: 98

"Artikel 1
(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 Art. 8 Abs. 2 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 Abs. 3 sind nur unter den in Abs. 2 genannten Voraussetzungen zulässig.

[…]

6. Abschnitt
Rechtsschutz
Kontrollbefugnisse der Datenschutzbehörde

§ 30. (1) Jedermann kann sich wegen einer behaupteten Verletzung seiner Rechte oder ihn betreffender Pflichten eines Auftraggebers oder Dienstleisters nach diesem Bundesgesetz mit einer Eingabe an die Datenschutzbehörde wenden.
(2) Die Datenschutzbehörde kann im Fall eines begründeten Verdachtes auf Verletzung der im Abs. 1 genannten Rechte und Pflichten Datenanwendungen überprüfen. Hiebei kann sie vom Auftraggeber oder Dienstleister der überprüften Datenanwendung insbesondere alle notwendigen Aufklärungen verlangen und Einschau in Datenanwendungen und diesbezügliche Unterlagen begehren.
(2a) Sofern sich eine zulässige Eingabe nach Abs. 1 oder ein begründeter Verdacht nach Abs. 2 auf eine meldepflichtige Datenanwendung (Datei) bezieht, kann die Datenschutzbehörde die Erfüllung der Meldepflicht überprüfen und erforderlichenfalls nach den §§ 22 und 22a vorgehen.
(3) Datenanwendungen, die der Vorabkontrolle gemäß § 18 Abs. 2 unterliegen, dürfen auch ohne Vorliegen eines Verdachts auf rechtswidrige Datenverwendung überprüft werden. Dies gilt auch für jene Bereiche der Vollziehung, in welchen ein Auftraggeber des öffentlichen Bereichs die grundsätzliche Anwendbarkeit der §§ 26 Abs. 5 und 27 Abs. 5 in Anspruch nimmt.
(4) Zum Zweck der Einschau ist die Datenschutzbehörde nach Verständigung des Inhabers der Räumlichkeiten und des Auftraggebers (Dienstleisters) berechtigt, Räume, in welchen Datenanwendungen vorgenommen werden, zu betreten, Datenverarbeitungsanlagen in Betrieb zu setzen, die zu überprüfenden Verarbeitungen durchzuführen sowie Kopien von Datenträgern in dem für die Ausübung der Kontrollbefugnisse unbedingt erforderlichen Ausmaß herzustellen. Der Auftraggeber (Dienstleister) hat die für die Einschau notwendige Unterstützung

zu leisten. Die Kontrolltätigkeit ist unter möglichster Schonung der Rechte des Auftraggebers (Dienstleisters) und Dritter auszuüben.
(5) Informationen, die der Datenschutzbehörde oder ihren Beauftragten bei der Kontrolltätigkeit zukommen, dürfen ausschließlich für die Kontrolle im Rahmen der Vollziehung datenschutzrechtlicher Vorschriften verwendet werden. Dazu zählt auch die Verwendung für Zwecke der gerichtlichen Rechtsverfolgung durch den Einschreiter oder die Datenschutzbehörde nach § 32. Im Übrigen besteht die Pflicht zur Verschwiegenheit auch gegenüber Gerichten und Verwaltungsbehörden, insbesondere Abgabenbehörden; dies allerdings mit der Maßgabe, dass dann, wenn die Einschau den Verdacht einer strafbaren Handlung nach den §§ 51 oder 52 dieses Bundesgesetzes, einer strafbaren Handlung nach den §§ 118a, 119, 119a, 126a bis 126c, 148a oder § 278a des Strafgesetzbuches, BGBl. Nr. 60/1974, oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, ergibt, Anzeige zu erstatten ist und hinsichtlich solcher Verbrechen und Vergehen auch Ersuchen nach § 76 der Strafprozessordnung, BGBl. Nr. 631/1975, zu entsprechen ist.
(6) Zur Herstellung des rechtmäßigen Zustandes kann die Datenschutzbehörde, sofern nicht Maßnahmen nach den §§ 22 und 22a oder nach Abs. 6a zu treffen sind, Empfehlungen aussprechen, für deren Befolgung erforderlichenfalls eine angemessene Frist zu setzen ist. Wird einer solchen Empfehlung innerhalb der gesetzten Frist nicht entsprochen, so kann die Datenschutzbehörde je nach der Art des Verstoßes von Amts wegen insbesondere
1. Strafanzeige nach §§ 51 oder 52 erstatten, oder
2. bei schwerwiegenden Verstößen durch Auftraggeber des privaten Bereichs Klage vor dem zuständigen Gericht gemäß § 32 Abs. 5 erheben, oder
3. bei Verstößen von Auftraggebern, die Organe einer Gebietskörperschaft sind, das zuständige oberste Organ befassen. Dieses Organ hat innerhalb einer angemessenen, jedoch zwölf Wochen nicht überschreitenden Frist entweder dafür Sorge zu tragen, dass der Empfehlung der Datenschutzbehörde entsprochen wird, oder der Datenschutzbehörde mitzuteilen, warum der Empfehlung nicht entsprochen wurde. Die Begründung darf von der Datenschutzbehörde der Öffentlichkeit in geeigneter Weise zur Kenntnis gebracht werden, soweit dem nicht die Amtsverschwiegenheit entgegensteht.
(6a) Liegt durch den Betrieb einer Datenanwendung eine wesentliche unmittelbare Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen (Gefahr im Verzug) vor, so kann die Datenschutzbehörde die Weiterführung der Datenanwendung mit Bescheid gemäß § 57 Abs. 1 des Allgemeinen Verwaltungsverfahrensgesetzes 1991 – AVG, BGBl. Nr. 51, untersagen. Wenn dies technisch möglich, im Hinblick auf den Zweck der Datenanwendung sinnvoll und zur Beseitigung der Gefährdung ausreichend scheint, kann die Weiterführung auch nur teilweise untersagt werden. Wird einer Untersagung nicht sogleich Folge geleistet, ist Strafanzeige nach § 52 Abs. 1 Z 3 zu erstatten. Nach Rechtskraft einer Untersagung nach diesem Absatz ist ein Berichtigungsverfahren nach

§ 22a Abs. 2 formlos einzustellen. Die Datenanwendung ist im Umfang der Untersagung aus dem Register zu streichen.
(7) Der Einschreiter ist darüber zu informieren, wie mit seiner Eingabe verfahren wurde.

Beschwerde an die Datenschutzbehörde

§ 31. (1) Die Datenschutzbehörde erkennt über Beschwerden von Personen oder Personengemeinschaften, die behaupten, in ihrem Recht auf Auskunft nach § 26 oder nach § 50 Abs. 1 dritter Satz oder in ihrem Recht auf Darlegung einer automatisierten Einzelentscheidung nach § 49 Abs. 3 verletzt zu sein, soweit sich das Auskunftsverlangen (der Antrag auf Darlegung oder Bekanntgabe) nicht auf die Verwendung von Daten für Akte im Dienste der Gesetzgebung oder der Gerichtsbarkeit bezieht.
(2) Die Datenschutzbehörde erkennt weiters über Beschwerden von Personen oder Personengemeinschaften, die behaupten, in ihrem Recht auf Geheimhaltung (§ 1 Abs. 1) oder in ihrem Recht auf Richtigstellung oder auf Löschung (§§ 27 und 28) verletzt zu sein, sofern der Anspruch nicht nach § 32 Abs. 1 vor einem Gericht geltend zu machen ist oder sich gegen ein Organ im Dienste der Gesetzgebung oder der Gerichtsbarkeit richtet.
(3) Die Beschwerde hat zu enthalten:
1. die Bezeichnung des als verletzt erachteten Rechts,
2. soweit dies zumutbar ist, die Bezeichnung des Rechtsträgers oder Organs, dem die behauptete Rechtsverletzung zugerechnet wird (Beschwerdegegner),
3. den Sachverhalt, aus dem die Rechtsverletzung abgeleitet wird,
4. die Gründe, auf die sich die Behauptung der Rechtswidrigkeit stützt,
5. das Begehren, die behauptete Rechtsverletzung festzustellen und
6. die Angaben, die erforderlich sind, um zu beurteilen, ob die Beschwerde rechtzeitig eingebracht ist.
(4) Einer Beschwerde nach Abs. 1 sind außerdem das zu Grunde liegende Auskunftsverlangen (der Antrag auf Darlegung oder Bekanntgabe) und eine allfällige Antwort des Beschwerdegegners anzuschließen. Einer Beschwerde nach Abs. 2 sind außerdem der zu Grunde liegende Antrag auf Richtigstellung oder Löschung und eine allfällige Antwort des Beschwerdegegners anzuschließen.
(5) Die der Datenschutzbehörde durch § 30 Abs. 2 bis 4 eingeräumten Kontrollbefugnisse kommen ihr auch in Beschwerdeverfahren nach Abs. 1 und 2 gegenüber dem Beschwerdegegner zu. Ebenso besteht auch hinsichtlich dieser Verfahren die Verschwiegenheitspflicht nach § 30 Abs. 5.
(6) Im Fall der Einbringung einer zulässigen Beschwerde nach Abs. 1 oder 2 ist ein auf Grund einer Eingabe nach § 30 Abs. 1 über denselben Gegenstand eingeleitetes Kontrollverfahren durch eine entsprechende Information (§ 30 Abs. 7) zu beenden. Die Datenschutzbehörde kann aber dennoch auch während der Anhängigkeit des Beschwerdeverfahrens von Amts wegen nach § 30 Abs. 2 vorgehen, wenn ein begründeter Verdacht einer über den Beschwerdefall hinausgehenden Verletzung datenschutzrechtlicher Verpflichtungen besteht. § 30 Abs. 3 bleibt unberührt.
(7) Soweit sich eine Beschwerde nach Abs. 1 oder 2 als berechtigt erweist, ist ihr Folge zu geben und die Rechtsverletzung festzustellen. Ist eine festgestellte

Verletzung im Recht auf Auskunft (Abs. 1) einem Auftraggeber des privaten Bereichs zuzurechnen, so ist diesem auf Antrag zusätzlich die – allenfalls erneute – Reaktion auf das Auskunftsbegehren nach § 26 Abs. 4, 5 oder 10 in jenem Umfang aufzutragen, der erforderlich ist, um die festgestellte Rechtsverletzung zu beseitigen. Soweit sich die Beschwerde als nicht berechtigt erweist, ist sie abzuweisen.

(8) Ein Beschwerdegegner, gegen den wegen Verletzung in Rechten nach den §§ 26 bis 28 Beschwerde erhoben wurde, kann bis zum Abschluss des Verfahrens vor der Datenschutzbehörde durch Reaktionen gegenüber dem Beschwerdeführer gemäß § 26 Abs. 4 oder § 27 Abs. 4 die behauptete Rechtsverletzung nachträglich beseitigen. Erscheint der Datenschutzbehörde durch derartige Reaktionen des Beschwerdegegners die Beschwerde als gegenstandslos, so hat sie den Beschwerdeführer dazu zu hören. Gleichzeitig ist er darauf aufmerksam zu machen, dass die Datenschutzbehörde das Verfahren formlos einstellen wird, wenn er nicht innerhalb einer angemessenen Frist begründet, warum er die ursprünglich behauptete Rechtsverletzung zumindest teilweise nach wie vor als nicht beseitigt erachtet. Wird durch eine derartige Äußerung des Beschwerdeführers die Sache ihrem Wesen nach geändert (§ 13 Abs. 8 AVG), so ist von der Zurückziehung der ursprünglichen Beschwerde und der gleichzeitigen Einbringung einer neuen Beschwerde auszugehen. Auch diesfalls ist das ursprüngliche Beschwerdeverfahren formlos einzustellen und der Beschwerdeführer davon zu verständigen. Verspätete Äußerungen sind nicht zu berücksichtigen.

[…]

Anrufung der Gerichte

§ 32. (1) Ansprüche wegen Verletzung der Rechte einer Person oder Personengemeinschaft auf Geheimhaltung, auf Richtigstellung oder auf Löschung gegen natürliche Personen, Personengemeinschaften oder Rechtsträger, die in Formen des Privatrechts eingerichtet sind, sind, soweit diese Rechtsträger bei der behaupteten Verletzung nicht in Vollziehung der Gesetze tätig geworden sind, auf dem Zivilrechtsweg geltend zu machen.

(2) Sind Daten entgegen den Bestimmungen dieses Bundesgesetzes verwendet worden, so hat der Betroffene Anspruch auf Unterlassung und Beseitigung des diesem Bundesgesetz widerstreitenden Zustandes.

(3) Zur Sicherung der auf dieses Bundesgesetz gestützten Ansprüche auf Unterlassung können einstweilige Verfügungen erlassen werden, auch wenn die in § 381 EO bezeichneten Voraussetzungen nicht zutreffen. Dies gilt auch für Verfügungen über die Verpflichtung zur Anbringung eines Bestreitungsvermerks.

(4) Für Klagen und Anträge auf Erlassung einer einstweiligen Verfügung nach diesem Bundesgesetz ist in erster Instanz das mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betraute Landesgericht zuständig, in dessen Sprengel der Kläger (Antragsteller) seinen gewöhnlichen Aufenthalt oder Sitz hat. Klagen (Anträge) können aber auch bei dem Landesgericht erhoben werden, in dessen Sprengel der Beklagte seinen gewöhnlichen Aufenthalt oder Sitz oder eine Niederlassung hat.

(5) Die Datenschutzbehörde hat in Fällen, in welchen der begründete Verdacht einer schwerwiegenden Datenschutzverletzung durch einen Auftraggeber des privaten Bereichs besteht, gegen diesen eine Feststellungsklage (§ 228 ZPO) bei dem gemäß Abs. 4 zweiter Satz zuständigen Gericht zu erheben.
(6) Die Datenschutzbehörde hat, wenn ein Einschreiter (§ 30 Abs. 1) es verlangt und es zur Wahrung der nach diesem Bundesgesetz geschützten Interessen einer größeren Zahl von natürlichen Personen geboten ist, einem Rechtsstreit auf Seiten des Einschreiters als Nebenintervenient (§§ 17 ff ZPO) beizutreten.
(7) Anlässlich einer zulässigen Klage nach Abs. 1, die sich auf eine nach Ansicht des Gerichts meldepflichtige Datenanwendung bezieht, kann das Gericht die Datenschutzbehörde um Überprüfung nach den §§ 22 und 22a ersuchen. Die Datenschutzbehörde hat das Gericht vom Ergebnis der Überprüfung zu verständigen. Dieses ist sodann vom Gericht auch den Parteien bekannt zu geben, sofern das Verfahren noch nicht rechtskräftig beendet ist."

III. Erwägungen

Der Verfassungsgerichtshof hat über die in sinngemäßer Anwendung der §§ 187 und 404 ZPO iVm § 35 Abs. 1 VfGG zur gemeinsamen Verhandlung, Beratung und Entscheidung verbundenen Anträge erwogen: 99

1. Prozessvoraussetzungen

1.1. Der Verfassungsgerichtshof ging in seinem Beschluss vom 28. November 2012, VfSlg. 19.702/2012, mit dem dem Gerichtshof der Europäischen Union Fragen zur Vorabentscheidung vorgelegt wurden (siehe oben I.8), für die Zwecke des Gesetzesprüfungsverfahrens vorläufig davon aus, dass der Antrag der Kärntner Landesregierung zu G 47/2012 und die Individualanträge zu G 59/2012 und zu G 62,70,71/2012 zulässig sind (siehe IV.1.1. des Beschlusses vom 28. November 2012, VfSlg. 19.702/2012). Im nunmehr fortzusetzenden Gesetzesprüfungsverfahren ist die Zulässigkeit der Anträge im Einzelnen zu prüfen. 100

1.2. Der Gerichtshof der Europäischen Union hat mit seinem Urteil in den verbundenen Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland und Seitlinger ua.*, vom 8. April 2014 (siehe dazu oben I.9), das u.a. auf Grund eines Vorabentscheidungsersuchens des Verfassungsgerichtshofes (VfSlg. 19.702/2012) ergangen ist, die Vorratsdatenspeicherungsrichtlinie für ungültig erklärt, ohne die zeitliche Wirkung der Ungültigerklärung zu beschrän- 101

ken. Die Ungültigerklärung wirkt daher zeitlich zurück (vgl. EuGH 13.5.1981, Rs 66/80, *International Chemical Corporation*, Slg. 1981, 1191 [Rz 13 ff.]). Die Vorratsdatenspeicherungsrichtlinie wurde damit mit Wirkung ex tunc aus dem Bestand des Unionsrechts ausgeschieden (vgl. allgemein zur zeitlichen Wirkung von Urteilen des Gerichtshofes der Europäischen Union in Vorabentscheidungsverfahren, mit denen Unionsrecht für ungültig erklärt wird, zB *Kadelbach*, Die Wirkungen von im Vorabentscheidungsverfahren ergangenen Urteilen, in: Holoubek/Lang [Hrsg.], Das EuGH-Verfahren in Steuersachen, 2000, 119 [126 ff.]; *B. Schima*, Das Vorabentscheidungsverfahren vor dem EuGH², 2004, 106 ff.; *Öhlinger/Potacs*, EU-Recht und staatliches Recht[5], 2014, 76 f.).

1.3. Eine unmittelbare Anwendung von Bestimmungen der Vorratsdatenspeicherungsrichtlinie oder anderer unionsrechtlicher Bestimmungen, die den Verfassungsgerichtshof allenfalls zur Wahrnehmung des Anwendungsvorrangs des Unionsrechts veranlassen müsste und die sich insbesondere auf die Zulässigkeit der Individualanträge zu G 59/2012 und zu G 62,70,71/2012 auswirken würde (vgl. zB VfSlg. 15.771/2000, 17.508/2005, 18.298/2007), kommt daher nicht in Betracht. 102

1.4. Zum Antrag zu G 47/2012: 103

1.4.1. Gemäß Art. 140 Abs. 1 Z 2 B-VG erkennt der Verfassungsgerichtshof über die Verfassungswidrigkeit eines Bundesgesetzes auch auf Antrag einer Landesregierung. Der Antrag der Kärntner Landesregierung ist ein solcher Antrag. 104

1.4.2. Die Grenzen der Aufhebung einer auf ihre Verfassungsmäßigkeit hin zu prüfenden Gesetzesbestimmung sind, wie der Verfassungsgerichtshof sowohl für von Amts wegen als auch für auf Antrag eingeleitete Gesetzesprüfungsverfahren schon wiederholt dargelegt hat (VfSlg. 13.965/1994 mwN, 16.542/2002, 16.911/2003), notwendig so zu ziehen, dass einerseits der verbleibende Gesetzesteil nicht einen völlig veränderten Inhalt bekommt und dass andererseits die mit der aufzuhebenden Gesetzesstelle untrennbar zusammenhängenden Bestimmungen auch erfasst werden. 105

1.4.3. Dieser Grundposition folgend darf im Gesetzesprüfungsverfahren der Anfechtungsumfang der in Prüfung gezogenen Norm bei sonstiger Unzulässigkeit des Prüfungsantrags nicht zu eng gewählt werden (vgl. zB VfSlg. 8155/1977, 12.235/1989, 13.915/1994, 14.131/1995, 14.498/1996, 14.890/1997, 16.212/2002). Die Antragsteller haben all jene Normen anzufechten, welche für die Beurteilung der allfälligen Verfassungswidrigkeit der Rechtslage eine untrennbare Einheit bilden. Es ist Sache des Verfassungsgerichtshofes, darüber zu befinden, auf welche Weise eine solche Verfassungswidrigkeit – sollte der Verfassungsgerichtshof die Auffassung des antragstellenden Gerichtes teilen – beseitigt werden kann (VfSlg. 16.756/2002, 19.496/2011). Der Umfang einer zu prüfenden und allenfalls aufzuhebenden Bestimmung ist derart abzugrenzen, dass einerseits nicht mehr aus dem Rechtsbestand ausgeschieden wird, als zur Beseitigung der zulässigerweise geltend gemachten Rechtswidrigkeit erforderlich ist, dass aber andererseits der verbleibende Teil keine Veränderung seiner Bedeutung erfährt; da beide Ziele gleichzeitig niemals vollständig erreicht werden können, ist in jedem Einzelfall abzuwägen, ob und inwieweit diesem oder jenem Ziel der Vorrang vor dem anderen gebührt (vgl. VfSlg. 19.496/2011 mwN). 106

1.4.4. Vor diesem Hintergrund erweist sich der Antrag der Kärntner Landesregierung als unzulässig, da der Umfang der angefochtenen Rechtsvorschriften zu eng gefasst ist. Dadurch, dass die antragstellende Landesregierung zwar eine Vielzahl an Bestimmungen im TKG 2003, die ihrer Ansicht nach in untrennbarem Zusammenhang mit der Vorratsdatenspeicherung und insbesondere § 102a TKG 2003 stünden, angefochten hat, nicht aber jene Bestimmungen in der StPO und im SPG, die die "Beauskunftung" der Vorratsdaten regeln, hat sie nicht alle Bestimmungen angefochten, die für die Beurteilung der allfälligen Verfassungswidrigkeit der Regelungen über die Vorratsdatenspeicherung eine untrennbare Einheit bilden (vgl. dazu unten III.2.3). 107

1.4.5. Der Antrag der Kärntner Landesregierung ist daher schon aus diesem Grund zurückzuweisen. 108

1.5. Zum Antrag zu G 59/2012: 109

1.5.1. Gemäß Art. 140 Abs. 1 Z 1 lit. c B-VG erkennt der Verfassungsgerichtshof über die Verfassungswidrigkeit von Gesetzen auf Antrag einer Person, die unmit- 110

telbar durch diese Verfassungswidrigkeit in ihren Rechten verletzt zu sein behauptet, wenn das Gesetz ohne Fällung einer gerichtlichen Entscheidung oder ohne Erlassung eines Bescheides für diese Person wirksam geworden ist. Wie der Verfassungsgerichtshof in seiner mit VfSlg. 8009/1977 beginnenden ständigen Rechtsprechung ausgeführt hat, ist daher grundlegende Voraussetzung für die Antragslegitimation, dass das Gesetz in die Rechtssphäre der betroffenen Person unmittelbar eingreift und sie – im Fall seiner Verfassungswidrigkeit – verletzt. Hiebei hat der Verfassungsgerichtshof vom Antragsvorbringen auszugehen und lediglich zu prüfen, ob die vom Antragsteller ins Treffen geführten Wirkungen solche sind, wie sie Art. 140 Abs. 1 Z 1 lit. c B-VG als Voraussetzung für die Antragslegitimation fordert (vgl. zB VfSlg. 11.730/1988, 15.863/2000, 16.088/2001, 16.120/2001).

1.5.2. Nicht jedem Normadressaten aber kommt die Anfechtungsbefugnis zu. Es ist darüber hinaus erforderlich, dass das Gesetz selbst tatsächlich in die Rechtssphäre des Antragstellers unmittelbar eingreift. Ein derartiger Eingriff ist jedenfalls nur dann anzunehmen, wenn dieser nach Art und Ausmaß durch das Gesetz selbst eindeutig bestimmt ist, wenn er die (rechtlich geschützten) Interessen des Antragstellers nicht bloß potentiell, sondern aktuell beeinträchtigt und wenn dem Antragsteller kein anderer zumutbarer Weg zur Abwehr des – behaupteterweise – rechtswidrigen Eingriffes zur Verfügung steht (VfSlg. 11.868/1988, 15.632/1999, 16.616/2002, 16.891/2003). 111

1.5.3. Hinsichtlich der Kriterien der Rechtsprechung für den Umfang der im vorliegenden Individualantrag beantragten Aufhebung von gesetzlichen Bestimmungen kann auf die Ausführungen zum Antrag der Kärntner Landesregierung unter 1.4.2 und 1.4.3 verwiesen werden. 112

1.5.4. Der Individualantrag richtet sich gegen § 102a TKG 2003 sowie näher bezeichnete Bestimmungen, die in untrennbarem Zusammenhang mit § 102a TKG 2003 stünden. Der Zweitantragsteller bekämpft eventualiter auch § 134 Z 2a und § 135 Abs. 2a StPO sowie näher bezeichnete Wortfolgen in § 53 Abs. 3a Z 3 und § 53 Abs. 3b SPG, weil diese in untrennbarem Zusammenhang mit § 102a TKG 2003 stünden (siehe oben I.10.2). 113

1.5.5. Nach Ansicht der Bundesregierung sei Adressat des § 102a TKG 2003 nicht ein "Endkunde" wie der Zweitantragsteller. Er sei daher von dieser Bestimmung nicht rechtlich betroffen. Dem ist entgegenzuhalten, dass sich die angefochtene Bestimmung des § 102a TKG 2003 auf Grund ihrer sprachlichen Fassung – wie die Bundesregierung in ihren Äußerungen betont – zwar lediglich an "Anbieter von öffentlichen Kommunikationsdiensten", "Anbieter von Internet-Zugangsdiensten", "Anbieter öffentlicher Telefondienste einschließlich Internet-Telefondiensten" und "Anbieter von E-Mail-Diensten" richtet. Sie ist jedoch ihrem Inhalt und Zweck nach von einer solchen Wirkung auf den Zweitantragsteller als "Benutzer" (vgl. § 92 Abs. 3 Z 2 TKG 2003) von öffentlichen Kommunikationsdiensten, dass damit nicht nur dessen tatsächliche Situation berührt wird, sondern auch in die – insbesondere auch durch die verfassungsgesetzlich gewährleisteten Rechte aus Art. 8 EMRK und § 1 DSG 2000 geprägte – Rechtssphäre des Zweitantragstellers eingegriffen wird. Der Zweitantragsteller ist daher jedenfalls dem Zweck und Inhalt dieser angefochtenen Bestimmung nach als Normadressat anzusehen (vgl. VfSlg. 13.038/1992, 13.558/1993, 19.349/2011). 114

1.5.6. Zur Frage eines zumutbaren anderen Weges, um Bedenken an den Verfassungsgerichtshof heranzutragen, ist Folgendes festzuhalten: 115

1.5.6.1. Auf Grund der Anordnung in § 102a TKG 2003 sind die dort genannten Anbieter verpflichtet, bestimmte, den Zweitantragsteller betreffende Daten zu speichern. Die Verpflichtung und Ermächtigung zur Speicherung trifft den Zweitantragsteller unmittelbar in seiner Rechtssphäre, ohne dass es noch eines konkretisierenden Rechtsaktes bedürfte oder ein solcher vorgesehen wäre. Anders als in Fällen, in denen beispielsweise staatliche Einrichtungen durch die Rechtsordnung ermächtigt werden, bestimmte Maßnahmen zu ergreifen, die unter Umständen und erst im Fall ihrer Inanspruchnahme zu einer Beeinträchtigung der Rechtssphäre Rechtsunterworfener führen (vgl. zB VfSlg. 18.831/2009), liegen im vorliegenden Fall jene Umstände, die in die Rechtssphäre eingreifen, schon durch die andauernde Speicherverpflichtung und deren Befolgung vor. 116

1.5.6.2. Unter den Umständen des vorliegenden Falles kann der Verfassungsgerichtshof nicht finden, dass dem Zweitantragsteller ein zumutbarer anderer Weg zur Verfügung stünde, um die durch die behauptete Rechtswidrigkeit der angefochtenen Bestimmungen bewirkte Rechtsverletzung wirksam abzuwehren: 117

1.5.6.3. Die von der Bundesregierung in ihren Äußerungen im Wesentlichen ins Treffen geführten Wege zur Geltendmachung der behaupteten Verfassungswidrigkeiten, Feststellungsbescheide oder Entscheidungen der ordentlichen Gerichte nach dem DSG 2000 zu erwirken, sind nicht geeignet, eine für den Zweitantragsteller zumutbare Alternative zur Stellung eines Individualantrags aufzuzeigen. 118

1.5.6.4. Die Bundesregierung scheint einerseits davon auszugehen, dass der Zweitantragsteller hinsichtlich der nach § 102a TKG 2003 gespeicherten Daten Auskunftsbegehren gemäß § 26 DSG 2000 hätte erheben können, um sich in der Folge mit einer Beschwerde an die (seinerzeitige) Datenschutzkommission zu wenden, mit der Behauptung, im Recht auf Auskunft nach § 26 DSG 2000 verletzt zu sein. Die Datenschutzkommission hätte dann mit Bescheid über die Beschwerde zu entscheiden gehabt. Gegen diesen hätte Beschwerde nach Art. 144 B-VG erhoben werden können. Auf diesem Wege hätten die Bedenken im Hinblick auf die Verfassungsmäßigkeit der Bestimmungen über die Vorratsdatenspeicherung an den Verfassungsgerichtshof herangetragen werden können. Andererseits bringt die Bundesregierung vor, der Zweitantragsteller hätte im Wege eines Zivilprozesses die Löschung der auf Vorrat gespeicherten Daten begehren können (§ 27 iVm § 32 DSG 2000). Die dazu berufenen Gerichte (vgl. § 32 Abs. 4 DSG 2000) hätten in der Folge allfällige Verfassungswidrigkeiten der von ihnen anzuwendenden Bestimmungen vor dem Verfassungsgerichtshof geltend zu machen gehabt (vgl. Art. 89 Abs. 2 zweiter Satz, Art. 140 Abs. 1 Z 1 lit. a B-VG). 119

1.5.6.5. Es ist zutreffend, dass der Verfassungsgerichtshof u.a. im Zusammenhang mit Bestimmungen des SPG ausgesprochen hat, dass Personen, die den konkreten Verdacht hegen, dass ihre Daten auf Grund der Bestimmungen des SPG ermittelt wurden, die Erwirkung eines Feststellungsbescheids über das Auskunftsrecht gemäß § 26 DSG 2000, die Erwirkung eines Bescheids über das Löschungsrecht gemäß § 27 DSG 2000, das Beschwerderecht gemäß § 31 DSG 2000 iVm § 90 SPG, sowie die Eingabe an die (seinerzeitige) Datenschutzkommission gemäß § 30 Abs. 1 DSG 2000, die im Fall eines begründeten Verdachts zu einer Systemprüfung gemäß § 30 Abs. 2 DSG 2000 führen kann, als zumutbare Wege zur Verfügung stehen bzw. standen (VfSlg. 18.831/2009). Der 120

Verfassungsgerichtshof sieht im Hinblick auf den vorliegenden Antrag keinen Anlass, von dieser Rechtsprechung abzugehen.

1.5.6.6. Die genannten Wege der Rechtsverfolgung erweisen sich im konkreten Fall jedoch als nicht zumutbar. Zu bedenken ist zunächst, dass der Zweitantragsteller durch die angefochtenen Bestimmungen insofern unmittelbar und aktuell betroffen ist, als er jedenfalls davon ausgehen muss, dass bestimmte, ihn betreffende Daten – wenn auch nicht jedenfalls von staatlichen Einrichtungen ermittelt, so doch auf gesetzliche Anordnung hin, nämlich auf Grund der Anordnung in § 102a Abs. 1 TKG 2003, zum Zweck der "Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs. 2a StPO rechtfertigt" – gespeichert wurden und werden. In § 102a Abs. 1 TKG 2003 wird festgelegt, dass diese Daten nicht nur in Ausnahmefällen und betreffend einen bestimmten, eingeschränkten Personenkreis zu speichern sind, sondern dass von der Verpflichtung zur Speicherung *alle* Anbieter von öffentlichen Kommunikationsdiensten nach Maßgabe der Abs. 2 bis 4 dieser Bestimmung ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation erfasst sind. 121

1.5.6.7. Es trifft zu, dass sich der Zweitantragsteller mit einem Auskunftsbegehren nach § 26 DSG 2000 oder einem Löschungsbegehren nach § 27 DSG 2000 an jene Anbieter von öffentlichen Kommunikationsdiensten richten hätte können, hinsichtlich derer er weiß, dass sie Daten über ihn speichern. In weiterer Folge hätte er die Reaktionen der Anbieter im Rechtsweg entsprechend bekämpfen können. Auch wenn der Zweitantragsteller theoretisch unmittelbar (Art. 144 B-VG) oder mittelbar (Art. 89 Abs. 2 zweiter Satz, Art. 140 Abs. 1 Z 1 lit. a B-VG) seine Bedenken ob der Verfassungsmäßigkeit der in Rede stehenden Bestimmungen an den Verfassungsgerichtshof herantragen könnte, so bestehen im vorliegenden Fall außergewöhnliche, besondere Umstände, die den Zweitantragsteller davon entbinden, diesen Weg zu beschreiten: 122

1.5.6.8. Wie der Verfassungsgerichtshof im Zusammenhang mit nach Art. 139 und 140 B-VG gestellten Individualanträgen wiederholt festgestellt hat, ist den von einer generellen Rechtsvorschrift Betroffenen nur bei Vorliegen besonderer, außergewöhnlicher Umstände das Recht auf Einbringung eines Verordnungs- oder Gesetzesprüfungsantrags eingeräumt, wenn die grundsätzliche Möglichkeit 123

besteht, ein gerichtliches oder verwaltungsbehördliches Verfahren anhängig zu machen, das diesen Personen letztlich Gelegenheit bieten würde, die Einleitung eines amtswegigen Normenprüfungsverfahrens durch den Verfassungsgerichtshof anzuregen; andernfalls gelangte man zu einer Doppelgleisigkeit des Rechtsschutzes, die mit dem Grundsatz, dass der Individualantrag ein bloß subsidiärer Rechtsbehelf ist, nicht im Einklang stünde (vgl. zB VfSlg. 8312/1978, 11.344/1987, 15.786/2000, 18.182/2007, 19.126/2010).

1.5.6.9. Die besonderen und außergewöhnlichen Umstände sind folgende: Durch die Verpflichtung zur Speicherung nach § 102a TKG 2003 und die Auskunftserteilung nach den § 135 Abs. 2a StPO sowie § 53 SPG liegt ein großer Kreis an Daten vor, die entweder bei den Anbietern von öffentlichen Kommunikationsdiensten oder (nach Erteilung von Auskünften) bei den Sicherheits- oder Strafverfolgungsbehörden gespeichert sind. Die Speicherungsverpflichtung trifft im Übrigen nicht nur jene Anbieter, mit denen der Zweitantragsteller Verträge hatte oder hat, sondern auch die Anbieter der "Kommunikationspartner" des Zweitantragstellers, dh. jener Personen, mit denen der Zweitantragsteller zB telefonierte oder denen er E-Mails sandte (vgl. § 102a Abs. 3 Z 1 und Z 3 TKG 2003; für Mobilfunknetze § 102a Abs. 3 Z 6 TKG 2003; für E-Mail-Dienste § 102a Abs. 4 Z 3 und Z 4 TKG 2003). Der Zweitantragsteller ist mit einer kaum überblickbaren Anzahl an Anbietern konfrontiert, die über ihn auf Grund des § 102a TKG 2003 Daten gespeichert haben könnten. Es ist praktisch nicht möglich, zu eruieren, welcher Anbieter welche Daten in welchen Zeiträumen auf Grund des § 102a TKG 2003 gespeichert hat oder speichert. 124

1.5.6.10. Überdies ist zu bedenken, dass für den Fall, dass der Zweitantragsteller ein gerichtliches Löschungsverfahren betreffend die über ihn gespeicherten Vorratsdaten im Hinblick auf einen Anbieter führen würde, weiterhin fortlaufend Daten auf Grund des § 102a TKG 2003 bei Anbietern gespeichert werden. Die Daten, deren Löschung der Zweitantragsteller gerichtlich begehren würde, wären im Zeitpunkt, in dem der Verfassungsgerichtshof über einen Antrag nach Art. 89 Abs. 2 B-VG zu entscheiden hätte, bereits gelöscht, womit die Zulässigkeit des Antrages in Frage stünde. 125

1.5.6.11. Diese Umstände entsprechen nach dem Gewicht des drohenden Nachteils jenen Umständen, deretwegen der Verfassungsgerichtshof schon bisher die Beschreitung des an sich zur Verfügung stehenden anderen Weges für unzumutbar erachtet hat (vgl. VfSlg. 11.853/1988, 12.379/1990, 15.786/2000). 126

1.5.7. Im Hinblick auf diese Besonderheiten der Vorratsdatenspeicherung stand dem Zweitantragsteller kein zumutbarer anderer Weg als ein Individualantrag zur Verfügung. 127

1.5.8. Der Antrag erweist sich jedoch insoweit als unzulässig, als die Aufhebung des § 1 Abs. 4 Z 5 (gemeint: Z 7) TKG 2003 begehrt wird, weil diese Bestimmung ebenfalls mit BGBl. I 27/2011 kundgemacht worden sei und "in der geltenden Fassung (BGBl. I 102/2011)" bekämpft werde sowie in untrennbarem Zusammenhang mit § 102a TKG 2003 stehe und den "Hinweis über die Umsetzung der Richtlinie 2006/24/EG" beinhalte. 128

1.5.8.1. Wie oben dargelegt wurde (siehe 1.5.1), hat der Verfassungsgerichtshof bei der Beurteilung der Zulässigkeit eines Individualantrags ausschließlich von den Angaben im Antrag auszugehen. 129

1.5.8.2. Vor diesem Hintergrund vermag der Zweitantragsteller aber nicht darzulegen, inwiefern die zur Aufhebung beantragte Rechtsvorschrift in Widerspruch zu einer verfassungsgesetzlichen Bestimmung stehen soll und worin der geltend gemachte "untrennbare Zusammenhang" zwischen den in § 102a TKG 2003 gesehenen Verfassungswidrigkeiten und der angefochtenen Bestimmung liegen soll. Der Antrag auf Aufhebung des § 1 Abs. 4 Z 7 TKG 2003 ist daher zurückzuweisen. 130

1.5.9. § 102c Abs. 1, 4 und 5 TKG 2003 in der angefochtenen Fassung wurde gemäß Art. 2 der DSG-Novelle 2014, BGBl. I 83/2013, mit Wirkung vom 1. Jänner 2014 durch eine neue Fassung ersetzt. Da sich der Antrag insoweit gegen Bestimmungen richtet, die bereits außer Kraft getreten sind, ist der Antrag in dieser Hinsicht zurückzuweisen. 131

1.5.10. Soweit sich der Antrag nicht gegen § 1 Abs. 4 Z 7 und gegen § 102c Abs. 1, 4 und 5 TKG 2003 richtet, ist er zulässig. 132

1.6. Zum Antrag zu G 62,70,71/2012: 133

1.6.1. Im Hinblick auf den Drittantragsteller ist nichts hervorgekommen, was zu einer vom Antrag zu G 59/2012 abweichenden Beurteilung führen würde (siehe oben 1.5). 134

1.6.2. Auch dieser Antrag ist zulässig. 135

2. In der Sache

2.1. Der Verfassungsgerichtshof hat sich in einem auf Antrag eingeleiteten Verfahren zur Prüfung der Verfassungsmäßigkeit eines Gesetzes gemäß Art. 140 B-VG auf die Erörterung der aufgeworfenen Fragen zu beschränken (vgl. VfSlg. 12.691/1991, 13.471/1993, 14.895/1997, 16.824/2003). Er hat sohin ausschließlich zu beurteilen, ob die angefochtene Bestimmung aus den in der Begründung des Antrages dargelegten Gründen verfassungswidrig ist (VfSlg. 15.193/1998, 16.374/2001, 16.538/2002, 16.929/2003). 136

2.2. Zum Prüfungsmaßstab: 137

2.2.1. In den vorliegenden Anträgen wird geltend gemacht, die angefochtenen Bestimmungen verstießen gegen § 1 DSG 2000, Art. 8 EMRK sowie gegen die Art. 7 und 8 GRC. 138

2.2.2. Wie der Verfassungsgerichtshof bereits in seinem Beschluss VfSlg. 19.702/2012, mit dem er den Gerichtshof der Europäischen Union um Vorabentscheidung ersucht hat, ausgeführt hat, enthält das Bundesverfassungsrecht neben Art. 8 EMRK ein selbständiges 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 Abs. 1 DSG 2000, siehe oben II.6). § 1 Abs. 2 DSG 2000 enthält einen materiellen Gesetzesvorbehalt, demzufolge abgesehen von der Verwendung von personen- 139

bezogenen Daten im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig sind, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 EMRK genannten Gründen notwendig sind.

2.2.3. Für die gesetzliche Grundlage verlangt § 1 Abs. 2 DSG 2000 über Art. 8 Abs. 2 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. 140

2.2.4. Der Verfassungsgerichtshof hat im Beschluss VfSlg. 19.702/2012 erwogen, dass die Vorratsdatenspeicherungsrichtlinie – dies war der Grund für das Vorabentscheidungsverfahren – nur in einer das Grundrecht des § 1 DSG 2000 verletzenden Weise umgesetzt werden könnte und dem Verfassungsgerichtshof als Folge dessen eine Prüfung der gesetzlichen Regelungen über die Vorratsdatenspeicherung verwehrt sein könnte (vgl. VfSlg. 15.427/1999). Da insoweit kein Spielraum zu einer verfassungskonformen Umsetzung bestünde, wäre dem Verfassungsgerichtshof eine Prüfung der gesetzlichen Regelungen am Maßstab des § 1 DSG 2000 verwehrt. Mit der Nichtigerklärung der Richtlinie durch den Gerichtshof der Europäischen Union ist diese Erwägung hinfällig, sodass § 1 DSG 2000 und Art. 8 EMRK jedenfalls wieder uneingeschränkt Maßstab im Gesetzesprüfungsverfahren sind. 141

2.2.5. Dieses Ergebnis steht im Einklang damit, dass der Gerichtshof der Europäischen Union angesichts der Ungültigkeit der Vorratsdatenspeicherungsrichtlinie die Beantwortung der zur Auslegung der Art. 7, 8, 52 und 53 GRC gestellten Fragen (siehe oben I.8) nicht für erforderlich hielt (EuGH, *Digital Rights Ireland und Seitlinger ua.*, Rz 72). 142

2.2.6. An diesem Ergebnis ändert auch Art. 15 Abs. 1 zweiter Satz RL 2002/58/EG nichts. Die Regelung bestimmt lediglich, dass die Mitgliedstaaten durch Rechtsvorschriften vorsehen können, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden können. Solche 143

Maßnahmen müssen "den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen" (Art. 15 Abs. 1 letzter Satz RL 2002/58/EG). Gemäß Art. 15 Abs. 2 RL 2002/58/EG gelten die Bestimmungen des Kapitels III der Richtlinie 95/46/EG über Rechtsbehelfe, Haftung und Sanktionen im Hinblick auf innerstaatliche Vorschriften, die nach der RL 2002/58/EG erlassen werden, und im Hinblick auf die aus dieser Richtlinie resultierenden individuellen Rechte. Nähere Bestimmungen zur Umsetzung der in Art. 15 Abs. 1 zweiter Satz RL 2002/58/EG vorgesehenen Beschränkung sieht diese Richtlinie jedoch nicht vor, sodass auch deshalb davon auszugehen ist, dass der Gesetzgeber über einen weiten Spielraum bei der Umsetzung verfügt; ein Vorrang gegenüber innerstaatlichem Verfassungsrecht und namentlich den beiden genannten verfassungsgesetzlich gewährleisteten Rechten kommt daher nicht in Betracht.

2.2.7. Auch die Art. 7 und 8 GRC kommen in diesem Gesetzesprüfungsverfahren als Maßstab in Betracht. Wie der Verfassungsgerichtshof im Vorabentscheidungsersuchen VfSlg. 19.702/2012 im Anschluss an seine Vorjudikatur dargelegt hat (VfSlg. 19.632/2012), bilden die von der GRC garantierten Rechte im Anwendungsbereich der GRC (Art. 51 Abs. 1 GRC) einen Prüfungsmaßstab in Verfahren der Normenkontrolle, insbesondere in Verfahren nach Art. 139 und 140 B-VG. Dies gilt jedenfalls dann, wenn die betreffende Garantie der GRC in ihrer Formulierung und Bestimmtheit verfassungsgesetzlich gewährleisteten Rechten der österreichischen Bundesverfassung gleicht. Gesetzliche Regelungen, die in Umsetzung einer Richtlinie ergingen, bilden jedenfalls einen Fall der Durchführung des Unionsrechts (VfSlg. 19.632/2012). Auch wenn die Vorratsdatenspeicherungsrichtlinie nunmehr (mit Wirkung ex tunc) für ungültig erklärt wurde, ergingen die angefochtenen Bestimmungen – insbesondere jene, die mit BGBl. I 27/2011 kundgemacht wurden – schon allein deshalb in Durchführung des Rechts der Union, weil sie im Anwendungsbereich der RL 2002/58/EG und namentlich ihres Art. 15 Abs. 1 erlassen wurden. 144

2.2.8. Wenn der Gesetzgeber in Wahrnehmung seines Umsetzungsspielraums bei der Durchführung von Unionsrecht Regelungen schafft, die neben einem Grundrecht der GRC auch ein (anderes) verfassungsgesetzlich gewährleistetes 145

Recht berühren, entscheidet der Verfassungsgerichtshof auf der Grundlage dieses Rechts, wenn es den gleichen Anwendungsbereich wie das Recht der GRC hat (VfSlg. 19.632/2012) und wenn die Grenzen für zulässige Eingriffe des Gesetzgebers in die verfassungsgesetzlich gewährleisteten Rechten enger oder wenigstens nicht weiter gezogen sind als in den korrespondierenden Rechten der GRC. Davon ist sowohl für Art. 8 EMRK als auch für § 1 DSG 2000 auszugehen:

2.2.8.1. Art. 8 EMRK bestimmt die Auslegung des Art. 7 GRC dergestalt, dass er ihm ausweislich der Erläuterungen zu Art. 7 GRC "entspricht" und folglich die "gleiche Bedeutung und Tragweite" wie dieser hat (Art. 52 Abs. 3 GRC, in diesem Sinne auch die Hinweise auf die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte im Urteil des Gerichtshofes der Europäischen Union, *Digital Rights Ireland und Seitlinger ua.*, Rz 35, 47, 54 f.). 146

2.2.8.2. § 1 DSG 2000 enthält einen materiellen Gesetzesvorbehalt, der die Grenzen für Eingriffe in das Grundrecht enger zieht, als dies Art. 8 Abs. 2 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 Art. 8 Abs. 2 EMRK genannten Gründen notwendig sind. 147

Für die gesetzliche Grundlage verlangt § 1 Abs. 2 DSG 2000 über Art. 8 Abs. 2 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. 148

2.2.9. Nach der Rechtsprechung des Verfassungsgerichtshofes folgt aus dieser Regelung, dass an die Verhältnismäßigkeit des Eingriffs in das Grundrecht auf Datenschutz nach § 1 DSG 2000 ein strengerer Maßstab angelegt werden muss, als er sich bereits aus Art. 8 EMRK ergibt (VfSlg. 16.369/2001, 18.643/2008). 149

Dieses Schutzniveau bleibt von der GRC auch in jenen Fällen unangetastet, in denen der Gesetzgeber über einen Spielraum in Durchführung des Unionsrechts verfügt (vgl. Art. 53 GRC; siehe schon oben 2.2.6). Vor diesem Hintergrund sind die angefochtenen Bestimmungen am Maßstab des Bundesverfassungsrechts, und zwar des § 1 DSG 2000 und des Art. 8 EMRK, zu messen.

2.3. Zu den geltend gemachten Bedenken gegen § 134 Z 2a und § 135 Abs. 2a StPO sowie § 53 Abs. 3a Z 3 und § 53 Abs. 3b SPG und gegen § 102a TKG 2003: 150

2.3.1. Die Antragsteller begehren die Aufhebung des § 102a TKG 2003 u.a. mit der Begründung, dass dieser gegen das durch § 1 DSG 2000 garantierte verfassungsgesetzlich gewährleistete Recht verstoße. § 134 Z 2a und § 135 Abs. 2a StPO sowie § 53 Abs. 3a Z 3 und § 53 Abs. 3b SPG seien "als Einheit mit den Normen zur Speicherpflicht (§ 102a TKG) und zur Verwendung von Vorratsdaten (§ 102b TKG, § 99 Abs. 5 Z 2 bis 4 TKG) zu sehen" (so der Drittantragsteller), auch diese Bestimmungen würden das genannte Grundrecht verletzen, insbesondere, weil die durch die genannten Bestimmungen in der StPO und im SPG gewährten "Zugriffsmöglichkeiten" überschießend seien (so insbesondere der Zweitantragsteller). 151

2.3.2. Durch § 102a Abs. 1 TKG 2003 werden Anbieter von öffentlichen Kommunikationsdiensten (vgl. § 92 Abs. 3 Z 1 TKG 2003) verpflichtet, "über die Berechtigung zur Speicherung oder Verarbeitung gemäß den §§ 96, 97, 99, 101 und 102 hinaus" bestimmte Datenkategorien, die im Zuge der Bereitstellung von öffentlichen Kommunikationsdiensten erzeugt oder verarbeitet werden (vgl. § 102a Abs. 5 erster Satz TKG 2003), ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation zu speichern. Die Speicherung erfolgt nach § 102a Abs. 1 letzter Satz TKG 2003 ausschließlich zur Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs. 2a StPO rechtfertigt. 152

2.3.3. § 135 Abs. 2a StPO bestimmt durch einen Verweis auf § 135 Abs. 2 Z 2 bis 4 StPO, dass eine Auskunft über Vorratsdaten (§ 134 Z 2a StPO) zulässig ist, wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen 153

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 (§ 135 Abs. 2 Z 2 StPO); 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 (§ 135 Abs. 2 Z 3 StPO); oder 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 (§ 135 Abs. 2 Z 4 StPO). Die Auskunft über Vorratsdaten nach § 135 Abs. 2a StPO ist von der Staatsanwaltschaft auf Grund einer gerichtlichen Bewilligung anzuordnen (§ 137 Abs. 1 StPO). Gegen eine derartige Bewilligung kann nach deren Zustellung an den Betroffenen (§ 138 Abs. 5 StPO) Beschwerde gemäß § 87 StPO erhoben werden. Nach § 147 Abs. 1 Z 2a StPO obliegt dem Rechtsschutzbeauftragten die Prüfung und Kontrolle der Anordnung, Genehmigung, Bewilligung und Durchführung der Auskunft über Vorratsdaten nach § 135 Abs. 2a StPO. Gegen die Bewilligung einer Ermittlungsmaßnahme nach § 147 Abs. 1 Z 2a StPO steht dem Rechtsschutzbeauftragten das Recht der Beschwerde zu (§ 147 Abs. 3 StPO). Nach Beendigung der Ermittlungsmaßnahme ist dem Rechtsschutzbeauftragten Gelegenheit zu geben, die gesamten Ergebnisse einzusehen, bevor diese zum Akt genommen werden. Er ist ferner berechtigt, die Vernichtung von Ergebnissen oder Teilen davon zu beantragen und sich von der ordnungsgemäßen Vernichtung dieser Ergebnisse zu überzeugen (§ 147 Abs. 4 StPO).

2.3.4. Nach § 53 Abs. 3a Z 3 SPG sind die Sicherheitsbehörden berechtigt, von Betreibern öffentlicher Kommunikationsdienste Auskunft über Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, zu verlangen, wenn sie diese Daten als wesentliche Voraussetzung zur Abwehr einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht (§ 19 SPG), eines gefährlichen Angriffs (§ 16 Abs. 1 Z 1 SPG) oder einer kriminellen Verbindung (§ 16 Abs. 1 Z 2 SPG) benötigen, "auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 4 iVm § 102a TKG 2003 erforderlich 154

ist". Auf Grund des § 53 Abs. 3b SPG sind die Sicherheitsbehörden des Weiteren berechtigt, von Betreibern öffentlicher Telekommunikationsdienste Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) der von einem gefährdeten oder diesen begleitenden Menschen mitgeführten Endeinrichtung zu verlangen, "auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 iVm § 102a TKG 2003 erforderlich ist."

Voraussetzung einer Auskunftserteilung nach § 53 Abs. 3b SPG ist, dass auf Grund bestimmter Tatsachen anzunehmen ist, dass eine gegenwärtige Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen besteht und die Sicherheitsbehörden im Rahmen der ihnen obliegenden Hilfeleistung oder Gefahrenabwehr einschreiten (§ 53 Abs. 3b SPG). Ein Vorgehen der Sicherheitsbehörden nach den genannten Bestimmungen im SPG bedarf keiner richterlichen Genehmigung. Nach § 91c Abs. 1 SPG ist der Rechtsschutzbeauftragte über diese Auskunftsverlangen "ehestmöglich zu informieren". Ihm obliegt die Prüfung derartiger Meldungen (§ 91c Abs. 1 letzter Satz SPG). 155

2.3.5. Nach § 1 Abs. 1 DSG 2000 hat jedermann Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit er daran ein schutzwürdiges Interesse, insbesondere im Hinblick auf die Achtung des Privat- und Familienlebens, hat. Beschränkungen dieses Grundrechts sind nach dem Gesetzesvorbehalt des § 1 Abs. 2 DSG 2000 (abgesehen von lebenswichtigen Interessen des Betroffenen an der Verwendung personenbezogener Daten oder seiner Zustimmung hiezu) bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen zulässig, die aus den in Art. 8 Abs. 2 EMRK genannten Gründen notwendig sind und die ausreichend präzise, also für jedermann vorhersehbar, regeln, unter welchen Voraussetzungen die Ermittlung bzw. die Verwendung personenbezogener Daten für die Wahrnehmung konkreter Verwaltungsaufgaben erlaubt ist (vgl. VfSlg. 16.369/2001, 18.146/2007, 18.963/2009, 18.975/2009, 19.657/2012, 19.738/2013). 156

Gesetzliche Beschränkungen des Grundrechts auf Datenschutz müssen in einer Abwägung zwischen der Schwere des Eingriffs und dem Gewicht der mit ihnen verfolgten Ziele verhältnismäßig sein (vgl. auch Art. 8 iVm Art. 52 Abs. 1 GRC und 157

EuGH, *Digital Rights Ireland und Seitlinger ua.*, Rz 38, 47, 69 sowie EGMR 4.12.2008 [GK], Fall *S. und Marper*, Appl. 30.562/04, EuGRZ 2009, 299 [Z 101]). 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 (§ 1 Abs. 2 zweiter Satz DSG 2000).

Auch im Fall nach Art. 8 Abs. 2 EMRK zulässiger Beschränkungen darf gemäß dem letzten Satz des § 1 Abs. 2 DSG 2000 der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden. Der jeweilige Gesetzgeber muss daher eine diesen Anforderungen genügende materienspezifische Regelung in dem Sinn vorsehen, dass die Fälle zulässiger Eingriffe in das Grundrecht auf Datenschutz konkretisiert und begrenzt werden (vgl. zB VfSlg. 18.643/2008, 19.657/2012, 19.659/2012, 19.738/2013). 158

2.3.6. Das Grundrecht auf Datenschutz, das durch § 1 DSG 2000 gewährleistet wird, verbürgt einen verfassungsrechtlichen Schutz vor Ermittlung personenbezogener Daten (VfSlg. 12.228/1989, 12.880/1991, 16.369/2001). Bei den nach § 102a TKG 2003 zu speichernden und nach § 135 Abs. 2a StPO und § 53 Abs. 3a Z 3 sowie § 53 Abs. 3b SPG zu beauskunftenden Daten handelt es sich um personenbezogene Daten iSd § 1 Abs. 1 DSG 2000. Insbesondere sind alle der in den Abs. 2 bis 4 des § 102a TKG 2003 angeführten Datenkategorien solche, nach denen die Identität des Betroffenen bestimmt oder zumindest bestimmbar ist. Im Hinblick vor allem auf die auch von den Antragstellern angeführten Möglichkeiten der Verknüpfung mit anderen Informationen (zB den Schlüssen, die aus gehäuften Anrufen einer bestimmten Teilnehmernummer gezogen werden können) besteht an den betroffenen Daten jedenfalls ein schutzwürdiges Geheimhaltungsinteresse iSd § 1 Abs. 1 DSG 2000. 159

2.3.7. Die den Anbietern öffentlicher Kommunikationsdienste durch § 102a Abs. 1 TKG 2003 auferlegte Pflicht zur Speicherung von Daten nach Maßgabe der Abs. 2 bis 4 dieser Bestimmung greift in das Grundrecht auf Datenschutz nach § 1 DSG 2000 sowie in das Recht auf Achtung des Privat- und Familienlebens aus Art. 8 EMRK der Benutzer öffentlicher Kommunikationsdienste ein (VfSlg. 19.738/2013; vgl. Erläut. zur RV der TKG-Novelle BGBl. I 27/2011, 1074 160

BlgNR 24. GP, 21; vgl. auch *Feiel*, Datenspeicherung auf Vorrat und Grundrechtskonformität, jusIT 2008, 97 [99]; zum Eingriff in Art. 8 EMRK ferner VfSlg. 12.689/1991; EGMR 26.3.1987, Fall *Leander*, Appl. 9248/81 [Z 48]; EGMR 16.2.2000 [GK], Fall *Amann*, Appl. 27.798/95, ÖJZ 2001, 71 [Z 65 ff.]; EGMR 4.5.2000 [GK], Fall *Rotaru*, Appl. 28.341/95, ÖJZ 2001, 74 [Z 43]; EGMR 3.4.2007, Fall *Copland*, Appl. 62.617/00, EuGRZ 2007, 415 [Z 43 f.]; EGMR, Fall *S. und Marper*, Z 67; *Kolb*, Vorratsdatenspeicherung, 2011, 113).

2.3.7.1. Der Umstand, dass die Speicherung durch Anbieter öffentlicher Kommunikationsdienste – also durch Private – erfolgt, die durch § 102a TKG 2003 zur Speicherung verpflichtet werden, ändert nichts am Vorliegen eines Eingriffs in § 1 DSG 2000 und Art. 8 EMRK durch den Gesetzgeber. "Anbieter eines Kommunikationsdienstes" ist jeder, der einen Kommunikationsdienst (§ 92 Abs. 3 erster Halbsatz iVm § 3 Z 9 TKG 2003) anbietet, aber – im Gegensatz zum "Betreiber eines Kommunikationsdienstes" (§ 3 Z 3 TKG 2003) – nicht notwendigerweise alle Funktionen dieses Dienstes kontrolliert (*Steinmaurer*, in: Stratil [Hrsg.], TKG[4], 2013, § 92 Anm. 6). Das TKG 2003 geht davon aus, dass sowohl "Anbieter" als auch "Betreiber" von Kommunikationsdiensten (private) Unternehmen sind (siehe nur §§ 1 Abs. 1, 34 ff. TKG 2003). 161

2.3.7.2. Diesen Unternehmen steht hinsichtlich der ihnen in § 102a TKG 2003 auferlegten Speicherpflicht kein Handlungsspielraum zu. Nach § 109 Abs. 3 Z 22 TKG 2003 würden sie eine Verwaltungsübertretung begehen, wenn sie entgegen § 102a TKG 2003 Daten nicht speicherten. 162

2.3.8. Die Speicherung von Daten auf Grund der Verpflichtung nach § 102a TKG 2003 und der Zugriff auf diese ("Beauskunftung") durch Sicherheits- und Strafverfolgungsbehörden – insbesondere auf Grund des § 135 Abs. 2a StPO und des § 53 Abs. 3a Z 3 sowie § 53 Abs. 3b SPG – stellen einen Eingriff in das Grundrecht auf Datenschutz (§ 1 DSG 2000) und das Recht auf Achtung des Privat- und Familienlebens aus Art. 8 EMRK dar (vgl. zB VfGH 1.10.2013, G 2/2013 mwN; zum Eingriff in Art. 8 EMRK ferner EGMR, Fall *Leander*, Z 48; EGMR, Fall *Rotaru*, Z 46; EGMR 29.6.2006 [Zulässigkeitsentscheidung], Fall *Weber und Saravia*, Appl. 54.934/00 [Z 79]). 163

2.3.9. Regelungen, die wie die angefochtenen einen gravierenden Grundrechtseingriff bilden, können zur Bekämpfung schwerer Kriminalität zulässig sein, sofern sie mit den strengen Anforderungen des § 1 DSG 2000 und Art. 8 EMRK im Einklang stehen. Ob ein solcher Eingriff im Hinblick auf § 1 Abs. 2 DSG 2000 und Art. 8 Abs. 2 EMRK zulässig ist, hängt von der Ausgestaltung der Bedingungen der Speicherung von Daten auf Vorrat und den Anforderungen an deren Löschung sowie von den gesetzlichen Sicherungen bei der Ausgestaltung der Möglichkeiten des behördlichen und privaten Zugriffs auf diese Daten ab. Die angefochtenen Vorschriften des TKG 2003, der StPO und des SPG erfüllen diese Anforderungen nicht: 164

2.3.10. Die Vorschriften betreffend die Vorratsdatenspeicherung einschließlich der Bestimmungen über die Erteilung von Auskünften über Vorratsdaten in der StPO und im SPG dienen der Erreichung von in Art. 8 Abs. 2 EMRK genannten Zielen, nämlich insbesondere der Aufrechterhaltung der öffentlichen Ruhe und Ordnung und dem Schutz der Rechte und Freiheiten anderer. Auch konnte der Gesetzgeber im Rahmen seines Beurteilungsspielraums vertretbarerweise davon ausgehen, dass Regelungen über eine Vorratsdatenspeicherung zur Erreichung dieser Ziele abstrakt geeignet sind (vgl. auch EuGH, *Digital Rights Ireland und Seitlinger ua.*, Rz 44 und 49 zu Art. 7 und 8 GRC). 165

2.3.11. Weitere Voraussetzung für die Verhältnismäßigkeit und damit die Zulässigkeit des Eingriffs ist jeweils, dass die Schwere des konkreten Eingriffs nicht das Gewicht und die Bedeutung der mit der Vorratsdatenspeicherung verfolgten Ziele übersteigt. 166

2.3.11.1. Ausgangspunkt der Beurteilung der Verhältnismäßigkeit der Vorratsdatenspeicherung ist die Einsicht, dass das Grundrecht auf Datenschutz in einer demokratischen Gesellschaft – in der hier bedeutsamen Schutzrichtung – auf die Ermöglichung und Sicherung vertraulicher Kommunikation zwischen den Menschen gerichtet ist. Der Einzelne und seine freie Persönlichkeitsentfaltung sind nicht nur auf die öffentliche, sondern auch auf die vertrauliche Kommunikation in der Gemeinschaft angewiesen; die Freiheit als Anspruch des Individuums und als Zustand einer Gesellschaft wird bestimmt von der Qualität der Informationsbeziehungen (vgl. *Berka,* Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT, 2012, Band I/1, 22). 167

2.3.11.2. Bedeutung und Gewicht der mit der Vorratsdatenspeicherung verfolgten Ziele, wie sie der Gesetzgeber auch mit der Zweckbindung in § 102a Abs. 1 letzter Satz TKG 2003 zum Ausdruck bringt, sind erheblich. Doch auch wenn die Regelung ausweislich des Wortlauts des Abs. 1 einem wichtigen öffentlichen Interesse dient (siehe oben 2.3.10), ist es angesichts der "Streubreite" des Eingriffs (siehe unten 2.3.14.3), des Kreises und der Art der betroffenen Daten (siehe unten 2.3.14.5) und der daraus folgenden Schwere des Eingriffs in das Recht auf informationelle Selbstbestimmung (es kann auf Daten zugegriffen werden, welche im Falle ihrer Verknüpfung nicht nur die Erstellung von Bewegungsprofilen ermöglichen, sondern auch Rückschluss auf private Vorlieben und den Bekanntenkreis einer Person zulassen; siehe unten 2.3.14.5) erforderlich, dass der Gesetzgeber durch geeignete Regelungen sicherstellt, dass diese Daten nur bei Vorliegen eines vergleichbar gewichtigen öffentlichen Interesses im Einzelfall für Strafverfolgungsbehörden zugänglich gemacht werden und dies einer richterlichen Kontrolle unterliegt. Dabei ist zu berücksichtigen, dass staatliches Handeln durch die rasche Verbreitung der Nutzung "neuer" Kommunikationstechnologien (zB Mobiltelefonie, E-Mail, Informationsaustausch im Rahmen des World Wide Web, etc.) in den vergangenen zwei Jahrzehnten in vielerlei Hinsicht – nicht zuletzt auch im Rahmen der Bekämpfung der Kriminalität, der die Vorratsdatenspeicherung dienen soll – vor besondere Herausforderungen gestellt wurde und wird. Dieses geänderte Umfeld polizeilicher Ermittlungen hat die Rechtsprechung des Verfassungsgerichtshofes stets berücksichtigt (vgl. zB VfSlg. 16.149/2001, 16.150/2001, 18.830/2009, 18.831/2009, 19.657/2012). Dabei ist zu berücksichtigen, dass die Erweiterung der technischen Möglichkeiten auch dazu führt, dass den Gefahren, die diese Erweiterung für die Freiheit des Menschen in sich birgt, in einer dieser Bedrohung adäquaten Weise entgegengetreten werden muss. 168

2.3.11.3. Der Gerichtshof der Europäischen Union hat in seinem Urteil in der Rs. *Digital Rights Ireland und Seitlinger ua.* betont, dass die Vorratsdatenspeicherungsrichtlinie kein objektives Kriterium vorsieht, das es ermöglicht, den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung zwecks Verhütung, Feststellung oder strafrechtlicher Verfolgung auf Straftaten zu beschränken, die im Hinblick auf das Ausmaß und die Schwere des Eingriffs in 169

die in Art. 7 und Art. 8 der Charta verankerten Grundrechte als hinreichend schwer angesehen werden können, um einen solchen Eingriff zu rechtfertigen (Rz 60). Die Vorratsdatenspeicherungsrichtlinie nehme im Gegenteil in ihrem Art. 1 Abs. 1 lediglich allgemein auf die von jedem Mitgliedstaat in seinem nationalen Recht bestimmten schweren Straftaten Bezug.

2.3.11.4. Die Bundesregierung betont in ihrer Äußerung zum Urteil des Gerichtshofes der Europäischen Union in der Rs. *Digital Rights Ireland und Seitlinger ua.*, dass eine Auskunft über Vorratsdaten gegen den Willen des "Überwachten" erst zulässig sei, wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, zu erwarten ist. Die Beauskunftung von Vorratsdaten im Hinblick auf den Tatbestand des § 135 Abs. 2 Z 2 StPO ziele "nicht zuletzt" darauf ab, Opfern von beharrlicher Verfolgung (§ 107a StGB – sogenanntes "Stalking") eine Möglichkeit der wirksamen Verfolgung von Tätern zu bieten. 170

2.3.11.5. Die Bundesregierung ist mit ihrem Vorbringen, die in § 135 Abs. 2a iVm § 135 Abs. 2 Z 2 bis 4 StPO getroffene Regelung sei hinreichend differenziert und dadurch verhältnismäßig, nicht im Recht. Wie der Gerichtshof der Europäischen Union betont hat, soll die Vorratsdatenspeicherungsrichtlinie zur Bekämpfung schwerer Kriminalität beitragen (EuGH, *Digital Rights Ireland und Seitlinger ua.*, Rz 60). Nichts anderes gilt für die die Richtlinie umsetzenden Rechtsvorschriften im TKG 2003, in der StPO und im SPG. Es wäre dem Gesetzgeber zwar unbenommen, im Hinblick auf die Beauskunftung von Vorratsdaten auf die Aufklärung von Straftaten abzustellen, die mit einem bestimmten Strafmaß bedroht sind. Der Gesetzgeber hätte allerdings darüber hinaus sicherzustellen, dass die Schwere der Straftat – die durch die jeweilige Strafdrohung zum Ausdruck kommt – im Einzelfall den Eingriff in verfassungsgesetzlich gewährleistete Rechte jener Personen rechtfertigt, die durch die Beauskunftung "ihrer" Vorratsdaten betroffen sind. Insofern ist der von § 135 Abs. 2a iVm § 135 Abs. 2 Z 2 bis 4 StPO umfasste Kreis der Delikte zu undifferenziert und als Folge dessen zu weit gefasst. Er stellt nicht sicher, dass Auskunftsersuchen nur bei Delikten zulässig sind, für die entweder schwere Strafen drohen (zB § 207a StGB) oder für deren Aufklärung die Verwendung der auf Vorrat gespeicherten Daten wegen der Art der Tatbegehung in besonderem Maße notwendig ist (zB § 107a Abs. 1 iVm Abs. 2 Z 2 StGB). 171

2.3.11.6. Die Verhältnismäßigkeit der Speicherung von Daten auf Vorrat ist – ungeachtet des Vorbehalts der gerichtlichen Bewilligung der Auskunft über Vorratsdaten (§ 135 Abs. 2a iVm § 137 Abs. 1 StPO), der Befassung des Rechtsschutzbeauftragten und seines Beschwerderechts nach § 147 Abs. 1 Z 2a und Abs. 3 zweiter Satz StPO – daher schon alleine deshalb nicht gewahrt, weil durch § 135 Abs. 2a StPO iVm §§ 102a, 102b Abs. 1 TKG 2003 nicht gewährleistet wird, dass über Vorratsdaten nur dann Auskunft erteilt wird, wenn sie zur strafprozessualen Verfolgung und Aufklärung von Straftaten dienen, die im Einzelfall eine gravierende Bedrohung der in Art. 8 Abs. 2 EMRK genannten Ziele darstellen und die einen solchen Eingriff rechtfertigen. § 135 Abs. 2a StPO verstößt daher gegen § 1 Abs. 2 DSG 2000. 172

2.3.12. § 134 Z 2a StPO, der den Begriff "Auskunft über Vorratsdaten" für den Anwendungsbereich der StPO definiert, steht in untrennbarem Zusammenhang mit § 135 Abs. 2a StPO und ist daher aus diesem Grund aufzuheben. 173

2.3.13. Die Zweit- und Drittantragsteller begehren, die Wortfolge "auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 4 iVm § 102a TKG 2003 erforderlich ist," in § 53 Abs. 3a Z 3 SPG und in § 53 Abs. 3b SPG die Wortfolge ", auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 iVm § 102a TKG 2003 erforderlich ist," als verfassungswidrig aufzuheben. 174

2.3.13.1. Die Erteilung von Auskünften über Vorratsdaten bedarf – anders als nach der StPO – nach dem SPG keiner richterlichen Genehmigung. Die Befassung des Rechtsschutzbeauftragten gemäß § 91c Abs. 1 SPG, dem "die Prüfung der nach diesem Absatz erstatteten Meldungen" – also eine Prüfung ex post – obliegt (§ 91c Abs. 1 letzter Satz SPG), ist jedenfalls nicht ausreichend. 175

2.3.13.2. Im Übrigen gelten die oben zu § 135 Abs. 2a StPO geäußerten Bedenken auch für die angefochtenen Wortfolgen in den angeführten Bestimmungen des SPG. Den sicherheitspolizeilichen Befugnissen zum Zugriff auf Vorratsdaten fehlt jede auf die Schwere einer drohenden Straftat bezogene Einschränkung. Lediglich Fahrlässigkeitsdelikte sind von ihnen nicht erfasst. 176

2.3.13.3. Damit ist den Anforderungen an die Verhältnismäßigkeit des Eingriffs in das Grundrecht auf Datenschutz durch Zugriffe nach § 53 Abs. 3a Z 3 oder § 53 Abs. 3b SPG nicht Genüge getan. Die angefochtenen Wortfolgen in diesen Bestimmungen sind daher als verfassungswidrig aufzuheben. 177

2.3.13.4. Der Umstand, dass die Sicherheitsbehörden nach § 53 Abs. 3a Z 3 SPG "nur" Name und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war, und nach § 53 Abs. 3b SPG "nur" Standortdaten beauskunften können, die im Rahmen der Verpflichtung nach § 102a TKG 2003 gespeichert wurden, ändert im Lichte der Ausführungen oben zu III.2.3.13 nichts an diesem Ergebnis (vgl. *Berka*, aaO, 141, unter Hinweis auf BVerfGE 125, 260). 178

2.3.14. Im Zusammenhang mit den Vorschriften zur Auskunftserteilung erweist sich auch § 102a TKG 2003 als verfassungswidrig. Mit den Vorschriften betreffend die Beauskunftung von Vorratsdaten bilden auch die Vorschriften des TKG 2003, welche die Speicherung von Vorratsdaten anordnen, einen Grundrechtseingriff von erheblichem Gewicht in das verfassungsgesetzlich gewährleistete Recht auf Datenschutz aus § 1 DSG 2000 der "Benutzer" (§ 92 Abs. 3 Z 2 TKG 2003) öffentlicher Kommunikationsdienste oder sonst von der Speicherung Betroffener und damit auch des Zweitantragstellers und des Drittantragstellers (siehe schon oben 2.3.7). 179

2.3.14.1. Dass die Speicherung und Verarbeitung von Daten der in § 102a TKG 2003 genannten Art gänzlich ungeeignet wäre, zur Aufklärung schwerer Straftaten einen Beitrag zu leisten, wurde von den antragstellenden Parteien weder behauptet, noch ist dies in der mündlichen Verhandlung hervorgekommen. Die Eignung des Grundrechtseingriffs ist insofern abstrakt zu prüfen, als sie weder einen bestimmten konkreten Prozentsatz bei der Häufigkeit der Anwendung der Rechtsvorschrift in der Praxis voraussetzt, noch eine bestimmte "Erfolgsquote" bei der Aufklärung von Straftaten. Es genügt, wenn der Gesetzgeber mit Grund von der Eignung der Maßnahme, dem ins Auge gefassten "Zweck" wirksam zu dienen, ausgehen durfte (vgl. in diesem Zusammenhang den siebenten Erwägungsgrund der für ungültig erklärten Vorratsdatenspeicherungsrichtlinie; EuGH, *Digital Rights Ireland und Seitlinger ua.*, Rz 43). Ob jedes einzelne nach § 102a TKG 2003 auf Vorrat zu speichernde Datum diese Eignung aufweist, 180

ist vom Verfassungsgerichtshof in diesem Verfahren nicht zu prüfen. Es steht nämlich keineswegs bei allen Daten, deren Speicherung auf Vorrat und Verarbeitung § 102a TKG 2003 in Umsetzung der nicht mehr gültigen Vorratsdatenspeicherungsrichtlinie anordnet, von vornherein fest, dass ihre Speicherung verhältnismäßig ist. Die bloße Möglichkeit, neue Technologien zu zusätzlichen Überwachungsmaßnahmen zu nutzen, rechtfertigt nicht von vornherein einen Eingriff in die von § 1 DSG 2000 und Art. 8 EMRK geschützte Freiheitssphäre.

2.3.14.2. Der Verfassungsgerichtshof hat bereits im Beschluss VfSlg. 19.702/2012 betont, dass die "Streubreite" der anlasslosen Speicherung jene der bisher in seiner Rechtsprechung zu beurteilenden Eingriffe in die durch § 1 DSG 2000 geschützte Rechtssphäre übertrifft (vgl. BVerfGE 125, 260 [318 ff.]), und zwar sowohl hinsichtlich des betroffenen Personenkreises als auch des Kreises und der Art der Daten sowie der Aufgaben, für die sie angeordnet wird, als auch der Modalitäten der Datenverwendung. 181

2.3.14.3. In personeller Hinsicht ist zu berücksichtigen, dass von der Speicherung im Wesentlichen die Nutzer von Festnetz, Mobilfunk, Internet-Zugangs- und E-Mail-Diensten (§ 92 Abs. 3 Z 14 und 15 TKG 2003) und damit große Teile der Bevölkerung in Österreich betroffen sind. So hatte Ende 2013 jedes Unternehmen im Durchschnitt zwei Festnetzanschlüsse und mehr als jeder zweite Haushalt hatte einen solchen Anschluss. Auf jeden Einwohner entfielen im Schnitt 1,5 SIM-Karten für Mobiltelefonie. Internetzugang über mobiles oder festes Breitband hatten rund 60 % der Haushalte und Unternehmen, die Marktdurchdringung bei Breitband im Rahmen von Smartphonetarifen belief sich auf 87 % für Haushalte und Unternehmen (siehe den RTR Telekom Monitor Jahresbericht 2013 betreffend Nutzung von Festnetz, Mobilfunk und Internet in Österreich, http://www.rtr.at/de/komp/TKMonitor_2013/TM_Jahresbericht_2013.pdf). Von der durch § 102a TKG 2003 angeordneten Vorratsdatenspeicherungsverpflichtung ist somit nahezu die gesamte Bevölkerung betroffen (so auch EuGH, *Digital Rights Ireland und Seitlinger ua.*, Rz 56). 182

2.3.14.4. Wie der Verfassungsgerichtshof bereits in seinem Beschluss VfSlg. 19.702/2012 festgestellt hat, erfasst die Vorratsdatenspeicherung fast 183

ausschließlich Personen, die keinerlei Anlass – in dem Sinne, dass sie ein Verhalten gesetzt hätten, das ein staatliches Einschreiten erfordern würde – für die Datenspeicherung gegeben haben (vgl. auch EuGH, *Digital Rights Ireland und Seitlinger ua.*, Rz 58). Vielmehr nutzt der ganz überwiegende Anteil der Bevölkerung öffentliche Kommunikationsdienste zur Ausübung von Grundrechten, namentlich vor allem der Meinungsäußerungs-, Informations- und Kommunikationsfreiheit.

Der Zweitantragsteller macht geltend, dass er unbescholten sei. Dies trifft auf nahezu alle von der Vorratsdatenspeicherung Betroffenen zu. Im Hinblick auf diese Mehrheit wiegt die Beschränkung des Rechts auf Geheimhaltung ihrer personenbezogenen Daten iSd § 1 Abs. 1 DSG 2000 und ihr Recht auf Löschung aus § 1 Abs. 3 DSG 2000 besonders schwer. 184

2.3.14.5. Hinsichtlich des Kreises und der Art der Daten gilt, dass von der Speicherverpflichtung des § 102a TKG 2003 bestimmte "Verkehrs-" und "Standortdaten" umfasst sind, die im Zuge der Bereitstellung von öffentlichen Kommunikationsdiensten erzeugt oder verarbeitet werden. Verkehrsdaten sind "Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden" (so § 92 Abs. 3 Z 4 TKG 2003). Standortdaten sind "Daten, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben, im Fall von festen Telekommunikationsendeinrichtungen sind Standortdaten die Adresse der Einrichtung" (so § 92 Abs. 3 Z 6 TKG 2003). Die Speicherung von Inhalten einer Kommunikation, insbesondere von Daten über im Internet aufgerufene Adressen, wird durch § 102a Abs. 7 TKG 2003 ausdrücklich untersagt. 185

Ungeachtet dessen kann im Falle einer Erteilung von Auskünften über Vorratsdaten im Rahmen des § 135 Abs. 2a StPO und des § 53 SPG nicht ausgeschlossen werden, dass sich aus den Vorratsdaten Schlüsse ziehen lassen, die dem Anspruch auf Geheimhaltung personenbezogener Daten, wie er durch § 1 Abs. 1 DSG 2000 gewährleistet wird, zuwiderlaufen. Hiebei sind vor allem auch die Möglichkeiten der Verknüpfung von in unterschiedlichen Zusammenhängen ermittelten Daten zu berücksichtigen (*Berka,* aaO, 76 und 111 f.). Als entspre- 186

chend schwer ist daher auch der Eingriff im Hinblick auf den Kreis und die Art der gespeicherten Daten zu werten.

2.3.14.6. Überdies ist zu bedenken, dass angesichts der Vielzahl der Anbieter öffentlicher Kommunikationsdienste und damit von Speicherungsverpflichteten auch ein nicht überblickbarer Kreis von Personen potentiell Zugriff auf gemäß § 102a TKG 2003 gespeicherte Daten hat. Das diesbezüglich bestehende Missbrauchspotential ist wiederum bei der Beurteilung der Schwere des Eingriffs zu veranschlagen (vgl. BVerfGE 125, 260 [320]). Dabei ist zwar zu berücksichtigen, dass der Gesetzgeber hinsichtlich dieses Risikos Vorkehrungen getroffen hat, die über die Anforderungen der Vorratsdatenspeicherungsrichtlinie, die der Gerichtshof der Europäischen Union für mangelhaft befunden hat, hinausgehen (vgl. insbesondere die ausdrückliche Verpflichtung zur Verschlüsselung in § 94 Abs. 4 TKG 2003 und die technischen und organisatorischen Maßnahmen der auf Grund des § 94 Abs. 4 TKG 2003 erlassenen Datensicherheitsverordnung [DSVO] und die diesbezüglich weniger weitgehende Bestimmung des Art. 7 der für ungültig erklärten Vorratsdatenspeicherungsrichtlinie). Daneben enthält § 109 TKG 2003 Strafbestimmungen, die dem Schutz vor Missbrauch dienen. Allerdings ist zu veranschlagen, dass insbesondere Bestimmungen fehlen, die eine missbräuchliche Verwendung von Vorratsdaten durch die zur Speicherung verpflichteten Anbieter unter Strafe stellen (vgl. dagegen § 301 Abs. 3 StGB betreffend Mitteilungen über den Inhalt von Ergebnissen aus einer Auskunft über Vorratsdaten): 187

2.3.14.7. Der Verfassungsgerichtshof hat in seinem Vorlagebeschluss VfSlg. 19.702/2012 an den Gerichtshof der Europäischen Union explizit auf das erhöhte Risiko des Missbrauchs hingewiesen, das mit der Vorratsdatenspeicherung verbunden ist, weil angesichts der Vielzahl der Anbieter von Telekommunikationsdienstleistungen und damit von Speicherungsverpflichteten ein nicht überblickbarer Kreis von Personen Zugriff auf solche auf Vorrat für mindestens sechs Monate zu speichernde Verkehrsdaten hat. Der Gerichtshof der Europäischen Union kam zum Ergebnis (EuGH, *Digital Rights Ireland und Seitlinger ua.*, Rz 66), dass Art. 8 GRC zur Folge hat, dass Garantien dafür geschaffen werden müssen, dass die auf Vorrat gespeicherten Daten wirksam vor Missbrauchsrisi- 188

ken sowie vor jedem unberechtigten Zugang zu ihnen und jeder unberechtigten Nutzung geschützt sind. Dasselbe Erfordernis besteht nach Art. 8 EMRK und § 1 DSG 2000.

§ 102c TKG 2003 sieht nun einzelne Vorschriften für die Datensicherheit der auf Vorrat gespeicherten Daten und die Protokollierung des Zugriffs auf sie vor. § 109 Abs. 3 TKG 2003 enthält weiters Verwaltungsstrafbestimmungen (mit einer Strafdrohung von Geldstrafe bis zu € 37.000,--) für Fälle, in denen entgegen § 102a Abs. 8 TKG 2003 Daten nicht gelöscht werden (Z 23), entgegen § 102b TKG 2003 Daten ohne Vorliegen einer gerichtlichen Bewilligung beauskunftet werden (Z 24) und entgegen § 102b TKG 2003 Daten in nicht verschlüsselter Form über ein Kommunikationsnetz übermittelt werden (Z 25). 189

Zunächst ist festzuhalten, dass (sofern keine gerichtlich strafbare Tat vorliegt) die "bloße" unbefugte Verwendung von Daten, die im Rahmen der Vorratsdatenspeicherung erfasst werden, nicht mit Verwaltungsstrafe bedroht ist, sodass insofern ein Missbrauch dieser Daten mit den Mitteln des (Verwaltungs-)Strafrechts nicht bekämpft wird. Darüber hinaus hat die mündliche Verhandlung ergeben, dass die Datenschutzkommission bzw. die Datenschutzbehörde seit Inkrafttreten der Vorschriften über die Vorratsdatenspeicherung zur Überprüfung der Einhaltung dieser Vorschriften nicht tätig geworden ist. 190

2.3.15. Ungeachtet des Umstandes, dass der Gesetzgeber die Speicherung von Daten auf Grund des § 102a TKG 2003 zwar explizit und ausschließlich zur Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs. 2a StPO rechtfertigt, zulässt (§ 102a Abs. 1 letzter Satz TKG 2003) und damit einen gesetzlich festgelegten Zweck schafft, liegt bereits in der Speicherung ein Eingriff von besonderem Gewicht. 191

2.3.15.1. Dabei ist zu veranschlagen, dass für die Daten jener Betroffenen, die keinerlei Anlass zur Speicherung gegeben haben und somit in keinerlei Zusammenhang mit dem in § 102a Abs. 1 letzter Satz TKG 2003 festgelegten Speicherungszweck stehen, das einen Teil des Grundrechts auf Datenschutz bildende Recht auf Löschung gemäß § 1 Abs. 3 DSG 2000 (vgl. zB VfSlg. 16.150/2001) für den in § 102a TKG 2003 angeordneten Zeitraum von sechs bzw. sieben Monaten (§ 102a Abs. 8 TKG 2003) nicht gegeben ist. Hinzu kommt, dass Löschungsbegeh- 192

ren nur hinsichtlich jener speicherungspflichtigen Anbieter gestellt werden können, von denen der Betroffene weiß, dass diese ihn betreffende Vorratsdaten gespeichert haben. Hinsichtlich aller Anbieter, die zwar Vorratsdaten betreffend eine Person gespeichert haben, diese Person von diesem Umstand aber nichts weiß, kann das Recht auf Löschung ebenfalls nicht ausgeübt werden.

2.3.15.2. Eine Beschränkung des Rechts auf Löschung ist gemäß § 1 Abs. 4 DSG 2000 – wie Beschränkungen des Rechts aus § 1 Abs. 1 DSG 2000 – nur unter den in § 1 Abs. 2 DSG 2000 genannten Voraussetzungen zulässig. Nach der Rechtsprechung des Verfassungsgerichtshofes (vgl. zB VfSlg. 12.768/1991 zu § 1 DSG 1978) fordert das Recht auf Löschung gemäß § 1 Abs. 3 DSG 2000 zwar (nur) gesetzliche Bestimmungen, die ein konkretes Recht auf Löschung einräumen, steht aber jeder Auslegung solcher Bestimmungen entgegen, die § 1 Abs. 3 DSG 2000 nicht Rechnung tragen oder das Recht auf Löschung in einer den Anforderungen des § 1 Abs. 2 DSG 2000 nicht genügenden Weise beschränken. 193

2.3.15.3. Hinzu kommt, dass die Verpflichtung zur Speicherung nach § 102a TKG 2003 als Folge der Verfassungswidrigkeit und Aufhebung des § 135 Abs. 2a StPO und der angefochtenen Wortfolgen in den genannten Bestimmungen des SPG (siehe oben 2.3.11.6 und 2.3.13.3) ihren – im Hinblick auf § 135 Abs. 2a StPO in § 102a Abs. 1 letzter Satz TKG 2003 ausdrücklich festgelegten – Zweck zur Gänze verliert. Eine Speicherung auf Vorrat ohne konkreten Zweck – sei es auch nur für einen kurzen Zeitraum – wäre aber jedenfalls verfassungswidrig (vgl. in anderem Zusammenhang bereits *Pernthaler*, Die Verfassungsmäßigkeit des Bundesgesetzes über das land- und forstwirtschaftliche Betriebsinformationssystem [LFBIS-Gesetz] unter dem Gesichtswinkel der bundesstaatlichen Kompetenzverteilung und Verwaltungsorganisation, in: Funk/Pernthaler, Verfassungsfragen des land- und forstwirtschaftlichen Informationswesens, 1982, 51 [66]). Damit erfüllt auch § 102a TKG 2003 – ebenso wie die Vorratsdatenspeicherungsrichtlinie – nicht das Erfordernis eines Zusammenhangs zwischen den auf Vorrat gespeicherten Daten und der Bedrohung der öffentlichen Sicherheit (EuGH, *Digital Rights Ireland und Seitlinger ua.*, Rz 59). 194

2.3.16. Schließlich sind die Regelungen über die Löschung von Daten nicht in einer Weise bestimmt, die dem Erfordernis einer gesetzlichen Regelung im Sinne von § 1 Abs. 2 DSG 2000 entspräche. Im Besonderen ist unklar, ob die auf Grund der Verpflichtung aus § 102a Abs. 1 TKG 2003 gespeicherten Daten unwiderruflich zu löschen sind (vgl. in diesem Zusammenhang Art. 7 lit. d der für ungültig erklärten Vorratsdatenspeicherungsrichtlinie: "die Daten werden am Ende der Vorratsdatenspeicherungsfrist vernichtet, mit Ausnahme jener Daten, die abgerufen und gesichert worden sind."). 195

2.3.16.1. In Anbetracht der Schwere des Eingriffs an sich lassen die Vorschriften betreffend die Vorratsdatenspeicherung – insbesondere §§ 94 Abs. 4, 102a Abs. 8, 102c TKG 2003 und auch die auf Grund der §§ 94 Abs. 4 und 102c TKG 2003 ergangene DSVO – Bestimmungen vermissen, die für die von der Speicherung Betroffenen und die zur Speicherung Verpflichteten klarstellen, dass mit der "Löschung" der auf Vorrat gespeicherten Daten der Ausschluss von deren Wiederherstellbarkeit verbunden zu sein hat (siehe in diesem Sinne zu § 4 Z 9 DSG 2000 OGH 15.4.2010, 6 Ob 41/10p). Daran vermag die Praxis der Anbieter, die wohl schon aus Wirtschaftlichkeitsüberlegungen die auf Vorrat gespeicherten Daten in regelmäßigen Abständen "überschreiben" und so letztlich deren Wiederherstellbarkeit verhindern, sowie der Gerichte und Behörden, die beauskunfteten Daten – ausweislich der entsprechenden Ausführungen in der mündlichen Verhandlung vor dem Verfassungsgerichtshof – "physisch" zu löschen, nichts zu ändern. Eine "Löschung" in dem Sinn, dass bloß der Zugriff auf die weiterhin existenten (und rekonstruierbaren) Daten verhindert wird, genügt den dargelegten strengen verfassungsrechtlichen Anforderungen (siehe oben 2.2.8.2) nicht. Da dies durch § 102a Abs. 8 TKG 2003 und durch andere Bestimmungen nicht eindeutig klar gestellt wird, wird hinsichtlich des durch § 102a Abs. 1 TKG 2003 bewirkten Eingriffs auch das Erfordernis einer hinreichend präzisen gesetzlichen Grundlage (§ 1 Abs. 2 DSG 2000) nicht erfüllt. 196

2.3.16.2. Ein Mangel der gesetzlichen Grundlage liegt auch hinsichtlich der Pflichten der Betreiber und Behörden im Zusammenhang mit sogenannten "always-on-Diensten" vor (vgl. die Erläuterungen zur RV der TKG-Novelle BGBl. I 27/2011, 1074 BlgNR 24. GP, 23). Wird ein Internet-Zugangsdienst als "always-on-Dienst" betrieben und genutzt, so stellt sich die Frage, wann im Sinne des § 102a Abs. 1 TKG 2003 die "Kommunikation" als beendet gilt. Die Bundesre- 197

gierung hat in der mündlichen Verhandlung vor dem Verfassungsgerichtshof die Ansicht vertreten, § 102a Abs. 1 und § 102a Abs. 2 TKG 2003 seien "verfassungskonform" dergestalt zu interpretieren, dass bei Internet-Zugangsdiensten die Kommunikation mit dem Entzug der öffentlichen IP-Adresse durch den Anbieter als beendet im Sinne des § 102a Abs. 1 TKG 2003 anzusehen sei. Die Daten nach § 102a Abs. 2 TKG 2003 seien daher sechs Monate ab Entzug einer öffentlichen IP-Adresse durch den Anbieter zu speichern.

2.3.16.3. Selbst wenn es zutrifft, dass die geschilderte Auslegung zu einem praktikablen Ergebnis führen kann, vermag die bloße Möglichkeit auch einer solchen Auslegung aber keine hinreichende gesetzliche Determinierung des Grundrechtseingriffs zu ersetzen, sodass auch in diesem Fall den strengen Anforderungen an die gesetzliche Grundlage für Eingriffe in das Grundrecht auf Datenschutz (siehe oben 2.2.8.2) nicht Genüge getan ist. 198

2.3.17. Im Ergebnis sind die antragstellenden Parteien daher insoweit im Recht, als sie der Sache nach geltend machen, dass die Regelungen in ihrem Zusammenhang nicht verhältnismäßig sind: Die Beschränkungen dieses Grundrechts auf Datenschutz nach dem Gesetzesvorbehalt des § 1 Abs. 2 DSG 2000 wären nur auf Grund von Gesetzen zulässig, die aus den in Art. 8 Abs. 2 EMRK genannten Gründen notwendig sind und die ausreichend präzise, also für jedermann vorhersehbar, regeln, unter welchen Voraussetzungen die Ermittlung bzw. die Verwendung personenbezogener Daten für die Wahrnehmung konkreter Verwaltungsaufgaben erlaubt ist. Gesetzliche Beschränkungen des Grundrechts auf Datenschutz müssen das gelindeste Mittel zur Zielerreichung bilden und in einer Abwägung zwischen der Schwere des Eingriffs und dem Gewicht der mit ihnen verfolgten Ziele verhältnismäßig sein. 199

Diese Anforderungen erfüllen die Regelungen betreffend die Vorratsdatenspeicherung in ihrer Zusammenschau (§ 135 Abs. 2a StPO iVm § 102a TKG 2003, § 53 Abs. 3a Z 3 SPG iVm § 102a TKG 2003, § 53 Abs. 3b SPG iVm § 102a TKG 2003) aus den angeführten Gründen nicht. 200

2.4. Zum Vorbringen in Bezug auf andere Bestimmungen des TKG 2003: 201

Die Zweit- und Drittantragsteller begehren die Aufhebung weiterer Bestimmungen des TKG 2003, weil diese in untrennbarem Zusammenhang mit § 102a TKG 2003 stünden, und stellen jeweils die entsprechenden Anträge, näher bezeichnete Bestimmungen zur Gänze oder in eventu genau bezeichnete Wortfolgen aus den Bestimmungen aufzuheben. 202

2.4.1. § 102b ("Auskunft über Vorratsdaten") und § 102c Abs. 2, 3 und 6 TKG 2003 sind wegen untrennbaren Zusammenhangs mit § 102a TKG 2003 aufzuheben. Dasselbe gilt für § 92 Abs. 3 Z 6b (Legaldefinition des Begriffs "Vorratsdaten") und ebenso für die Ziffern 22, 23, 24, 25 und 26 in § 109 Abs. 3 TKG 2003 (Verwaltungsstrafbestimmungen), die aufzuheben sind. 203

2.4.2. Ferner sind die folgenden Wortfolgen wegen untrennbaren Zusammenhangs mit § 102a TKG 2003 aufzuheben: 204

In § 93 Abs. 3 TKG 2003 die Wortfolge "einschließlich Vorratsdaten"; in § 94 Abs. 1 TKG 2003 die Wortfolge "einschließlich der Auskunft über Vorratsdaten"; in § 94 Abs. 2 TKG 2003 die Wortfolge "einschließlich der Auskunft über Vorratsdaten"; in § 94 Abs. 4 TKG 2003 die Wortfolgen "einschließlich der Übermittlung von Vorratsdaten," und "sowie die näheren Bestimmungen betreffend die Speicherung der gemäß § 102c angefertigten Protokolle"; in § 98 Abs. 2 TKG 2003 die Wortfolge ", auch wenn hiefür ein Zugriff auf gemäß § 102a Abs. 3 Z 6 lit. d gespeicherte Vorratsdaten erforderlich ist"; in § 99 Abs. 5 Z 2 TKG 2003 die Wortfolge ", auch wenn diese als Vorratsdaten gemäß § 102a Abs. 2 Z 1, Abs. 3 Z 6 lit. a und b oder § 102a Abs. 4 Z 1, 2, 3 und 5 längstens sechs Monate vor der Anfrage gespeichert wurden,"; in § 99 Abs. 5 Z 3 TKG 2003 die Wortfolge ", auch wenn hiefür ein Zugriff auf gemäß § 102a Abs. 3 Z 6 lit. d gespeicherte Vorratsdaten erforderlich ist"; in § 99 Abs. 5 Z 4 TKG 2003 die Wortfolgen "auch" und "als Vorratsdaten gemäß § 102a Abs. 2 Z 1 oder § 102a Abs. 4 Z 1, 2, 3 und 5". 205

2.5. Bei diesem Ergebnis erübrigt sich ein Eingehen auf das Vorbringen der Antragsteller, dass die angefochtenen Bestimmungen auch andere verfassungsgesetzlich gewährleistete Rechte verletzen. 206

IV. Ergebnis

1. § 135 Abs. 2a StPO, die Wortfolgen "auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 4 iVm § 102a TKG 2003 erforderlich ist," in § 53 Abs. 3a Z 3 SPG und ", auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 iVm § 102a TKG 2003 erforderlich ist," in § 53 Abs. 3b SPG sowie § 102a TKG 2003 und die mit den genannten Bestimmungen in untrennbarem Zusammenhang stehenden, im Spruch näher genannten Bestimmungen der StPO und des TKG 2003 oder Teile davon sind daher als verfassungswidrig aufzuheben. 207

2. Der Antrag zu G 59/2012 ist, soweit er zulässig ist und die Aufhebung des § 94 Abs. 4 TKG 2003 sowie die Aufhebung des § 99 Abs. 5 Z 4 TKG 2003 begehrt wird, abzuweisen, soweit das jeweilige Aufhebungsbegehren über die im Spruch näher genannten, als verfassungswidrig aufgehobenen Wortfolgen in diesen Bestimmungen hinausgeht (VfSlg. 16.989/2003 mwN). 208

3. Der Ausspruch, dass frühere gesetzliche Bestimmungen nicht wieder in Kraft treten, beruht auf Art. 140 Abs. 6 erster Satz B-VG. 209

4. Die Verpflichtung des Bundeskanzlers zur unverzüglichen Kundmachung der Aufhebung und der damit im Zusammenhang stehenden sonstigen Aussprüche erfließt aus Art. 140 Abs. 5 erster Satz B-VG und § 64 Abs. 2 VfGG iVm § 3 Z 3 BGBlG. 210

5. Im Gesetzesprüfungsverfahren ist nach § 65a VfGG ein Kostenzuspruch nur für jene Antragsteller vorgesehen, deren Antragslegitimation sich aus Art. 140 Abs. 1 Z 1 lit. c B-VG ergibt. Den obsiegenden Antragstellern zu G 59/2012 und G 62,70,71/2012 sind daher Kosten zuzusprechen. 211

5.1. In den zugesprochenen Kosten sind jeweils die zum Zeitpunkt der Einbringung der Individualanträge gültigen Pauschalsätze, nämlich ein Grundbetrag von € 2.000,-- sowie der Ersatz der Eingabengebühr in Höhe von € 220,-- und Umsatzsteuer in Höhe von € 400,-- enthalten. Diese Pauschalsätze decken sämtliche Vertretungshandlungen, auch in Zwischenverfahren wie dem Vorabentschei- 212

dungsverfahren vor dem Gerichtshof der Europäischen Union, ab (VfSlg. 17.065/2003).

5.2. Der vom Drittantragsteller begehrte Streitgenossenzuschlag ist nicht zuzusprechen, da sich der Antrag zu G 62,70,71/2012 hinsichtlich aller Antragsteller außer dem Drittantragsteller als unzulässig erwiesen hat. 213

5.3. Dem Zweitantragsteller sind Barauslagen für Reisekosten aus Anlass der Teilnahme an der mündlichen Verhandlung im Verfahren C-594/12 vor dem Gerichtshof der Europäischen Union in der Höhe von € 1.077,76 zu ersetzen. 214

Wien, am 27. Juni 2014
Der Präsident:
Dr. HOLZINGER

Schriftführer:
Mag. SIMON