TE Vfgh Erkenntnis 2014/6/27 G47/2012 ua

JUSLINE Entscheidung

Veröffentlicht am 27.06.2014

Index

10/10 Grundrechte, Datenschutz, Auskunftspflicht
25/01 Strafprozess
41/01 Sicherheitsrecht
91/01 Fernmeldewesen

Norm

B-VG Art140 Abs1 / Prüfungsumfang
B-VG Art140 Abs1 Z1 litc
B-VG Art140 Abs1 Z2
TelekommunikationsG 2003 §1, §92 ff, §98, §99, §102a, §102b, §102c
StPO §134, §135
SicherheitspolizeiG §53 Abs3a, Abs3b
DSG 2000 §1
EMRK Art8
EU-Grundrechte-Charta Art7, Art8
VfGG §65a

Leitsatz

Verfassungswidrigkeit von Bestimmungen des TelekommunikationsG 2003, der StPO und des SicherheitspolizeiG über die Vorratsdatenspeicherung wegen unverhältnismäßigen Eingriffs in das Recht auf Datenschutz und das Recht auf Privat- und Familienleben; gravierender Grundrechtseingriff durch die angeordnete Speicherungsverpflichtung der Anbieter öffentlicher Kommunikationsdienste und den Zugriff auf diese Daten (Beauskunftung) durch Sicherheits- und Strafverfolgungsbehörden; keine Verhältnismäßigkeit der Regelungen angesichts der Streubreite des Eingriffs, des Kreises und der Art der betroffenen Daten und der daraus folgenden Schwere des Eingriffs in das Recht auf informationelle Selbstbestimmung; Beauskunftung nicht nur zwecks Aufklärung schwerer Straftaten vorgesehen; Kreis der Delikte zu weit gefasst; nahezu gesamte Bevölkerung von anlassloser Speicherung betroffen; Missbrauchspotential nicht ausreichend berücksichtigt; Regelungen über die Löschung der Daten nicht hinreichend bestimmt; Zulässigkeit der Individualanträge; Zurückweisung des Gesetzesprüfungsantrags der Kärntner Landesregierung als zu eng gefasst

Spruch

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 Abs3 Z6b;

– in §93 Abs3 die Wortfolge "einschließlich Vorratsdaten";

– in §94 Abs1 die Wortfolge "einschließlich der Auskunft über Vorratsdaten";

– in §94 Abs2 die Wortfolge "einschließlich der Auskunft über Vorratsdaten";

– in §94 Abs4 die Wortfolgen "einschließlich der Übermittlung von Vorratsdaten," und "sowie die näheren Bestimmungen betreffend die Speicherung der gemäß §102c angefertigten Protokolle";

– in §98 Abs2 die Wortfolge ", auch wenn hiefür ein Zugriff auf gemäß §102a Abs3 Z6 litd gespeicherte Vorratsdaten erforderlich ist";

– in §99 Abs5 Z2 die Wortfolge ", auch wenn diese als Vorratsdaten gemäß §102a Abs2 Z1, Abs3 Z6 lita und b oder §102a Abs4 Z1, 2, 3 und 5 längstens sechs Monate vor der Anfrage gespeichert wurden,";

– in §99 Abs5 Z3 die Wortfolge ", auch wenn hiefür ein Zugriff auf gemäß §102a Abs3 Z6 litd gespeicherte Vorratsdaten erforderlich ist";

– in §99 Abs5 Z4 die Wortfolgen "auch" und "als Vorratsdaten gemäß §102a Abs2 Z1 oder §102a Abs4 Z1, 2, 3 und 5";

– §102a;

– §102b;

– §102c Abs2, 3 und 6;

– in §109 Abs3 die Z22, 23, 24, 25 und 26.

II. §134 Z2a und §135 Abs2a der Strafprozeßordnung 1975 (StPO), BGBl Nr 631, in der FassungBGBl 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 Abs3a Z3 in der FassungBGBl I Nr 33/2011, die Wortfolge "auch wenn hiefür die Verwendung von Vorratsdaten gemäß §99 Abs5 Z4 iVm §102a TKG 2003 erforderlich ist,";

– in §53 Abs3b in der FassungBGBl I Nr 13/2012, die Wortfolge ", auch wenn hiefür die Verwendung von Vorratsdaten gemäß §99 Abs5 Z3 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 G47/2012 wird zurückgewiesen.

VII. Der Antrag des **** ******* **********, *****, zu G59/2012 wird zurückgewiesen, soweit er sich gegen §1 Abs4 Z7 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 Abs1, 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 **** *** ******** ******* zu G62,70,71/2012 wird zurückgewiesen, soweit er sich gegen §102c Abs1, 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 G59/2012 zuhanden seines Rechtsvertreters die mit € 3.697,76 bestimmten Prozesskosten binnen 14 Tagen bei sonstiger Exekution zu ersetzen und dem Antragsteller zu G62,70,71/2012 zuhanden seines Rechtsvertreters die mit € 2.620,-- bestimmten Prozesskosten binnen 14 Tagen bei sonstiger Exekution zu ersetzen.

Begründung

Entscheidungsgründe

I. Anträge und Vorverfahren

1. Der Antrag zu G47/2012:

1.1. Die Kärntner Landesregierung (in der Folge: die antragstellende Landesregierung) stellt auf Grund ihres Beschlusses vom 27. März 2012 gemäß Art140 Abs1 B-VG iVm §§62 ff. VfGG den Antrag,

"[d]ie Bestimmungen der [...]

§90 Abs6, Abs7 bis 8,

§92 Abs3 Z2a bis 2b, Abs3 Z3 lita bis c, Abs3 Z6a bis 6b, Abs3 Z8, Abs3 Z8a,

§93 Abs5,

§94 Abs1 bis 2, Abs3, Abs4,

§98 Abs2,

§99 Abs1, Abs5 Z1 bis 4,

§102a Abs1 bis 7, Abs8,

§102b Abs1, Abs2, Abs3,

§102c Abs1, Abs2

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 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 Art8 EMRK, das Grundrecht auf Datenschutz des [§] 1 DSG, das Fernmeldegeheimnis des Art10a StGG, das Kommunikationsgeheimnis des §93 TKG, das Recht auf freie Meinungsäußerung der Art10 EMRK und Art13 StGG, die Unschuldsvermutung des Art6 Abs2 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.

1.4. Unter "Kritikpunkte an einzelnen Paragraphen des TKG" werden im Antrag die §§90 Abs6 bis Abs8, 92 Abs3 Z2a bis Z3 litc, Z6a und Z6b, Z8a und Z8b, 93 Abs5, 94, 98 Abs2, 99 Abs1, 99 Abs5, 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 Abs8 TKG 2003), "widersprüchlich und unpräzise" (zu §92 Abs3 Z3 lita bis c TKG 2003) oder "unbestimmt, unpräzise" (zu §§92 Abs3 Z6b, 94 Abs3 TKG 2003). Durch die angeführten Bestimmungen ergäben sich "massive" bzw. "gravierende Eingriffe" (zB im Falle der §§90 Abs6 bis 8, 92 Abs3 Z8, 93 Abs5, 94 Abs3 und 4, 99 Abs1, 102b Abs3 TKG 2003) in Grundrechte. Auch die übrigen der angeführten Bestimmungen seien grundrechtswidrig bzw. verstießen gegen das Bestimmtheitsgebot des Art18 B-VG.

1.5. Im Rahmen der Ausführungen zu§102a TKG 2003 wird vorgebracht, dass die Daten, deren Speicherung durch §102a Abs3 Z3 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.

Die in §102a Abs2 bis 4 TKG 2003 vorgesehene Speicherung von Daten sei nicht das gelindeste, zum Ziel führende Mittel iSd §1 Abs2 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 Art8 EMRK verankerte Grundrecht auf Achtung des Privat- und Familienlebens eingegriffen. Dieser Eingriff sei untauglich, nicht erforderlich und unverhältnismäßig.

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

2.1. Im Rahmen eines abstrakten Gesetzesprüfungsverfahrens nach Art140 B-VG habe der Antrag die gegen die Verfassungsmäßigkeit des Gesetzes sprechenden Bedenken im Einzelnen darzulegen (§62 Abs1 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.

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 Strafprozeßordnung 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 Abs3 Z3 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.

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.

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

"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 Art8 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 Art8 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 Art8 EMRK vor. Allerdings ist dieser Eingriff gerechtfertigt: Denn der gesetzlich vorgesehene Eingriff stellt eine Maßnahme dar, die nach Art8 Abs2 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, Z57 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 Abs5 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 Abs1 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, privaten 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 Abs3 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 Art8 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 Art1 Abs1 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 Abs1 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 Art10 der [Vorratsdatenspeicherungsrichtlinie] nachkommen zu können.

[...]

4. Zu den Kritikpunkten an einzelnen Bestimmungen des TKG 2003

[...]

4.3.4. Zu §92 Abs3 Z6b 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 Abs3 Z6b und 102a TKG 2003 bezüglich der Vorratsdaten nicht dem Determinierungsgebot entsprechen. Dazu ist Folgendes auszuführen: Die Definition des Vorratsdatums nach §92 Abs3 Z6b 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 Abs2a 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 Abs2a StPO zu speichern sind.

[...]

4.6. Zu §94 Abs3 und 4 TKG 2003

§94 Abs3 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 Abs3 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 Abs3 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 Abs4 TKG 2003 lassen sich eindeutig auslegen. Der Verordnungsgeber hat eine nähere Spezifizierung mit der DSVO [Datensicherheitsverordnung] erlassen.

4.7. Zu §98 Abs2 TKG 2003

Der Inhalt des §98 Abs2 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 Abs1 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 Abs2 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 Abs5 TKG 2003

§99 Abs5 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. Z2 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 Abs8 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 Abs2 TKG 2003 von der [Vorratsdatenspeicherungsrichtlinie] vorgegeben ist.

§102a Abs1 TKG 2003 sieht die Speicherverpflichtung für in Abs2 bis 4 genannte Datenkategorien zu Zwecken der Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach §135 Abs2a 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 Abs2a 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 Abs6 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 Abs6 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 Abs1 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 Abs2 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 Abs3 TKG 2003

Durch den in §102b Abs3 TKG 2003 zu findenden Verweis auf die Regelung des§94 Abs4 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 Abs4 TKG 2003 [...] wird daher verwiesen.

4.15. Zu §102c Abs2 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.

3. Der Antrag zu G59/2012:

3.1. Der Antragsteller zu G59/2012 (in der Folge: der Zweitantragsteller) stellt gemäß Art140 Abs1 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 Abs4 Z5 (gemeint wohl §1 Abs4 Z7), §92 Abs3 Z6b, in §93 Abs3 die Wortfolge "einschließlich Vorratsdaten", in §94 Abs1 die Wortfolge "einschließlich der Auskunft über Vorratsdaten", §94 Abs4, §99 Abs5 Z2, 3, und 4, §102b, §102c, §109 Abs3 Z22 bis 26 TKG 2003 stünden mit §102a TKG 2003 in untrennbarem Zusammenhang und seien deshalb ebenfalls aufzuheben. Hinsichtlich des §94 Abs4 und des §99 Abs5 Z2, 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 Abs3a sowie 3b SPG bzw. – wiederum "in eventu" – bestimmte Wortfolgen aus diesen Bestimmungen wegen untrennbaren Zusammenhangs mit §102a TKG 2003 sowie aus demselben Grund §134 Z2a StPO und §135 Abs2a StPO als verfassungswidrig aufzuheben.

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 Vertragsverhältnisse 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 Abs2 bis 4 TKG 2003 genannten Daten verpflichtet. Eine Ausnahme von dieser Speicherpflicht bestehe nach §102a Abs6 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 Abs6 TKG 2003.

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.

Da die in §102a Abs2 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 Abs1 TKG 2003 unmittelbar und aktuell in seinen Rechten betroffen.

Für den Zweitantragsteller bestünden keine anderen Möglichkeiten, als durch den vorliegenden, auf Art140 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.

3.3. Die in §102a TKG 2003 vorgesehene Speicherverpflichtung verletze den Zweitantragsteller in seinem verfassungsgesetzlich gewährleisteten Recht auf Achtung des Privat- und Familienlebens nach Art8 EMRK und Art7 GRC. Nach der Judikatur des Europäischen Gerichtshofes für Menschenrechte sei das Fernmeldegeheimnis vom Anwendungsbereich des Art8 EMRK erfasst. Die verpflichtende Speicherung der in §102a Abs2 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.

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.

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 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 Abs6 TKG 2003 fallen.

Darüber hinaus unterlägen Anbieter von Diensten der Informationsgesellschaft im Sinne von §1 Abs2 Z2 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 Z9 TKG 2003 sei. Zur Speicherung von Daten nach §102a TKG 2003 seien aber nur Anbieter öffentlicher Kommunikationsdienste verpflichtet.

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 Z9 TKG 2003 seien.

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.

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.

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.

Dass die von der Vorratsdatenspeicherungsrichtlinie vorgegebene Speicherpflicht nach §102a TKG 2003 weder notwendig noch geeignet iSd Art8 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.

Der Eingriff in die durch Art8 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]."

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.

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 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.

3.5. Des Weiteren bringt der Zweitantragsteller vor, dass der Kreis der in§102a Abs1 TKG 2003 in Bezug genommenen Straftaten ("Straftaten, deren Schwere eine Anordnung nach §135 Abs2a 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).

3.6. Selbst unter der Annahme, dass die Vorratsdatenspeicherung nicht gegen Art8 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 Abs2 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 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 G59/2012, in der den im Antrag erhobenen Bedenken wie folgt entgegengetreten wird:

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 un

d nicht an Endkunden richteten. Überdies stehe dem Zweitantragsteller ein zumutbarer Weg zur Geltendmachung der behaupteten Verfassungswidrigkeiten zur Verfügung, der die Antragslegitimation des Zweitantragstellers ausschließe.

Einerseits könne der Zweitantragsteller die in §31 Abs1 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 Abs7 DSG 2000) Bescheid erwirken, der beim Verfassungsgerichtshof bekämpft werden könne. Andererseits erachte es die Bundesregierung für zumutbar, dass der Zweitantragsteller im Zivilrechtsweg (§32 Abs1 DSG 2000) gegen jenen Anbieter, dessen öffentliche Kommunikationsdienste er nutzt und der gleichzeitig sein Arbeitgeber ist, vorgeht.

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.

4.3. Im Hinblick auf die Behauptung des Zweitantragstellers, der Kreis der durch§102a Abs1 TKG 2003 in Bezug genommenen Straftaten sei überschießend, verweist die Bundesregierung auf die schon vor dem 1. April 2012 geltende 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 Abs2a 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.

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

5. Der Antrag zu G62,70,71/2012:

5.1. In einem als "Sammel-Individualantrag" bezeichneten und auf Art140 Abs1 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 (G62/2012-36, G70/2012-30, G71/2012-26).

Beantragt wird, §102a TKG 2003 sowie des Weiteren wegen untrennbaren Zusammenhangs mit dieser Bestimmung §102b, §102c, in §99 Abs5 Z2 die Wortfolge "auch wenn diese als Vorratsdaten gemäß §102a Abs2 Z1, Abs3 Z6 lita und b oder §102a Abs4 Z1, 2, 3 und 5 längstens sechs Monate vor der Anfrage gespeichert wurden,", in §99 Abs5 Z3 die Wortfolge ", auch wenn hiefür ein Zugriff auf gemäß §102a Abs3 Z6 litd gespeicherte Vorratsdaten erforderlich ist", in §99 Abs5 Z4 die Wortfolgen "auch" und "als Vorratsdaten gemäß §102a Abs2 Z1 oder §102a Abs4 Z1, 2, 3 und 5", §92 Abs3 Z6 litb zur Gänze, in §93 Abs3 die Wortfolge "einschließlich Vorratsdaten", in §94 Abs1 die Wortfolge "einschließlich der Auskunft über Vorratsdaten", in §94 Abs2 die Wortfolge "einschließlich der Auskunft über Vorratsdaten", in §94 Abs4 die Wortfolgen "einschließlich der Auskunft über Vorratsdaten" und "sowie die näheren Bestimmungen betreffend die Speicherung der gemäß §102c angefertigten Protokolle", in §98 Abs2 die Wortfolge ", auch wenn hiefür ein Zugriff auf gemäß §102a Abs3 Z6 litd gespeicherte Vorratsdaten erforderlich ist" und die Z22, 23, 24, 25 und 26 des §109 Abs3 TKG 2003 wegen Verletzung des Rechts auf Privat- und Familienleben und Schutz der Korrespondenz gemäß Art8 EMRK bzw. Art7 GRC, des Rechts auf Datenschutz gemäß §1 DSG 2000 bzw. Art8 GRC, des Rechts auf Meinungs- und Informationsfreiheit gemäß Art10 EMRK bzw. Art11 GRC, des Rechts auf Versammlungs- und Vereinigungsfreiheit gemäß Art11 EMRK bzw. Art12 GRC, des Rechts auf Schutz des Fernmeldegeheimnisses gemäß Art10a StGG sowie des Rechts auf die Unschuldsvermutung im Strafverfahren gemäß Art6 EMRK bzw. Art48 GRC aufzuheben.

Aus denselben Gründen begehrt der Drittantragsteller, §135 Abs2a und§134 StPO Z2a StPO als verfassungswidrig aufzuheben. Schließlich beantragt er die Aufhebung der Wortfolge "auch wenn hiefür die Verwendung von Vorratsdaten gemäß §99 Abs5 Z4 iVm §102a TKG 2003 erforderlich ist," in §53 Abs3a Z3 SPG und der Wortfolge "auch wenn hiefür die Verwendung von Vorratsdaten gemäß §99 Abs5 Z3 iVm §102a TKG 2003 erforderlich ist," in §53 Abs3b SPG. Dem Hauptbegehren des Drittantragstellers folgen umfangreiche Eventualbegehren.

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.

5.2. Zur Antragslegitimation wird ausgeführt, dass schon die nach Ansicht des Drittantragstellers überschießende und nicht gerechtfertigte Speicherung von Daten auf Vorrat Rechte aus §1 DSG 2000 und Art8 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 Art140 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 Abs2 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.

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