SCHEUCHER RECHTSANWALT GMBH

in Kooperation mit Mag. Tina Große Rechtsanwältin_Attorney at law

Mag. Ewald Scheucher
Rechtsanwalt_Attorney at law

[A] Lindengasse 39, A-1070 Wien
[T] +43/1/710 92 51
[F] +43/1/710 92 51-51
[E] office@scheucher.eu
[I] www.scheucher.eu

VERFASSUNGSGERICHTSHOF
Judenplatz 11
1010 Wien

120611/IA_VDS/konsolidierte_Fassung/ems/gt

Antragsteller:

1. **Ing. Dr. Christof TSCHOHL,** geb. 12.05.1978,
Jurist, Ludwig Boltzmann Institut für Menschenrechte
[redacted]
2. **Mag. Andreas KRISCH**, geb. 21.07.1970,
IT-Consultant, Obmann Arbeitskreis Vorratsdatenspeicherung
[redacted]
3. **Mag. Albert STEINHAUSER**, geb. 15.10.1971
Nationalratsabgeordneter, Justizsprecher der „Grünen"
[redacted]
4. **Jana HERWIG**, M.A:, 18.04.1974,
Medienwissenschafterin,
[redacted]
5. **Sigrid MAURER**, geb. 19.03.1985, Studentin,
[redacted]
6. **Mag. DDr. Erich SCHWEIGHOFER**, geb. 05.02.1960,
Ao. Univ. Prof. Universität Wien,
Leiter der Arbeitsgruppe Rechtsinformatik,
[redacted]
7. **Dr. Hannes TRETTER,** geb. 05.07.1951,
ao. Univ.-Prof., Universität Wien,
Direktor des Boltzmann-Instituts für Menschenrechte,
[redacted]
8. **SCHEUCHER Rechtsanwalt GmbH**, FN 335393a
[redacted]
9. **Dr. Maria WITTMANN-TIWALD,** geb. 16.03.1960, Richterin,
[redacted]
10. **Philipp SCHMUCK**, geb. 18.02.1992, Student,
[redacted]

11. **Dr. Stefan PROCHASKA**, geb. 21.11.1968, Rechtsanwalt
Vizepräsident der Rechtsanwaltskammer Wien
Geschäftsführer PHHV Rechtsanwälte OG
[redacted]

12. bis 11.130. **Antragsteller/in** gemäß vorzulegender CD

alle vertreten durch: **SCHEUCHER Rechtsanwalt GmbH**
1070 Wien, Lindengasse 39
RA-Code P131306

(Vollmachten gem. § 8 RAO erteilt)

Antragsgegnerin: **BUNDESREGIERUNG**
p.A. Bundeskanzleramt
1014 Wien, Ballhausplatz 2

wegen: §§ 102a, 102b, 102c, 99, 92 – 94, 98, 109 TKG 2003,
§ 76a Abs 2 StPO, § 53 Abs 3a, 3b SPG

INDIVIDUALANTRAG
gemäß Art 140 Abs 1 B-VG

3-fach
2 Anlagen (3-fach)

Inhaltsverzeichnis **Seite**

I. Vollmachtsbekanntgabe, Liste der Antragsteller/innen, Einleitung

I.1. Eine CD mit der vollständigen Liste der 11.130 Antragsteller/innen wird dem Verfassungsgerichtshof vorgelegt werden. Im Rubrum angeführt werden die sogenannten Erstantragsteller/innen, das sind einige jener Personen, die diesen „Sammel-Individualantrag" aktiv getragen, organisiert und/oder prominent öffentlich vertreten haben. Zu manchen dieser Erstantragsteller/innen wird eine Kopie der Verträge mit den jeweiligen Anbietern vorgelegt. Dem Rechtsvertreter wurde von sämtlichen Antragsteller/innen Vollmacht erteilt, auf welche er sich ausdrücklich beruft.

I.2. Einleitung

Die Umsetzung der Richtlinie 2006/24/EG im österreichischen TKG, der StPO und dem SPG stellen für die Antragsteller/innen einen Dammbruch dar, eine Art Quantensprung in den „Überwachungsstaat". Setzen sich diese Prinzipien durch und fort, ist die auf persönlicher Freiheit basierende Ordnung westlicher Demokratien am Ende – ungeachtet, wie das Staatswesen formal organisiert und verwaltet wird.

Die legalisierte präventive Überwachung des Kommunikationsverhaltens aller in Österreich lebenden und elektronisch kommunizierenden Menschen stellt einen unumkehrbaren Paradigmenwechsel dar, der mit dem Konzept eines von Grund- und Freiheitsrechten geprägten Rechtsstaates unvereinbar ist. Die vollständige Erfassung des Kommunikationsverhaltens stellt mit dem Argument, (weitgehende) Sicherheit in einer unsicheren Welt zum Preis der Aufgabe der bürgerlichen Privatsphäre schaffen zu können, das Konzept „unveräußerlicher Rechte", das seit der amerikanischen und französischen Revolution das geistige Fundament der freiheitlich geprägten westlichen Gesellschaften darstellt, gleichsam auf den Kopf.

Auf die Vielzahl der grundrechtlichen Unvereinbarkeiten wird im Detail in der materiellen Argumentation dieses Antrags eingegangen. An dieser Stelle sei vorweg genommen, dass die Vorratsdatenspeicherung nicht nur den Schutz der Privatsphäre völlig unterminiert, sondern auch eine nachhaltige Erosion von demokratischen Grundpfeilern wie der Meinungs- und Medienfreiheit, dem Schutz von Berufsgeheimnissen und schließlich der Unschuldsvermutung darstellt.

Im Kern leitet dieser Antrag dem VfGH die Frage zur Entscheidung zu, ob die Vorratsdatenspeicherung an sich mit der Europäischen Grundrechte-Charta und den Österreichischen Grundrechten, insbesondere der europäischen Menschenrechtskonvention vereinbar ist. Im Hinblick auf die innerstaatliche Rechtslage kann diese Klarstellung nur vom VfGH kommen. Er ist damit aus Sicht der Antragsteller/innen in Österreich gleichsam die letzte Verteidigungslinie einer auf Freiheitsrechten basierenden Staats- und Gesellschaftsordnung – wenn auf europäischer Ebene der Schutz der Grundrechte gemäß GRC nicht (mehr) gewährleistet wird oder werden kann. Ob dieser Schutz auf Ebene der EU gewährleistet wird, lässt sich in diesem Zusammenhang insbesondere im Rahmen einer Vorabentscheidung durch den EuGH gemäß Art 267 AEUV klären.

II. Darstellung der Rechtslage im Überblick

Dieser Antrag nimmt Bezug auf Bestimmungen nachstehender Gesetze:

TKG 2003: Telekommunikationsgesetz 2003, Stammfassung BGBl. I Nr. 70/2003 in der Fassung von BGBl. I Nr. 102/2011

DSG 2000: Bundesgesetz über den Schutz personenbezogener Daten, Stammfassung BGBl. I Nr. 165/1999 in der Fassung von BGBl. I Nr. 51/2012

StPO: Strafprozessordnung 1975, Stammfassung BGBl. Nr. 631/1975 in der Fassung von BGBl. I Nr. 53/2012

SPG: Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei, Stammfassung BGBl. Nr. 566/1991 in der Fassung von BGBl. I Nr. 13/2012

II.1 Richtlinie 2006/24/EG und die österreichische Umsetzung in TKG, StPO und SPG

II.1.1 Die

„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."

(in der Folge: VDS-RL) wurde durch eine Novelle zum Telekommunikationsgesetz mit BGBl. I 27/2011 (in der Folge: TKG-Novelle 2011) in österreichisches Recht umgesetzt. Im Wesentlichen wurden dabei vor allem die neuen Bestimmungen **§§ 102a, 102b und 102c TKG** eingeführt.

II.1.2 Die für die Umsetzung relevanten Bestimmungen und Begriffe des TKG

§ 102a TKG ordnet eine Speicherpflicht für Anbieter von öffentlichen Kommunikationsdiensten hinsichtlich bestimmter Daten an.

§ 102b TKG normiert in der Folge die Grundsätze für die Verwendung von Vorratsdaten zu Auskunftszwecken gegenüber Strafverfolgungsbehörden.

§ 99 Abs. 5 TKG normiert die Zulässigkeit der Verwendung von Verkehrsdaten zum Zweck von **Datenauskünften** nach der **StPO** (§ 76a abs. 2 StPO) und dem **SPG** (§ 53 Abs. 3a und 3b SPG) und bezieht dabei – in Abweichung von den Grundsätzen des § 102b TKG – zum Teil (in Ziffer 2, 3 und 4) auch Vorratsdaten mit ein.

§ 102c TKG schließlich normiert die Pflichten zur Datensicherheit und zur Protokollierung auf Seiten der speicherpflichtigen Anbieter. In Bezug auf Datensicherheit steht die Bestimmung materiell und formell im Zusammenhang mit **§ 94 Abs. 4 TKG**, der entsprechende Datensicherheitsmaßnahmen bei der Übermittlung von Verkehrsdaten – sowohl Vorratsdaten als auch „Betriebsdaten" – anordnet und die Konkretisierung dieser Maßnahmen einer Verordnung vorbehält. Darauf basierend wurde am 06.12.2011 die „Datensicherheitsverordnung TKG" mit BGBl. II Nr. 402/2011 erlassen.

Mit der TKG-Novelle 2011 wurde nicht ausschließlich die VDS-RL umgesetzt, sondern auch einige Ergänzungen im Datenschutz-Teil des TKG 2003 vorgenommen.

II.1.3 Die für die Umsetzung relevanten Novellierungen der StPO und des SPG

Korrespondierend zur Umsetzung der Vorratsdatenspeicherung im TKG wurden mit BGBl. I Nr. 33/2011 auch Bestimmungen der StPO und des SPG novelliert, um die Regeln für den Zugriff auf Vorratsdaten der neuen Rechtslage nach dem TKG anzupassen. Die damit geänderten bzw. teilweise neu eingeführten Normen (**§ 76a Abs. 2 StPO, § 135 Abs. 2a StPO; § 53 Abs. 3a SPG, § 53 Abs. 3b SPG**) sind 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, weil diese Normen in ihrer Gesamtheit die Zweckbindung der Datenverwendung ergeben.

Diese Zweckbindung muss aber schon bei der Speicherung – dem ersten Grundrechtseingriff – immanent gesehen werden.

Eine prägnante Zusammenfassung zum Zusammenspiel der oben zitierten Bestimmungen findet sich in der Studie des Ludwig-Boltzmann-Instituts für Menschenrechte zur „Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung in Österreich"[1], die hier auszugsweise wiedergegeben wird:

Ermittlungsbefugnisse nach der StPO
Betrifft eine Auskunft Vorratsdaten, ist das Auskunftsbegehren auf die neue Bestimmung des § 135 (2a) StPO zu stützen, wobei jedoch die Voraussetzungen gleich sind, also eine Strafdrohung von mehr als einem Jahr und eine gerichtliche Bewilligung vorliegen muss. Dabei sind § 102b TKG und § 135 (2a) StPO korrespondierende Normen.

In Bezug auf IP-Adressen und E-Mail-Verkehrsdaten besteht jedoch eine wesentliche Ausnahme, mit der diese Ermittlungsbefugnisse aus der Grundsatzkonstruktion der Auskunft über Daten einer Nachrichtenübermittlung (Strafdrohungsgrenze und Richtervorbehalt) herausgelöst wurden. Gemäß § 99 (5) Z 2 TKG und § 76a (2) StPO sind Auskünfte über diese Daten, auch wenn sie Vorratsdaten sind, ohne jede Einschränkung auf Strafdrohungen oder bestimmte Straftatbestände

[1] http://bim.lbg.ac.at/files/sites/bim/BIM%20Studie%20Datensicherheit%20TKG%20Novelle%202010_final_online-Publikation.pdf S 30 ff.

für den gesamten Bereich des gerichtlichen Strafrechts zulässig.[2] Auch der Richtervorbehalt gilt diesbezüglich nicht, die Maßnahme muss lediglich vom Staatsanwalt angeordnet werden.

Die primäre Intention dieser Bestimmung bei der Entstehung war, die Zulässigkeit von Auskünften über Teilnehmer hinter einer dynamischen IP-Adresse auch für den niederschwelligen Strafrechtsbereich (also bei Strafdrohungen bis zu einem Jahr) zu normieren. Rechtspolitisch lässt sich das völlige Fehlen materieller Einschränkungen und einer richterlichen Genehmigung mit der bisherigen Praxis erklären, IP-Adressen-Auskünfte als reine Stammdatenabfragen zu qualifizieren. Grundrechtlich rechtfertigen lässt sich das Ergebnis damit jedoch nicht, insbesondere nicht für die Ausnahme bezüglich E-Mail-Daten. Damit wird es nämlich zulässig, selbst für jedes Bagatelldelikt eine Auskunft über den gesamten aktiven E-Mail Verkehr (d.h. Daten über alle E-Mails, die von dieser Adresse versendet wurden) der letzten 6 Monate ohne richterliche Genehmigung zu verlangen.

Ermittlungsbefugnisse nach dem SPG:
Neben der Befugnis zur Ermittlung von Stammdaten (vgl. § 53 Abs 3a Z 1 SPG) sind die Sicherheitsbehörden ausdrücklich ermächtigt, von Anbietern von Telekommunikationsdiensten und sonstigen Dienstanbietern kostenlos Auskunft zu IP-Adressen zu verlangen. Begehrt wird entweder die IP-Adresse zu einer - anhand relevanter Kriterien, etwa Pseudonym, Internetforum und Zeitraum (eingeschränkt auf eine Stunde) - bestimmten Nachricht samt dem Zeitpunkt ihrer Übermittlung (§ 53 Abs 3a Z 2 SPG), oder Name und Anschrift des Teilnehmers zu einer bereits bekannten IP-Adresse (§ 53 Abs 3a Z 3 SPG). In diesen Fällen ist keine gerichtliche oder sonstige Genehmigung notwendig. Der Anbieter erhält von einer der insgesamt 12 berechtigten Dienststellen eine schriftliche Anfrage und muss die angeforderten Daten ohne weiteres ausfolgen. Diese verfahrensrechtlichen Details sind nicht gesetzlich normiert sondern im Erlass des BM.I zu § 53 Abs 3b und 3b SPG, GZ 94762_101-GD_08 geregelt.

Für den präventiven Bereich gibt es auch nach der Novellierung der §§ 53 (3a) und (3b) SPG anlässlich der Vorratsdatenspeicherung keine Einschränkungen auf bestimmte Delikte oder den Schutz bestimmter besonders hochwertiger Rechtsgüter. Zwar findet sich prima facie eine solche Einschränkung in § 53 (3a) Z 2 und 3 SPG, wonach die Datenauskunft „eine wesentliche Voraussetzung zur Abwehr einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht" (EAH, § 19 SPG) sein muss. Allerdings gilt diese Rechtsgütereinschränkung nur für die Aufgabe der EAH, denn zur „Abwehr allgemeiner Gefahren (§ 16 SPG)" steht die Befugnis ohne Einschränkung zu.

Korrespondierend zu diesen Befugnissen wurden in § 99 (5) Z 3 und 4 TKG die Ausnahmen normiert, nach denen abweichend von § 102b TKG Verkehrsdatenauskünfte nach dem SPG auch im Hinblick auf Vorratsdaten zulässig sind, die nicht älter als 3 Monate sind. Betroffen sind dieselben Datenarten wie bei der eben beschriebenen Ausnahmekonstruktion des § 76a (2) StPO iVm § 99(5) Z 2 TKG, also insbesondere IP-Adressen und E-Mail Verkehrsdaten. Für den Bereich

2 Unter diese Ausnahmebestimmung fallen auch Auskünfte zur IMEI (Gerätekennung) und IMSI (Kennung der SIM-Karte) im Bereich des Mobilfunks.

des SPG wurden diese Ausnahmen im rechtspolitischen Entstehungsprozess ausdrücklich diskutiert und in dieser Form übernommen, weil das SPG selbst in § 53 Abs. 3a schon die Auskunftsbefugnis darauf einschränkt, dass immer ein Bezug zu einer bestimmten Nachricht zu einem möglichst genauen Zeitraum notwendig ist. Damit erfährt die Tragweite der Ausnahme auf SPG Seite eine entscheidende und notwendige Einschränkung, die im Vergleich dazu der StPO fehlt.

II.2. Die EU-rechtliche Dimension der Anfechtungsgegenstände

II.2.1 Die Rolle der Grundrechte-Charta

Der primäre Antrag (vgl dazu Punkt VI.1) bezieht sich auf den Kern der Vorratsdatenspeicherung an sich, nämlich auf die **verdachtsunabhängige flächendeckende Speicherung von Kommunikationsdaten**, wie sie **durch die Richtlinie 2006/24/EG insofern ohne Spielraum der Mitgliedsstaaten normiert** wird.

Dennoch besteht im vorliegenden Fall selbst unter Beachtung des Grundsatzes des Anwendungsvorrangs des Unionsrechts nach Meinung der Antragsteller/innen eine **Prüfungskompetenz des VfGH**.

Die **Grundrechte-Charta** (nachfolgend kurz: „GRC") ist seit dem Inkrafttreten des Vertrags von Lissabon am 01.12.2009 **Teil des Primärrechts der Europäischen Union**. Auch aus Art. 51 GRC folgt ihre unmittelbare Anwendbarkeit für die Mitgliedstaaten bei der Durchführung des Rechts der Union.

Nach der Rechtsprechung des Verfassungsgerichtshofes (VfGH 14.3.2012, U 466/11 ua) können auch die von der GRC garantierten Rechte vor dem Verfassungsgerichtshof als verfassungsgesetzlich gewährleistete Rechte gemäß Art. 144 bzw Art. 144a B-VG geltend gemacht werden und bilden im Anwendungsbereich der GRC einen Prüfungsmaßstab in Verfahren der generellen Normenkontrolle, insbesondere nach Art. 139 und Art. 140 B-VG.

Die Bestimmungen zur Umsetzung der Richtlinie 2006/24/EG die mit dem primären Antrag (Punkt VI.1) als verfassungswidrig bekämpft werden, insbesondere **§ 102a und § 102b TKG**, liegen im Anwendungsbereich des Unionsrechts, bei der Beurteilung ihrer Verfassungsmäßigkeit sind daher auch die Garantien der GRC Prüfungsmaßstab und zugleich unmittelbar anwendbare Bestimmungen des Unionsrechts. Konkret gerügt wird die Verletzung von

- **Artikel 7 GRC** (Achtung des Privat- und Familienlebens),
- **Artikel 8 GRC** (Schutz personenbezogener Daten),
- **Artikel 11 GRC** (Freiheit der Meinungsäußerung und Informationsfreiheit) sowie
- **Artikel 12 GRC** (Versammlungs- und Vereinigungsfreiheit).

Die Rechtsrüge im Detail wird in Kapitel V. bei der Darlegung der materiellen Bedenken ausgeführt.

II.2.2 Vorabentscheidung gemäß Art 267 AEUV

Der VfGH führt in der Entscheidung vom 14.03.2012, U 466/11 ua aus:

„Dabei ist für die Rechtsprechung des Verfassungsgerichtshofs im Anwendungsbereich der Grundrechte-Charta (Art 51 Abs 1 GRC) die Rechtsprechung des Gerichtshofs der Europäischen Union maßgebend, wobei dieser wiederum die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte ebenso berücksichtigt, wie es der Verfassungsgerichtshof tut. Dies bedeutet, dass der Verfassungsgerichtshof - wie schon bisher (vgl. VfSlg. 15.450/1999, 16.050/2000, 16.100/2001) - dann eine Frage dem Gerichtshof der Europäischen Union zur Vorabentscheidung vorlegt, wenn Zweifel an der Auslegung einer unionsrechtlichen Vorschrift bestehen, also auch im Falle der Grundrechte-Charta. Entstehen solche Zweifel insbesondere vor dem Hintergrund der EMRK und der dazu ergangenen Rechtsprechung des EGMR und anderer Höchstgerichte nicht, entscheidet der Verfassungsgerichtshof ohne Einholung einer Vorabentscheidung. Der Verfassungsgerichtshof ist in Fragen der Grundrechte-Charta vorlageverpflichtetes Gericht im Sinne des Art 267 Abs 3 AEUV."

Eine Vorlagepflicht an den Gerichtshof der Europäischen Union besteht dann nicht, wenn eine Rechtsfrage nicht entscheidungserheblich ist (vgl. EuGH 06.10.1982, Rs. 283/81, *Cilfit*, Slg. 1982, 3415; 15.09.2005, Rs. C-495/03, *Intermodal*, Slg. 2005, I-8151), das heißt, wenn die Antwort auf diese Frage, wie auch immer sie ausfällt, keinerlei Einfluss auf die Entscheidung des Rechtstreits haben kann. Dies ist im Bereich der GRC dann der Fall, wenn ein verfassungsgesetzlich gewährleistetes Recht, insbesondere ein Recht der EMRK, den gleichen Anwendungsbereich wie ein Recht der GRC hat. In diesem Fall erfolgt die Entscheidung des Verfassungsgerichtshofs daher auf Grund der österreichischen Verfassungslage, ohne dass eine Vorabentscheidung im Sinne des Art. 267 AEUV einzuholen wäre.

Nun hat sich die Rechtslage auf der Ebene des EU Primärrechts seit Inkrafttreten der Richtlinie 2006/24/EG und auch seit der (kompetenzrechtlichen) Entscheidung des EuGH zur Irischen Nichtigkeitsklage (Rechtssache C-301/06) in einem wesentlichen Punkt geändert. Vor dem 1. Dezember 2009 war die GRC nämlich kein verbindlicher Prüfmaßstab für Sekundärrecht. Zwar waren die Grundrechte schon vor dem Inkrafttreten der GRC für alle Organe, die Entscheidungen im Anwendungsbereich des Unionsrechts trafen, im Rahmen der allgemeinen Rechtsgrundsätze beachtlich (siehe zB VwGH 23.10.2000, 99/17/0193). „Die Geltung eines detaillierten Katalogs von Rechten und Pflichten, wie ihn die GRC enthält, ist aber nicht mit der Herleitung von Rechtspositionen aus allgemeinen Rechtsgrundsätzen vergleichbar." (VfGH 14. März 2012, U 466/11 ua). Seither ist auch keine Entscheidung des EuGH ergangen, die auch nur eine Prognose erlaubt, wie der Gerichtshof die Vereinbarkeit der Richtlinie 2006/24/EG mit den Bestimmungen der GRC beurteilen könnte, es handelt sich um eine offene Frage zur Auslegung insbesondere der Art. 7, 8, 11 und 12 GRC.

Auch die Entscheidung des EuGH vom 19. April 2012 in der Rechtssache C-461/10 enthält keine Aussage zur grundrechtlichen Zulässigkeit der Vorratsdatenspeicherung oder zu bestimmten Verwendungsfälle von Vorratsdaten. Die Entscheidung berührt nämlich gar nicht die Verwendung von Vorratsdaten sondern stellt lediglich klar, dass die VDS-RL (und deren "Beschränkung" auf

die Aufklärung, Feststellung und Verfolgung schwerer Straftaten) einer innerstaatlichen Bestimmung nicht entgegensteht, welche die Verwendung von Daten auch für solche Auskunftsverfahren zulässt, wenn die betreffenden Daten aus anderen Gründen im Einklang mit Art. 15 der RL 2002/58/EG und im Einklang mit dem innerstaatlichen Recht gespeichert und dann beauskunftet werden. Wie die Sache zu beurteilen ist, wenn es um Daten derselben Kategorie (nämlich Name und Anschrift des Teilnehmers, dem eine bestimmte IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war) geht, die nur noch aufgrund der Umsetzung der VDS-RL vorhanden sind, bleibt in dieser Entscheidung gerade offen. Entgegen den in einigen Medien in den letzten Monaten immer wieder kolportierten Meldungen gibt es bislang auch keine Bestätigung, dass beim EuGH bereits ein Vorabentscheidungsverfahren nach Irischer Vorlage anhängig sei, bei dem sich der EuGH im Kern mit der grundrechtlichen Zulässigkeit der VDS zu beschäftigen hätte. Auf eine Anfrage an die Kanzlei des EuGH vom 1. Juni 2012 durch Herrn Christopher Schack **(Anlage./A)** wurde geantwortet, dass ein derartiges Verfahren derzeit nicht anhängig sei.

Gleichzeitig gibt es auch keine ausdrückliche Rechtsprechung des EGMR zur Frage der Vorratsdatenspeicherung im Sinne der Richtlinie 2006/24/EG, weil diese konkrete Frage bisher kein Verfahrensgegenstand beim Menschenrechtsgerichtshof in Straßburg war. Die bestehende Judikatur zu Fragen des Datenschutzes im Rahmen der Rechtsprechung insbesondere zu Artikel 8 EMRK lässt aber durchaus darauf schließen, dass die Vorratsdatenspeicherung den Anforderungen der EMRK nicht genügt (siehe im Detail dazu die Ausführungen zu den materiellen Bedenken in Kapitel V).

Aus diesen Gründen wird angeregt, dem EuGH zur Vorabentscheidung gemäß Art. 267 AEUV die Frage vorzulegen, ob die Vorratsdatenspeicherung im Sinne der VDS-RL mit der EU Grundrechte-Charta vereinbar ist, insbesondere zumal die GRC erst nach Verabschiedung der VDS-RL verbindliches Primärrecht geworden ist. Einen Vorschlag für entsprechende Vorabentscheidungsfragen wird unter Punkt VI.11 formuliert.

Angemerkt wird, dass offenbar auch auf politischer Ebene der Wunsch besteht, diese Frage einer Klärung durch den EuGH zuzuführen. So hält es das Bundeskanzleramt in dessen Stellungnahme zur Bürgerinitiative (37/BI) betreffend "Stoppt die Vorratsdatenspeicherung" „für wünschenswert, das Instrument der Vorratsdatenspeicherung als solches einer Prüfung am Maßstab der EU Grundrechte-Charta zu unterziehen. Eine solche Prüfung kann freilich nur der Gerichtshof der Europäischen Union vornehmen. Sollte es – etwa im Wege eines Vorabentscheidungsverfahrens zu einer solchen Prüfung kommen und eine Unvereinbarkeit mit der EU Grundrechte-Charta festgestellt werden, wäre auch innerstaatlich der Weg frei für eine Anpassung der Rechtslage".

II.2.3 Das grundrechtliche Schutzniveau der Österreichischen Verfassung im Verhältnis zum Unionsrecht

Das österreichische Verfassungsrecht kennt nach herrschender Ansicht (zB *Öhlinger* Verfassungsfragen einer Mitgliedschaft zur EU S., Wien u.a. 1999, 182f.) keine Integrationsschranke gegenüber dem Unionsrecht (früher: Gemeinschaftsrecht). Dabei wird davon ausgegangen, dass durch die Volksabstimmung gem Art.44 Abs. 3 B-VG zum österreichischen EU-Betritt 1995 die österreichische Rechtsordnung „vorbehaltlos für das durch das BeitrittsBVG übernommene primäre und das (im Rahmen der damit begründeten Gemeinschaftskompetenzen erlassene) sekundäre Gemeinschaftsrecht geöffnet [wurde], so dass dessen autonome Geltung in Österreich in vollem Umfang zum Tragen kommt. Die Wirkungen des Gemeinschaftsrechts bestimmen sich demnach in Österreich ausschließlich nach dessen eigenen Kriterien. [...] Hingegen bilden die - durch den Beitrittsvertrag veränderten - Grundprinzipien der Verfassung sehr wohl Integrationsschranken für die Änderung **von Primärrecht**. Die seither in Kraft getretenen Änderungen des Primärrechts durch den Amsterdamer Vertrag, den Vertrag von Nizza und den Vertrag über den Beitritt neuer Mitgliedstaaten waren zwar verfassungsändernd, doch bewegten sie sich im Rahmen der Integrationsschranken und stellten insoweit „systemimmanente Fortentwicklungen" dar. Der Abschluss dieser Verträge erfolgte daher auf Grund einfacher verfassungsrechtlicher Ermächtigungen." (*Öhlinger/Potacs*: Gemeinschaftsrecht und staatliches Recht, 3. Auflage, Wien 2006, S. 57) Für die Ratifizierung des Vertrags von Lissabon wurde zwar diskutiert, ob es sich hierbei um eine Gesamtänderung handle und daher eine Volksabstimmung notwendig sei. Letztlich hat sich jedoch die Auffassung durchgesetzt, dass dafür eine einfache verfassungsgesetzliche Ermächtigung ausreiche. (vgl. *Öhlinger/Potacs*: Gemeinschaftsrecht und staatliches Recht, 3. Auflage, Wien 2006, S. 58)

Die Grenze des Anwendungsvorrangs von Unionsrecht ist daher jedenfalls erreicht, wenn eine Änderung eines der Grundprinzipien der Bundesverfassung im Sinne des Art. 44 Abs. 3 B-VG durch Unionsrecht bewirkt wird, egal ob es sich dabei um Primär- oder Sekundärrecht handelt (argumentum a maiori ad minus).

Die Antragsteller/innen vertreten die Ansicht, dass die Vorratsdatenspeicherung im Sinne des § 102a TKG in Umsetzung der Richtlinie 2006/24/EG das rechtstaatliche Prinzip insgesamt in Frage stellt.

Daraus folgt, dass die Vorratsdatenspeicherung im Sinne der Richtlinie 2006/24/EG in Österreich als eine Gesamtänderung im Sinne des Art. 44 Abs. 3 - die nicht von der Volksabstimmung zum EU-Beitritt erfasst wurde - zu sehen ist und daher ihrerseits einer Volksabstimmung bedürfte.

Diese Klarstellung kann in der aktuellen Rechts- und Verfassungslage nur vom VfGH kommen. Er ist aus Sicht der Antragsteller/innen dazu aufgerufen, wenn auf europäischer Ebene der Schutz der Grundrechte gemäß GRC nicht (mehr) gewährleistet wird oder werden kann. Ob dieser Schutz auf Ebene der EU gewährleistet wird lässt sich in diesem Zusammenhang insbesondere im Rahmen einer Vorabentscheidung durch den EuGH gemäß Art. 267 AEUV klären.

III. Prüfungsgegenstand

Nachfolgend werden von den Antragsteller/innen jene Normen angeführt, welche gemäß den Anträgen (Kapitel VI) Gegenstand der Prüfung durch den VfGH sind.

Zur besseren Orientierung sind die nach Rechtsansicht der Antragsteller/innen durch den VfGH aufzuhebenden Wortfolgen fett hervorgehoben.

III.1. TKG 2003 in der Fassung BGBl. I Nr. 102/2011

III.1.1 Kern der Anfechtung: Speicheranordnung im TKG einschließlich Verwendungszwecke

III.1.1.1 § 102a TKG ordnet die Vorratsspeicherung an und zählt die Kategorien von Daten auf. Diese Bestimmung wird zur Gänze angefochten, da der allenfalls verbleibende Rumpf (zB Ausnahme von der Speicherpflicht für „kleine Anbieter" nach Abs. 6) der Bestimmung keinen Sinn mehr ergäbe und sohin auch der Vollziehung nicht zugänglich wäre.

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.

III.1.1.2 **§ 102b TKG**, welcher die Verwendung von Vorratsdaten regelt, wird ebenfalls zur Gänze angefochten, weil er in untrennbarem Zusammenhang mit § 102a TKG steht. Im Eventualbegehren – für den Fall, dass § 102a TKG nicht aufgehoben werden sollte – wird die

Aufhebung dieser Norm begehrt, weil die Zweckbestimmung der Vorratsdaten überschießend und daher unverhältnismäßig und für sich verfassungswidrig ist.

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.

III.1.1.3 § 99 Abs 5 Z 2, 3 und 4 TKG werden teilweise angefochten, soweit sie in untrennbarem Zusammenhang mit § 102a TKG stehen. Im Eventualbegehren – für den Fall, dass § 102a TKG nicht aufgehoben werden sollte – wird die Aufhebung dieser Teile begehrt, weil die erweiterte Zweckbestimmung der Vorratsdaten überschießend und daher unverhältnismäßig und für sich verfassungswidrig ist. Diese Bestimmungen beinhalten außerdem Ausnahmen vom Grundprinzip des § 102b TKG zur Verwendung von Vorratsdaten, d.h. insbesondere auch Ausnahmen vom „Richtervorbehalt".

So sind gemäß § 99 Abs 5 Z 2 TKG insbesondere IP-Adressen gemäß § 76a Abs 2 StPO der Staatsanwaltschaft zur Verfügung zu stellen, gemäß Z 3 und Z 4 Standortdaten, IP-Adressen, IMSI, IMEI u.a. den Sicherheitsbehörden gemäß § 53 Abs. 3a und 3b SPG (dazu siehe unten Punkt III. 3). Diese Regelung ist nach Ansicht der Antragsteller/innen jedenfalls überschießend im Hinblick auf die Regelungsvorgaben der Richtlinie 2006/24/EG.

Verkehrsdaten

§ 99. (...)

(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.*

III.1.2 Anfechtung einzelner Bestimmungen im TKG, weil diese in untrennbaren Zusammenhang mit den als verfassungswidrig aufzuheben Normen (III.1.1) stehen.

Die hier angefochtenen Normen bewirken zwar nicht die Verfassungswidrigkeit, sie stehen aber in einem logisch untrennbaren Zusammenhang mit den Kern-Anfechtungsgegenständen und ergeben nach allfälliger Aufhebung von § 102a und 102b TKG keinen Sinn mehr.

III.1.2.1 § 1 Abs 4 Z 7 TKG: In dieser Bestimmung findet sich der Umsetzungshinweis betreffend die Richtlinie 2006/24/EG. Im Fall, dass der VfGH dem primären Antrag stattgibt, würde die Umsetzung der Richtlinie 2006/24/EG aus dem österreichischen Rechtsbestand beseitigt, sodass auch ein entsprechender Umsetzungshinweis nachträglich materiell unrichtig würde und daher zu beseitigen wäre.

(4) Durch dieses Bundesgesetz werden folgende Richtlinien der Europäischen Union umgesetzt:
(...)
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.

III.1.2.2 § 92 Abs. 3 Z 6b TKG: In dieser Bestimmung findet sich die Legaldefinition des Begriffs „Vorratsdaten", sie wäre zur Gänze zu streichen.

(3) In diesem Abschnitt bezeichnet unbeschadet des § 3 der Begriff
(...)
6b. „Vorratsdaten" Daten, die ausschließlich aufgrund der Speicherverpflichtung gemäß § 102a gespeichert werden;

III.1.2.3 § 93 Abs. 3 TKG: Diese Norm nimmt Bezug auf Vorratsdaten, die Streichung der Wortfolge „einschließlich Vorratsdaten" wäre unter Hinweis auf die als verfassungswidrig aufzuhebenden Normen (III.1.1) logisch unabdingbar.

§ 93 (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.*

III.1.2.4 § 94 Abs 1 TKG regelt die Verpflichtung zur Bereitstellung von technischen Einrichtungen; sie verliert ihren Sinn, soweit es auch Vorratsdaten betrifft.

> *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.*

III.1.2.5 § 94 Abs 2 TKG: Diese Bestimmung regelt die Mitwirkungspflicht von Anbietern. Wird nicht mehr auf Vorrat gespeichert, ist der Verweis auf Vorratsdaten ebenfalls sinnlos. Die bezughabende Wortfolge ist aufzuheben.

> *§ 94 (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.*

III.1.2.6 § 94 Abs. 4 TKG: Die Norm enthält Vorgaben zur technischen Einrichtung für die Datenübermittlung bei Auskünften nach StPO und SPG, sie betrifft „Betriebsdaten" und „Vorratsdaten", beantragt wird daher nur Aufhebung der Wortfolge: ***„einschließlich der Übermittlung von Vorratsdaten"***, sowie im letzten Satz: ***„sowie die näheren Bestimmungen betreffend die Speicherung der gemäß § 102c angefertigten Protokolle"***. Letzteres deswegen, weil § 102c TKG logisch untrennbar mit § 102a TKG verbunden und daher ebenfalls aufzuheben ist.

Der Rest des § 94 TKG kann und soll nach Ansicht der Antragsteller/innen bestehen bleiben, da

für das Datensicherheitsniveau und insbesondere die Durchlaufstelle auch in Bezug auf Auskünfte über betrieblich gespeicherte Daten gesetzliche Vorkehrungen zu treffen sind.

Technische Einrichtungen

§ 94. (1) (...)

(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.*

III.1.2.7 § 98 Abs 2 TKG: Von der allfälligen Aufhebung der in Punkt III.1.1 aufgezählten Normen wäre auch die hier genannte Bestimmung betroffen, soweit sie im Ausnahmefall den Rückgriff auf Vorratsdaten erlaubt (Standortdaten bei Notruf, eingeschränkt auf den letzten Kommunikationsvorgang, wenn eine live-Ortung nicht möglich ist).

Auskünfte an Betreiber von Notrufdiensten

§ 98. (1) (...)

(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.

(3)...

(4)...

(5)...

III.1.2.8 § 102c TKG schafft Datensicherheitsbestimmungen bezüglich Vorratsdaten; wenngleich die Norm eigentlich zur Verminderung des Grundrechtseingriffs beiträgt, ergibt sie keinen Sinn mehr, wenn die Anordnung zur Vorratsspeicherung entfällt. Die Bestimmung hat daher zur Gänze zu entfallen.

§ 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.

III.1.2.9 § 109 Abs. 3 Z 22 bis 26 TKG: Diese Verwaltungsstrafbestimmungen im Zusammenhang mit der Vorratsdatenspeicherung sind zur Gänze aufzuheben, weil die Tatbestände nach Aufhebung von §§ 102a, b und c TKG keinen Sinn mehr ergeben.

Verwaltungsstrafbestimmungen

§ 109. (1) (.....)

(2) (....)

(3) Eine Verwaltungsübertretung begeht und ist mit einer Geldstrafe bis zu 37 000 Euro zu bestrafen, wer (.....)

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) (...)

III.2 Anfechtung einzelner Bestimmungen in der StPO, weil diese in untrennbaren Zusammenhang mit den als verfassungswidrig aufzuhebenden Normen (III.1.1) stehen.

Das System der abschließenden Aufzählung von Fällen der zulässigen Verwendung von Verkehrsdaten (einschließlich „Vorratsdaten") ist in § 99 Abs. 1 TKG geregelt; die Aufzählung erfolgt im TKG dem Grunde nach, Details sind zum Teil in der StPO geregelt.

Die teilweise aufzuhebenden Bestimmungen lauten:

III.2.2 § 135 Abs 2a StPO wird zur Gänze angefochten, da diese Norm in untrennbarem logischem Zusammenhang mit § 102b TKG (Auskunft über „Vorratsdaten") steht.

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

§ 135. (1) (....)

(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) (...)

III.2.3 § 76a Abs 2 StPO: Für die teilweise Anfechtung dieser Norm besteht kein logischer Zwang, selbst wenn – wie beantragt – die §§ 102a und 102b TKG als verfassungswidrig aufgehoben würden. Sollte der VfGH aber § 99 Abs 5 Z 2 TKG nicht als verfassungswidrig aufheben, wäre die Beseitigung der geltend gemachten Verletzung verfassungsgesetzlich gewährleisteter Rechte – in geringerem Umfang, aber doch – durch die teilweise Aufhebung von § 76a Abs 2 StPO zu erreichen. § 76a Abs 2 StPO lautet:

Auskunft über Stamm- und Zugangsdaten

§ 76a. (1) (...)

(2) Gleiches gilt auf Anordnung der Staatsanwaltschaft (§ 102) für die Auskunft über folgende in § 99 Abs. 5 Z 2 TKG erwähnte Daten des Inhabers der betroffenen technischen Einrichtung:

1. Name, Anschrift und Teilnehmerkennung des Teilnehmers, dem eine öffentliche IP-Adresse zu einem bestimmten Zeitpunkt unter Angabe der zugrunde liegenden Zeitzone zugewiesen war, es sei denn, dass diese Zuordnung eine größere Zahl von Teilnehmern erfassen würde;

2. die bei Verwendung von E-Mail Diensten dem Teilnehmer zugewiesene Teilnehmerkennung;

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

4. die E-Mail-Adresse und die öffentliche IP-Adresse des Absenders einer E-Mail.

Die Bestimmungen der §§ 138 Abs. 5 und 139 gelten für diese Anordnung sinngemäß.

III.3 Anfechtung einzelner Bestimmungen im SPG, weil und soweit diese in untrennbarem Zusammenhang mit den als verfassungswidrig aufzuhebenden Normen (III.1.1) stehen.

Das System der abschließenden Aufzählung von Fällen der zulässigen Verwendung von Verkehrsdaten (einschließlich „Vorratsdaten") ist in § 99 Abs. 1 TKG geregelt; die Aufzählung erfolgt im TKG dem Grunde nach, Details sind zum Teil im SPG geregelt.

Die Anfechtung der Bestimmung des § 99 Abs 5 Z 4 TKG (betreffend Zugangsdaten, insbesondere IP-Adressen) sowie der Bestimmung des § 99 Abs 5 Z 3 TKG (bezüglich Standortdaten) wurden bereits oben (Punkt III.1) ausgeführt.

§ 53 (3a) Z 2 u 3 SPG korrespondiert mit § 99 Abs 5 Z 4 TKG, § 53 Abs 3b SPG mit § 99 Abs 5 Z 3 TKG:

Zulässigkeit der Verarbeitung

§ 53.

(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:

(...)

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,

(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.*

(....)

IV. Ausführungen zur Antragslegitimation

IV.1 Aktuelle und unmittelbare rechtliche Betroffenheit der Antragsteller

Der erste und wichtigste Anfechtungsgegenstand ist § 102a TKG, der die personenbezogene Speicherung bestimmter Daten anordnet. Schon die Speicherung von personenbezogenen Daten – nicht erst die weitere Verwendung solcher Daten – ist ein Eingriff in die grundrechtlich gewährleisteten Rechtspositionen der Antragsteller/innen gemäß **§ 1 Datenschutzgesetz 2000 (DSG)** bzw. dem Datenschutzgrundrecht gemäß **Art 8 GRC** sowie gemäß dem Schutz des Privatlebens und der Korrespondenz nach **Art. 8 EMRK** bzw. **Art. 7 GRC**.

Schon die Sammlung und Aufbewahrung allgemein zugänglicher Quellen wie Artikel in Zeitschriften stellt einen Eingriff in das Privatleben dar, sofern sie systematisch durch Behörden (Geheimdienste, Verfassungsschutz) erfolgt (Segerstedt-Wiberg u.a. v. Schweden, Nr. 62332/00, 06.06.2006, § 72).

Allein schon die überschießende bzw. nicht gerechtfertigte Speicherung von Daten verletzt § 1 DSG sowie Art. 8 EMRK.

In einer jüngeren Entscheidung wiederholt der EGMR, dass auch die bloße Speicherung von Daten, die sich auf das Privatleben einer Person beziehen, einen Eingriff iSv Art. 8 EMRK darstellt (S. und Marper gg. das Vereinigte Königreich, Urteil vom 04.12.2008, Große Kammer, Bsw. Nr. 30.562/04 und 30.566/04). Dies gilt unabhängig von einer nachfolgenden Verwendung der Informationen. Dass tatsächlich nur ein beschränkter Teil dieser Informationen von den Behörden verwendet und in einem Einzelfall kein unmittelbarer Nachteil verursacht wird, ändert nichts an dieser Schlussfolgerung.

Die Antragsteller sind auch durch jene Normen, die die Verwendungszwecke begrenzen, unmittelbar und aktuell betroffen, selbst wenn eine tatsächliche weitere Verwendung von personenbezogenen Daten erst später durch Anwendung der StPO und SPG Bestimmungen aktualisiert wird: **Der Grundrechtseingriff und damit die rechtliche Betroffenheit iSd Zulässigkeitsvoraussetzungen für einen Individualantrag nach Art 140 B-VG wird primär durch die Speicherung bewirkt, der Sitz der Verfassungswidrigkeit und die nachteilige Betroffenheit ist aber auch in der – in Relation zur Schwere des Grundrechtseingriffs unverhältnismäßigen – Zweckbestimmung der zu speichernden Daten zu sehen.**

Denn nach ständiger Rechtsprechung des EGMR verlangt das Bestimmtheitserfordernis, dass der zulässige Zweck der Maßnahme, die Reichweite und Grenzen eines allfälligen Ermessens sowie die Kriterien, nach denen es auszuüben ist, hinreichend erkennbar sind, insbesondere, dass vorhersehbar ist, unter welchen Umständen Eingriffe zulässig sind (EGMR, Malone gg. Großbritannien, 27.06. 1984; EGMR, Kopp gg. die Schweiz, 25.03. 1998). Die Verhältnismäßigkeit des unmittelbaren Eingriffs in die Rechte der Antragsteller/innen, nämlich durch die Speicherung von Vorratsdaten gemäß § 102a TKG, lässt sich nur beurteilen, wenn die Norm im Zusammenhang mit jenen Bestimmungen gelesen wird, welche die Begrenzung im Sinne der

zitierten Judikatur regeln.

Daher werden als Antragsgegenstände auch § 102b TKG iVm § 135 Abs 2a StPO (Verwendung von Vorratsdaten) und § 99 Abs. 5 Z 2 bis 4 TKG iVm § 76a Abs 2 StPO sowie § 53 Abs 3a und 3b SPG (Ausnahmen von den Prinzipien des § 102b TKG) releviert.

Die Aufhebung korrespondierender Bestimmungen der StPO und des SPG wird grundsätzlich (nur) soweit beantragt, als ein logisch und sprachlich untrennbarer Zusammenhang besteht. Die einzige Ausnahme diesbezüglich stellt die (eventualiter) Anfechtung des § 76a Abs 2 Z 1 und 4 StPO dar, der zwar nicht formell auf Vorratsdaten oder § 102a TKG verweist, aber durch den Verweis auf § 99 Abs 5 Z 2 TKG materiell (auch) die Verwendung von Vorratsdaten regelt.

IV.1.1 Zur unmittelbaren Betroffenheit

Obwohl § 102a TKG unmittelbar nur die Anbieter elektronischer Kommunikationsdienste adressiert, sind die Antragsteller/innen aber dennoch unmittelbar in ihrer Rechtssphäre betroffen. Es ist nämlich gerade der Zweck der Vorratsdatenspeicherung, die personenbezogenen Daten der Nutzer elektronischer Kommunikationsdienste zu erfassen und für 6 Monate zu speichern. Die Verarbeitung von personenbezogenen Daten ist jedenfalls ein Eingriff in die durch § 1 DSG 2000 und Art 8 EMRK geschützten Rechtspositionen der Antragsteller/innen.

Die Eigenschaft als Normadressat ist nicht unbedingt eine notwendige Voraussetzung für die unmittelbare Betroffenheit in der Rechtssphäre (vgl. dazu die unmittelbare Betroffenheit von Arbeitnehmerinnen durch ein – an die Arbeitgeber gerichtetes - Nachtarbeitsverbot für Frauen, VfSlg 13.038/1992).

Betroffen sind alle natürlichen und juristischen Personen, die bei einem speicherpflichtigen Anbieter im Sinne des § 102a TKG einen Vertrag zur Nutzung eines oder mehrerer der in § 102a Abs. 2 bis 4 aufgezählten Dienste (Mobilfunk- und Festnetztelefonie, Internetzugangsdienst, E-Mail Dienst, Voice over IP) abgeschlossen haben und daher mit ihren Teilnehmerdaten („Stammdaten") zu den jeweiligen Verkehrsdaten von der Vorratsdatenspeicherung erfasst werden. Zum Nachweis dieser Betroffenheit werden jedenfalls vom Erstantragsteller Kopien der entsprechenden Verträge bzw. Einzelgesprächsnachweise diesem Schriftsatz beigelegt. Die vorgelegten Verträge decken alle Datenkategorien der Abs. 2 bis 4 leg cit ab. Sollte die Vorlage entsprechender Nachweise für alle Antragsteller zum Nachweis der Legitimation erforderlich sein, können diese im Rahmen eines Verbesserungsauftrages nachgereicht werden.

Zur Beurteilung der Speicherpflicht der jeweiligen Anbieter hat das BMVIT eine Liste der aktuell speicherpflichtigen Anbieter im Internet veröffentlicht (**Anlage./B**). Festzuhalten ist, dass sämtliche Mobiltelefonie-Anbieter speicherpflichtig im Sinne des § 102a TKG sind und die entsprechenden Verträge im Regelfall (wie auch beim Erstantragsteller) einen mobilen Internetzugang sowie die Nutzung eines E-Mail Dienstes beinhalten.

Bei der Erfassung der großen Zahl an Antragsteller/innen haben die Initiatoren des „Arbeitskreis Vorratsdatenspeicherung“ (www.akvorrat.at) aus Vorsicht durch gezielte Information betreffend die Unterzeichnung der Vollmacht darauf aufmerksam macht, dass nur solche Personen im Rahmen dieses Antrags jedenfalls aktuell und unmittelbar rechtlich betroffen sind, die im eigenen Namen einen Vertrag mit einem speicherpflichtigen Anbieter abgeschlossen haben, weil dadurch auf jeden Fall personenbezogene Daten der Antragsteller/innen gespeichert werden.

Nur der Vollständigkeit halber sei erwähnt, dass auch Kunden nicht RTR-finanzierungspflichtiger (und damit nicht speicherpflichtiger) Anbieter von Telekommunikationsdiensten mit an Sicherheit grenzender Wahrscheinlichkeit von der VDS betroffen sind. Kommuniziert man nämlich mit einem Kunden eines „großen“/speicherpflichtigen Unternehmens, muss dieses auch die Verkehrsdaten des nicht der Speicherpflicht unterliegenden Anschlusses speichern. Aus der Sicht der nach §§ 102b und § 99 Abs 5 TKG auskunftsberechtigten Behörden sind auch diese Daten personenbezogen, weil diese sich in weiterer Folge mittels Stammdatenabfrage gemäß § 90 TKG beim „kleinen“ Anbieter mit rechtlich zulässigen Mitteln personalisieren lassen.

IV.1.2 Zur aktuellen Betroffenheit

Der Grundrechtseingriff wird gegenwärtig durch das Gesetz selbst bewirkt, ohne durch einen Bescheid oder ein Gerichtsurteil aktualisiert werden zu müssen. Wie eben ausgeführt, ist schon die Speicherung relevant und dazu braucht es keine zusätzlichen Konkretisierungen mehr.

„Ist ein weiterer Rechtsakt zwar möglich aber nicht erforderlich (wie etwa die Beantragung eines Feststellungsbescheides oder eines Feststellungsurteils bei völlig klarer Rechtslage), so steht dies einem Individualantrag nicht entgegen.“ (*Rohregger in* Korinek/Holoubek, Kommentar zum B-VG, zu Art 140, RZ 171).

Die Bestimmtheit der gesetzlichen Verpflichtung zur Speicherung der Daten gemäß § 102a TKG kommt in ihrer Präzision einem individuellen Rechtsakt gleich und lässt keinen Ermessensspielraum. Die anfechtungsgegenständlichen Bestimmungen sind seit 01.04.2012 in Kraft und seither ist die neue Rechtslage anwendbar auf sämtliche bestehenden Verträge: Verbindungsdaten, die am 1.4.2012 beim Anbieter noch aus betrieblichen Gründen vorgelegen sind und mangels weiterer betrieblicher Rechtfertigung seither eigentlich gelöscht werden müssten, sind nun aufgrund des § 102a TKG zu speichern. Die unmittelbarsten Auswirkungen bestehen dabei im Bereich der E-Mail Dienste, weil keiner der nun speicherpflichtigen Anbieter bisher E-Mail Verbindungsdaten für betriebliche Zwecke gespeichert hat.[3]

[3] Näheres bei http://bim.lbg.ac.at/de/digital-rights/studie-zur-datensicherheit-umsetzung-vorratsdatenspeicherung

IV.1.3 Zur rechtlichen Betroffenheit

Voraussetzung für die Zulässigkeit ist, dass die Antragsteller/innen in ihrer rechtlichen Sphäre betroffen sind und nicht bloß faktische/wirtschaftliche Interessen berührt sind. Die betroffenen Rechte müssen nicht notwendigerweise verfassungsgesetzlich gewährleistet sein. Erst im Hinblick auf die Verfassungswidrigkeit der angefochtenen Normen müssen konkrete verfassungsgesetzlich gewährleistete Rechte geltend gemacht werden. Die Speicheranordnung des § 102a TKG greift unmittelbar ein in die Rechte der Antragsteller/innen gemäß

- Art. 1 § 1 DSG 2000 (Art. 8 GRC, Grundrecht auf Datenschutz) und
- Art. 8 EMRK (Art. 7 GRC, Privatleben und Schutz der Kommunitkation).

Zum Bedeutungsgehalt der Rechte der EU Grundrechte-Charta bestimmt Art. 52 GRC: "So weit diese Charta Rechte enthält, die den durch die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten garantierten Rechten entsprechen, haben sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird. (...)".

Weiters garantiert das Prinzip des Art. 53 ein minimales Schutzniveau: "Keine Bestimmung dieser Charta ist als eine Einschränkung oder Verletzung der Menschenrechte und Grundfreiheiten auszulegen, die in dem jeweiligen Anwendungsbereich durch das Recht der Union und das Völkerrecht sowie durch die internationalen Übereinkommen, bei denen die Union, die Gemeinschaft oder alle Mitgliedstaaten Vertragsparteien sind, darunter insbesondere die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten, sowie durch die Verfassungen der Mitgliedstaaten anerkannt werden."

Art. 8 EMRK garantiert: „Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs." Die korrespondierende Norm auf EU Ebene Art. 7 GRC sichert jedermann das Recht auf „Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation" zu. Die Ersetzung des Ausdrucks „Korrespondenz" in Art 8 EMRK durch den Ausdruck „Kommunikation" in Art. 7 der GRC indiziert die Berücksichtigung der aktuellen technologischen Entwicklung.

Art. 8 GRC garantiert jeder Person das „Recht auf Schutz der sie betreffenden personenbezogenen Daten", wohingegen die EMRK ein Recht auf Datenschutz nicht explizit erwähnt. Allerdings hat der EGMR eine bemerkenswerte Dichte an Vorgaben in diesem Zusammenhang in seiner Rechtsprechung zu Art. 8 EMRK entwickelt (siehe zB *S. und Marper gg UK*, Erkenntnis vom 4. Dezember 2008). Wenngleich also das neue Grundrecht auf Datenschutz in Art. 8 GRC nicht ausdrücklich ein "entsprechendes Recht" in der EMRK hat, definiert doch die Rechtsprechung zu Art. 8 EMRK einen minimalen Standard für den Datenschutz in der EU. **Deshalb bestimmt der Art. 8 EMRK und seine Interpretation durch die Rechtsprechung des EGMR primär die Reichweite des neuen Grundrechts auf Datenschutz.**

Das innerstaatliche Datenschutzgrundrecht des § 1 DSG nimmt ausdrücklich Bezug auf die Achtung des Privat- und Familienlebens sowie (für staatliche Eingriffe) die

Eingriffsvoraussetzungen des Art. 8 Abs 2 EMRK. Dadurch wird auch für den Bedeutungsgehalt dieses Grundrechts die Judikatur des EGMR zu Art. 8 EMRK relevant.

Das Recht auf Datenschutz bezieht sich nach VfSlg 12.228/1989 nicht nur auf die Geheimhaltung von bereits erhobenen Daten, sondern auch bereits auf deren Ermittlung und Speicherung. Nach Ansicht des VfGH sind nicht nur personenbezogene, sondern auch berufsbezogene Daten, insbesondere Wirtschaftsdaten, vom sachlichen Geltungsbereich des Grundrechts umfasst. Die Eingriffe in Art. 8 EMRK, Art. 7 und 8 GRC sowie in § 1 DSG werden durch die Speicherpflicht des § 102a TKG bewirkt.

Das Ausmaß der Eingriffe wird aber auch von jenen Anfechtungsgegenständen bestimmt, welche die zulässigen Zwecke zur weiteren Datenverwendung normieren. Die Verhältnismäßigkeit der Speicherung selbst – also des primären Eingriffs – kann nur bestimmt werden, wenn sie in Verbindung mit den gesetzlich bestimmten Zwecken gesehen werden. Die Zweckbestimmungen und Zweckbindungen der

1. §§ 102b, 99 Abs. 5 Z 2 bis 4 TKG iVm
2. §§ 135 Abs. 2a, 76a Abs. 2 StPO sowie
3. § 53 Abs. 3a und Abs. 3b SPG

sind schon abstrakt unverhältnismäßig und bewirken daher für sich die Unverhältnismäßigkeit der Vorratsdatenspeicherung.

Obwohl § 102a TKG unmittelbar nur die Anbieter elektronischer Kommunikationsdienste adressiert, sind die Antragsteller/innen aber dennoch unmittelbar in ihrer Rechtssphäre betroffen. Es ist nämlich gerade der Zweck der Vorratsdatenspeicherung, die personenbezogenen Daten der Nutzer elektronischer Kommunikationsdienste zu erfassen und für 6 Monate zu speichern. Die Verarbeitung von personenbezogenen Daten ist jedenfalls ein Eingriff in die durch § 1 DSG 2000 und Art 8 EMRK geschützten Rechtspositionen der Antragsteller/innen. **Die Eigenschaft als Normadressat ist nicht unbedingt eine notwendige Voraussetzung für die unmittelbare Betroffenheit in der Rechtssphäre (vgl. dazu die unmittelbare Betroffenheit von Arbeitnehmerinnen durch ein – die Arbeitgeber adressierendes – Nachtarbeitsverbot für Frauen, VfSlg 13.038/1992).**

Die rechtliche Betroffenheit zeigt sich schließlich auch nach dem Vergleich der Situation der Betroffenen mit und ohne die angefochtenen Bestimmungen. Ohne die Speicherverpflichtung des § 102a TKG würden die personenbezogenen Verbindungsdaten in viel geringerem Umfang (zB keine E-Mail Daten) und regelmäßig für kürzere Zeit als 6 Monate gespeichert. Das Risiko einer rechtswidrigen Datenverwendung und damit das Ausmaß des weiteren Grundrechtseingriffs wären ohne Vorratsdatenspeicherung deutlich geringer.

IV.2 Zur Unzumutbarkeit eines Umwegs

IV.2.1 Allgemeines

Jedenfalls unzumutbar ist es nach der Judikatur des VfGH ein strafbares (zB VfSlg. 11.369/1987, 15.509/1999, 16.202/2001) oder auch nur rechtswidriges (zB VfSlg. 11.853/1988, 12.379/1990, 13.659/1993, 13.725/1994, 14.260/1995) Verhalten zu provozieren, nur um einen Weg zum VfGH zu finden. Als Endbetroffener von der Vorratsdatenspeicherung kann man das im Hinblick auf die Speicherung selbst auch gar nicht. Im Hinblick auf die Verwendung von Vorratsdaten ist es den Antragssteller/innen nicht zumutbar, „irgendeine" Straftat zu begehen, welche die Polizei nur mittels Vorratsdaten aufklären könnte. Auch einem Provider ist es nicht zumutbar, sich strafbar zu machen, indem er trotz erhaltenem Kostenersatz nicht speichert, nur um über den Strafbescheid einen Weg zum VfGH zu erhalten.

IV.2.2 Unzumutbarkeit bzw. Unmöglichkeit der Erlangung eines anfechtbaren Verwaltungsaktes

Das Rechtsschutzbegehren der Antragsteller/innen bezieht sich auf die Unterlassung der Speicherung bzw. die Löschung der personenbezogenen Daten, deren Speicherung durch § 102a TKG angeordnet wird.

Materiell kann sich ein solches Löschungsbegehren nur auf § 27 DSG stützen. Zur Durchsetzung im Verwaltungsweg kommt abstrakt nur die Datenschutzkommission in Frage. Diese ist im Zusammenhang mit der Vorratsdatenspeicherung aber nur für Streitigkeiten zu Auskunftsbegehren zuständig. Diese Zuständigkeit ist zwar nicht explizit normiert, lässt sich aber durch Interpretation der angefochtenen Bestimmungen in Bezug auf deren Entstehungsgeschichte erschließen.

Diese Auslegung hat Konsequenzen für die Zuständigkeit im Rechtsschutz, denn die Datenschutzkommission ist eine Kontrollbehörde und nur dann zuständig, wenn die Anbieter „als Auftraggeber des öffentlichen Bereiches" gelten. Die Datenschutzkommission wie auch der Verfassungsdienst des Bundeskanzleramts haben sich in ihren jeweiligen Stellungnahmen zur Begutachtung des Gesetzes dagegen ausgesprochen, dass ein Anbieter hinsichtlich der Verarbeitung von Vorratsdaten innerhalb des vom ihm beherrschten Bereiches als Auftraggeber des öffentlichen Bereichs gesetzlich bestimmt werden soll. Der in dieser Hinsicht vorgeschlagene § 102a Abs. 9 des Ministerialentwurfes betreffend ein Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 - TKG 2003 geändert wird (117/ME) sah Folgendes vor: *„(9) Im Hinblick auf Vorratsdaten gilt jener Anbieter, der die Daten den vorstehenden Absätzen entsprechend zu speichern hat, als Auftraggeber des öffentlichen Bereichs gemäß § 4 Z 4 in Verbindung mit § 5 Abs. 2 Z 2 DSG 2000. Im Hinblick auf Vorratsdaten, die gemäß § 102b übermittelt werden, richten sich die Ansprüche auf Information oder Auskunft über diese Datenverwendung ausschließlich nach den Bestimmungen der StPO."* Diese Bestimmung wurde jedoch letztlich nicht in die Novellierung aufgenommen. Dies legt den Schluss nahe, dass der Gesetzgeber die Anbieter im Sinne des §102a TKG gerade nicht als „Auftraggeber des öffentlichen Bereichs" iSd § 5 Abs 2 DSG einordnen wollte.

Wenn der Anbieter Auftraggeber des privaten Bereiches ist, liegt die datenschutzrechtliche Zuständigkeit im Falle von Löschungsbegehren auch bezüglich Vorratsdaten bei den ordentlichen Gerichten.

Der Auskunftsanspruch nach § 26 DSG bleibt aber jedenfalls in der Verantwortung der Datenschutzkommission. Verlangte man Auskunft und erhielte sie auch nach Anrufng der DSK nicht, würde der VfGH im Falle einer Bescheidbeschwerde gemäß Art 144 B-VG wohl als Minimum das Wort „ausschließlich" in § 102b Abs 1 TKG aufheben. Danach müsste/könnte nach § 26 DSG eine Auskunft an den Betroffenen erfolgen. Das bringt daher nichts im Hinblick auf die Speicherung. Auskunft ist ganz allgemein nicht zielführend, weil

- das Auskunftsbegehren jeden Tag gestellt und
- bei allen Providern eingereicht werden müsste
- und ein Auskunftsbegehren schließlich gar nicht dem Rechtschutzbegehren der Antragsteller/innen (auf Unterlassung der Speicherung und Löschung der gespeicherten Daten) entspricht.

Praktisch gesehen müsste man etwa bezüglich E-Mails bei allen Providern anfragen, wo denn jene Mitmenschen Kunden oder Kundinnen sind, die dem Betroffenen eine E-Mail geschickt haben. All dies müsste erst einmal ausfindig gemacht werden!

IV.2.3 Unzumutbarkeit der Erlangung eines gerichtlichen Urteils

Ein theoretisch möglicher Umweg wäre ein Zivilverfahren gemäß § 1 Abs. 5 DSG in Verbindung mit § 27 DSG (Recht auf Löschung) und §32 DSG (Zivilrechtsweg).

Dies ist schon theoretisch insofern völlig aussichtslos, da im Gesetz klar und detailliert normiert ist, was zu speichern ist. Die Gerichte haben daher keinen Entscheidungsspielraum, einem Löschungsbegehren in Bezug auf die nach § 102a TKG zu speichernden Daten stattzugeben, es sei denn, sie legen die Frage zur Vorabentscheidung dem EuGH nach Art. 267 AEUV oder dem VfGH nach Art. 89 Abs. 2 B-VG vor.

Unzumutbar ist es nach der Judikatur des VfGH (siehe RS VfSlg 11.402), einen Feststellungsbescheid zu beantragen, nur um einen Umweg zum VfGH zu eröffnen, obwohl der Rechtsschutzzweck mit dem Feststellungsbescheid im Verwaltungsverfahren gar nicht erreicht werden kann. Wenn der einzige Zweck des Feststellungsbescheides darin besteht, damit ein Mittel zu gewinnen, um die gegen ein Gesetz bestehenden verfassungsrechtlichen Bedenken an den VfGH heranzutragen, ist ein solcher Feststellungsbescheid seit Einführung des Individualantrages (anders als zuvor, vgl. zB VfSlg. 6392/1971) eben kein für eine zweckentsprechende Rechtsverfolgung notwendiges Mittel mehr (vgl. Erkenntnis des VfGH vom 20.03.1986 V40/84, V18/86, S 9, das zum selben Ergebnis kommt).

Was für die Erwirkung eines Feststellungsbescheides gilt, muss umso mehr gelten, wenn ein Zivilverfahren bei vollem Kostenrisiko allein zu dem Zweck geführt werden müsste, einen Umweg zum VfGH zu finden.

Einem Antrag auf Löschung der Vorratsdaten oder einem Begehren auf Unterlassung der Speicherung kann ein Zivilgericht nur stattgeben, wenn die gesetzliche Grundlage im § 102a TKG beseitigt wird. Ansonsten ist die Norm nämlich klar und unbedingt und lässt dem Gericht keinen Entscheidungsspielraum. Nur der VfGH ist innerstaatlich kompetent, die gesetzliche Grundlage für die Vorratsdatenspeicherung aufzuheben.

Für die Antragsteller ist es daher unzumutbar, ein Zivilverfahren (bei vollem Kostenrisiko) einzig deshalb zu führen, um nach Durchlaufen des Instanzenzuges einen Weg zum VfGH zu erhalten, falls das Gericht zweiter Instanz oder der Oberste Gerichtshof (siehe Artikel 89 B-VG) die Bedenken der Antragsteller in Bezug auf die Verfassungswidrigkeit der Vorratsdatenspeicherung teilt und die Frage dem VfGH vorlegt. Ein subjektives Antragsrecht der Partei gibt es in diesem Fall nicht. Allerdings hat der VfGH bereits mehrfach ausgesprochen, dass dies für sich kein Argument gegen die Zumutbarkeit des Umwegs über die Gerichte ist.

Das Rechtsschutzinteresse der Antragsteller (Unterlassung der Speicherung bzw. Löschung ihrer Daten) kann bei Einhaltung aller Vorschriften ausschließlich dann erfüllt werden, wenn der VfGH die gesetzliche Speicheranordnung (§ 102a TKG) aufhebt. Der Umweg über ein gerichtliches Verfahren widerspricht einer zweckentsprechenden Rechtsverfolgung – er bedeutet für die tausenden Antragsteller/innen einen hohen Zeitaufwand ohne jede Aussicht, dass ein ordentliches Gericht – ohne „zwischengeschaltete" Entscheidung des VfGH – ein Speicherverbot bzw. ein Löschungsgebot auferlegen kann.

Unzumutbar ist der „Umweg" eines Zivilverfahrens auch im Hinblick auf dessen Wirkung auf Dritte – nämlich die speicherpflichtigen Anbieter, die von den Antragsteller/innen beklagt werden müssen. Ein Anbieter müsste sich nämlich – ebenfalls bei vollem Kostenrisiko – jedenfalls auf einen Zivilprozess einlassen, um nicht eine Verwaltungsstrafe nach § 109 Abs 3 Z 22 TKG einzugehen. Dieses Risiko müsste ein Anbieter auf sich nehmen, obwohl er nur eine gesetzliche Pflicht erfüllt (also gar nicht die freie Entscheidung getroffen hat, diese Daten zu verarbeiten) und die gespeicherten Vorratsdaten nicht einmal für eigene Zwecke nutzen darf.

IV.2.4 Zusammenfassung

Da die Erlangung eines anfechtbaren Verwaltungsaktes unzumutbar bzw. unmöglich ist und die Erlangung eines gerichtlichen Urteils ebenfalls unzumutbar ist, führt der einzige zumutbare Weg, die grundrechtsverletzende Vorratsspeicherung zu bekämpfen, ohne Umweg zum VfGH. Der vorliegende Individualantrag ist daher zulässig.

V. Darlegung der Bedenken (materiell)

V.1 Allgemeine Überlegungen

Nachstehend sollen in der gebotenen Knappheit die Bedenken der Antragsteller/innen dargestellt werden. Die Verfassungswidrigkeit der angefochtenen Bestimmungen liegt nach Dafürhalten der Antragsteller/innen (insbesondere) in der Verletzung folgender verfassungsrechtlich garantierten Grundrechte:

- **Art. 8 EMRK / Art 7 GRC** (Privatleben und Familienleben, Schutz der Kommunikation)
- **Art. 1 § 1 DSG 2000 / Art 8 GRC** (Grundrecht auf Datenschutz)
- **Art. 10 EMRK / Art 11 GRC** (Meinungs- und Informationsfreiheit, Redaktionsgeheimnis)
- **Art. 11 EMRK / Art 12 GRC** (Versammlungs- und Vereinigungsfreiheit)
- **Art 10a StGG** (Fernmeldegeheimnis)
- **Art 6 EMRK / Art 48 GRC** (Unschuldsvermutung im Strafverfahren)

Grundsätzlich sollte das Verhältnis zwischen einem demokratischen Verfassungsstaat und seinen Bürgerinnen und Bürgern bzw. allen in seinem Machtbereich lebenden Menschen von Vertrauen geprägt sein. Die/der Einzelne soll darauf vertrauen können, dass in ihre/seine grundrechtlich geschützten Positionen im Zuge von Ermittlungstätigkeiten bzw. Strafverfolgungsmaßnahmen grundsätzlich nur bei Vorliegen entsprechender Verdachtsmomente, also als ultima ratio, unter Wahrung der rechtstaatlichen Prinzipien, insbesondere unter Beachtung des Verhältnismäßigkeitsprinzips eingegriffen wird. Der Grundsatz, dass gegen eine bestimmte Person ausschließlich bei Vorliegen von Verdachtsmomenten Ermittlungs- bzw. Verfolgungsmaßnahmen gesetzt werden, zieht sich gleich einem roten Faden durch alle rechtsstaatlichen Gesetzgebungen moderner demokratischer Prägung.

Die VDS-RL geht von diesem Grundsatz ab, indem sie eine **verdachtsunabhängige**, gleichsam antizipierte „**Sicherung von Beweismitteln**" vorschreibt. Die Grundidee dabei ist simpel: Potenziell ist jeder verdächtig.

Zwar werden schon derzeit vielfältig personenbezogene Daten ermittelt und verarbeitet. Diese Datenanwendungen erfolgen in aller Regel aber

- entweder zur individuellen Aufklärung und Verfolgung konkret begangener Straftaten, zur Erfüllung eines Vertrages und somit zumindest mittelbar auf Wunsch bzw. mit Zustimmung der datenschutzrechtlich Betroffenen,
- oder aber mit dem Ziel, der Gesellschaft die unterschiedlichsten Leistungen der öffentlichen Daseinsversorgung zur Verfügung zu stellen.

Davon unterscheidet sich die Vorratsdatenspeicherung im Sinne der Richtlinie schon durch ihre Zielsetzung in fundamentaler Weise, da personenbezogene Telekommunikations- und Bewegungsdaten aller Kunden, die Dienste eines Telekommunikationsunternehmens in Anspruch

nehmen, präventiv zum Zwecke der Ermittlung, Feststellung und Verfolgung von Straftaten ohne irgendeinen konkreten Tatverdacht gesammelt und verarbeitet werden.

Mit der grundrechtliche Eingriffe minimierenden rechtsstaatlichen Tradition bricht die Richtlinie. Mussten verarbeitete Verkehrs- und Standortdaten bisher teilweise sofort, grundsätzlich aber jedenfalls dann gelöscht werden, wenn und soweit sie etwa für die Bereitstellung von Telekommunikationsdiensten und in weiterer Folge für die Abrechnung nicht mehr erforderlich waren, wurde diese im Sinne eines effektiven und grundrechtskonformen Datenschutzes normierte Löschungsverpflichtung durch die Richtlinie 2006/24/EG in eine verdachtsunabhängige, flächendeckende Speicherungspflicht verkehrt, um „schwere Straftaten", insbesondere Terrorakte und organisierte Kriminalität, bekämpfen zu können.

Die österreichische Umsetzung durch **§ 102a TKG** stellt im Ergebnis einen **Paradigmenwechsel** dar, der **aus grundrechtlicher Sicht nicht zu rechtfertigen** ist. Eine vergleichbare Maßnahme in der realen Welt wäre, wenn künftig gesetzlich vorgeschrieben würde, alle Absender und Adressaten jedweden Briefes durch die Post dokumentieren zu lassen, weil potentiell jeder Briefkontakt ermittlungsrelevante Information liefern könnte.

V.2. Die schleichende (atmosphärische) Veränderung der Gesellschaft durch die VDS

Die Intensität des Eingriffs für den Grundrechtsträger wird davon beeinflusst, welche über die Informationserhebung hinausgehenden Nachteile ihm aufgrund der Maßnahme drohen oder von ihm nicht ohne Grund befürchtet werden. Die Schwere des Eingriffs nimmt mit der Möglichkeit der Nutzung der Daten für Folgeeingriffe in Grundrechte der Betroffenen zu, sowie mit der Möglichkeit der Verknüpfung mit anderen Daten, die wiederum andere Folgemaßnahmen auslösen können (Vgl BVerfGE 100, 313 (376); 113, 348 (382); 115, 320 (347 f); BVerfG, NJW 2007, 2464 (2469)). Zu bedenken ist auch, dass im Fall einer konkreten Datenverwendung durch Strafverfolgungsbehörden aber nicht nur in die Rechtssphäre etwa eines möglichen Straftäters oder dessen Komplizen eingegriffen wird, sondern auch in die Rechtssphäre derjenigen Personen, die mit den Adressaten der Maßnahme über Telekommunikationseinrichtungen nur zufällig in Verbindung standen oder stehen. Dies schafft nach der Ansicht des EGMR ein System der Überwachung zum Schutz der Sicherheit des Staates und der Gesellschaft, das die Demokratie bzw. die Rechtsstaatlichkeit, die es schützen soll, aushöhlen bzw. umgehen könnte.

Vor allem aber – und dies ist die Ansicht und die Sorge der Antragsteller/innen – verlieren die Menschen das Gefühl, frei, selbstbestimmt und unbeobachtet leben zu können und nicht behelligt zu werden, wenn, soweit und solange sie die Gesetze des Staates und der Gesellschaft achten und befolgen und nicht delinquent werden. Das Verhalten der Menschen wird sich unter der verdachtsunabhängigen Erfassung alltäglicher Lebensäußerungen schleichend verändern, wo Vertrauen die Basis zwischenmenschlicher Kommunikation war, wird Misstrauen herrschen.

Anhand einiger weniger Beispiele soll verdeutlicht werden, inwieweit Menschen durch die Vorratsdatenspeicherung in der angstfreien Inanspruchnahme ihrer Grundrechte eingeschränkt oder verunsichert werden können:

- Inanspruchnahme von Aidsberatungsstellen, psychologischen Diensten, Seelsorgern, Kontakt zu Rechtsanwälten, Ärzten generell, Kontakt zu diskriminierten bzw. unter Generalverdacht stehenden Gruppen usw. (**Art. 8 EMRK**);
- Mitteilungen an Medien/Redaktionen im öffentlichen Interesse (whistleblowing), Meinungsäußerung in Blogs, Foren etc (**Art. 10 EMRK**);
- Beitritt oder auch nur Besuch von oder Kontaktnahme zu politischen Parteien, Religionsgemeinschaften, Vereinigungen (zB unbequeme Bürgerinitiativen), Teilnahme an Demonstrationen etc. (**Art. 11 EMRK**).

Überall dort, wo Personen befürchten, aufgrund der Vorratsdatenspeicherung bei der Inanspruchnahme von Grundrechten eventuell Nachteile zu erleiden, beeinträchtigt die Vorratsdatenspeicherung diese Grundrechte.

V.3 Zur Bedeutung der Unschuldsvermutung in einem freien Gemeinwesen

Die garantierte Unschuldsvermutung ist eine wesentliche Voraussetzung einer auf angstfreier Kommunikation basierenden Gesellschaft freier Menschen. Der EGMR hat zur Bedeutung der Unschuldsvermutung in S. und Marper vs UK klargestellt (zitiert aus NL Menschenrechte, http://www.menschenrechte.ac.at/docs/08_6/08_6_14):

„Im vorliegenden Zusammenhang kommt der Gefahr der Stigmatisierung besondere Bedeutung zu. Diese ergibt sich aus der Tatsache, dass Personen in der Situation der Bf., die nicht verurteilt wurden und für die daher die Unschuldsvermutung gilt, gleich behandelt werden wie verurteilte Personen. Zwar kann die Speicherung der privaten Daten der Bf. nicht mit der Äußerung eines Verdachts gleichgesetzt werden. Ihre Wahrnehmung, nicht als unschuldig behandelt zu werden, wird aber dadurch verdeutlicht, dass ihre Daten ebenso wie die von verurteilten Personen unbeschränkt gespeichert werden, während die Daten von nie verdächtigten Personen vernichtet werden müssen. Die Regierung bringt dazu vor, der einzige Grund für die Speicherung der Daten bestehe in der Steigerung der Größe und damit der Nutzbarkeit der Datenbank zur künftigen Identifizierung von Straftätern. Der GH hält dieses Argument jedoch für schwer vereinbar mit der gesetzlichen Verpflichtung zur Vernichtung der Fingerabdrücke und Proben von Freiwilligen, hätte dieses Material doch ähnlichen Wert für die Vergrößerung der Datenbank."

Die flächendeckende Speicherung erhöht zwingend und logisch die Wahrscheinlichkeit, dass sich auch unbescholtene und unschuldige Menschen in einem Ermittlungsverfahren rechtfertigen müssen, warum sie in einer bestimmten Weise zu einer bestimmten Zeit mit einem bestimmten Anschluss in Kontakt standen. Allein in solche Ermittlungen zu geraten – auch wenn sich später herausstellt, dass es rein zufällig war und keine rechtlichen Konsequenzen folgen – kann schon zu erheblichen Nachteiligen privaten oder beruflichen Konsequenzen führen. Die Vorratsdatenspeicherung ist jedenfalls geeignet, den Kreis der Verdächtigen (letztendlich

unendlich) zu vergrößern, weil die Zahl der auswertbaren Kommunikationsverbindungen größer und umfassender wird.

Nicht mit Art. 8 EMRK bzw. Art. 7 GRC vereinbar ist auch die grundsätzliche Gefahr, die aus der systemimmanenten unzuverlässigen Aussagekraft riesiger Datenmengen resultiert, die durch die Vorratsspeicherung von Telekommunikations- und Internetzugangsdaten in allen EU Mitgliedsstaaten angesammelt werden. Die – unter Technikern – „goldene Regel zur Optimierung von Datensicherheit" ist das Prinzip der Datensparsamkeit. Das Risiko steigt exponentiell zur Menge der gesammelten Informationen. Auch der Schaden, der an der Informationsfreiheit durch die permanente Aufzeichnung des Kommunikationsverhaltens der gesamten europäischen Gesellschaft entsteht, lässt sich mit gleichwohl notwendigen „Safeguards" nicht beheben.

Die durch die angefochtenen Normen in Österreich (überschießend) umgesetzte Vorratsdatenspeicherung ist eine Abkehr vom Grundsatz der Vertraulichkeit der Kommunikation aufgrund und zugunsten eines generellen Misstrauens gegenüber allen Menschen.

Nach Auffassung des VfGH (zB VfSlg 12.228/1989 und 12.880/1991) haben unter Wahrung der Rahmenfunktion grundrechtlicher Anordnungen Gesetze, die staatliche Behörden zu Eingriffen in das Grundrecht auf Datenschutz ermächtigen, nicht nur einem der enumerativ aufgezählten Rechtsgüter des Art. 8 Abs 2 EMRK zu dienen; Eingriffsgesetze müssen vielmehr auch hinreichend konkret, zur Erreichung eines der enumerativ aufgezählten Eingriffsziele erforderlich sein und auf einer zulänglichen Interessenabwägung beruhen.

V.4 Argumentation nach dem Schema der Verhältnismäßigkeitsprüfung

V.4.1 Die Vorratsdatenspeicherung (VDS) betrifft alle Nutzer von Kommunikationsdiensten aktuell, unmittelbar und nachteilig in ihrer Grundrechtssphäre.

Schon die Speicherung der Verbindungsdaten ist ein Grundrechtseingriff, nicht erst eine allfällige Auskunft an die Behörden – diese aber natürlich auch.

Der EGMR wertet in *Segerstedt-Wiberg u.a.* v. Schweden, Nr. 62332/00, 06.06.2006 in § 72 des Urteils die Sammlung und Aufbewahrung allgemein zugänglicher Quellen wie Artikel in Zeitschriften als Eingriff in das Privatleben, sofern sie systematisch durch Behörden (Geheimdienste, Verfassungsschutz) erfolgt. **Revolutionär für den EGMR ist in *Segerstedt-Wiberg* aber die Feststellung, dass allein schon die (überschießende bzw. nicht gerechtfertigte) Speicherung von Daten einerseits Art. 8 EMRK verletzt, andererseits aber auch Art. 10 und 11 EMRK,** also die Rechte auf Meinungs- und Versammlungsfreiheit (in § 107 des Urteils stellte der GH fest, dass eine Speicherung von Daten zu politischen Überzeugungen, Tätigkeiten und Parteizugehörigkeit, die nicht nach Art. 8 Abs. 2 gerechtfertigt werden kann, ipso facto auch eine Verletzung der politischen Rechte aus Art. 10 und 11 EMRK bedeute).

Dieser Argumentation folgend bewirkt die in **§ 102a TKG** normierte Speicherverpflichtung einen Eingriff in **Art 8 EMRK / Art 7 GRC, § 1 DSG / Art 8 GRC, Art 10 EMRK / Art 11 GRC und**

Art 11 EMRK / Art 12 GRC. Der Eingriff in **Art 6 EMRK** / Art 48 GRC (Unschuldsvermutung) wurde bereits unter Punkt V.3 argumentiert.

Die darüber hinaus angefochtenen Bestimmungen **(§ 102b TKG, § 99 Abs 5 TKG, § 135 Abs 2a StPO, § 76a Abs 2 StPO sowie § 53 Abs 3a und 3b SPG)** regeln die Verwendungszwecke der gemäß § 102a TKG gespeicherten personenbezogenen Verkehrsdaten. Weil die Speicheranordnung nicht isoliert von ihrer Zweckbestimmung beurteilt werden kann, perpetuieren diese Bestimmungen die geltend gemachten Grundrechtseingriffe. Darüber hinaus bewirken sie auch einen Eingriff in das **Fernmeldegeheimnis gemäß Art 10a StGG**. Zwar hatte der VfGH bisher noch keine Entscheidung dazu zu treffen, ob auch Verkehrsdaten (oder nur Inhaltsdaten) im Schutzbereich des Art 10a StGG liegen. Eindeutig beantwortet hat jedoch der Verwaltungsgerichtshofe diese Frage in seinem Erkenntnis vom 27.5.2009 zu 2007/05/0280: „Verkehrsdaten unterliegen dem Fernmeldegeheimnis des Art 10a StGG und Art 8 EMRK und daher dem Richtervorbehalt (vgl. den Vorabentscheidungsbeschluss des OGH vom 13. November 2007, 4 Ob 141/07z, sowie den hiezu ergangenen Beschluss des EuGH vom 19. Februar 2009, C-557/07)." Konkret hat der VwGH diese Entscheidung in Bezug auf dynamische IP-Adressen bezogen, in diesem Sinne bewirken auch § 76a Abs 2 StPO sowie § 53 Abs 3a SPG – die sich vor allem auf IP-Adressen beziehen – einen Eingriff in Art 10a StGG.

V.4.2 Die VDS ist gar <u>nicht geeignet, die vorgeblichen Zwecke zu erreichen</u>

V.4.2.1 Die von der zugrundeliegenden Richtlinie vorgegebene Bekämpfung schwerer Kriminalität wird durch die VDS nicht merkbar gefördert (belegt durch Studien, keine Gegenstudien, immer nur emotionale Einzelfälle). Beispielsweise fasst eine aktuelle Studie des deutschen Max-Planck-Instituts für Strafrecht und Kriminologie als Ergebnis ihrer Untersuchung zu den deliktsspezifischen Aufklärungsquoten für den Zeitraum 1987 bis 2010 in Deutschland zusammen, dass der Wegfall der Vorratsdatenspeicherung nicht als Ursache für Bewegungen in der Aufklärungsquote herangezogen werden kann. Dieser Befund gilt insbesondere für die Bereiche der Computerkriminalität sowie der so genannten Internetkriminalität. Die Studie selbst liefert die Zahlen deliktsspezifisch und stellt fest, dass sich keine Bewegung durch den Wegfall der VDS ergibt.

Ein „ausweichen" ist in vielen Fällen trivial, Untersuchungen zeigten auch, dass Terroristen bereits jetzt gerade so kommunizieren, dass sie von der VDS nicht erfasst werden. Gerade Terrorismus ist auch ein „Langzeitdelikt", das sich über viele Jahre ziehen kann – 6 Monate sind daher hierfür auch ein kurzer Zeitraum (nach dem Denkmodell: vor Anschlag bitte 6 Monate warten?).

Nutzlos erscheint die VDS auch hinsichtlich der häufig besonders zur Rechtfertigung der VDS angeführten Einzeltäter (Breivik etc.): Diese kommunizieren nämlich mit gar niemandem (über die geplante Tat) und wären daher von der VDS gar nicht erfasst. Selbst dessen Suche nach Bombenbauanleitungen wäre mit der VDS nach aktueller Rechtslage auch nicht erfassbar, da die Speicherung von Inhaltsdaten ausdrücklich ausgeschlossen ist.

V.4.2.2 Selbst für den mittelschweren Bereich - zB Straftaten mit knapp über einem Jahr Strafrahmen - konnte kein Anstieg der Aufklärungsquote in jenen Mitgliedsstaaten belegt werden, in denen die VDS schon umgesetzt wurde. Gerade durch die Umsetzung könnte in diesem Bereich die Aufklärung sogar erschwert werden, da das Problem auch bei Kriminellen ins Blickfeld gerät und diese aktiv Gegenmaßnahmen ergreifen. Umgehungsmöglichkeiten werden allgemein bekannt. Beachtenswert sind in diesem Zusammenhang insbesondere die Pläne in Großbritannien, die VDS auszuweiten auf Facebook-, Twitter- und Online-Spiel-Kommunikation - also sind die bisherigen Mittel der VDS offensichtlich nicht ausreichend oder nicht geeignet.

V.4.3 Die VDS ist selbst dort, wo sie möglicherweise in manchen Einzelfällen die Ermittlungen unterstützt, nicht das schonendste Mittel, den Zweck zu erreichen

V.4.3.1 In den meisten Fällen würden schon betrieblich notwendig vorhandene Daten reichen, wenn die Investitionen zur VDS besser in mehr Personal der Exekutive investiert und Ermittlungen beschleunigt würden.

V.4.3.2 In den übrigen Fällen würde ein abgekürztes Verfahren reichen, bei dem ein Gericht bei entsprechender Verdachtslage anordnet, bestimmte Daten von bestimmten Teilnehmern "einzufrieren" (sog. "**Quick-Freeze**") Siehe dazu die **Cybercrime Konvention**, der Österreich zwar beigetreten ist (23.11.2001), welche aber nach mehr als 10 Jahren noch immer nicht ratifiziert ist – gar so dringend scheint die Verfolgung und der Datenbedarf also gar nicht zu sein. Laut (inoffiziellen) Aussagen von Polizisten scheint es insbesondere ein praktisches Problem zu sein, an benötigte Daten in anderen Ländern heranzukommen (sind diese vorhanden und ist die Auskunftserteilung legal etc). Es läge daher näher, das bereits bestehende „Arsenal" effektiv (bzw überhaupt) zu nutzen, bevor neue (weitere Daten) gesammelt werden.

V.4.4 Die VDS steht selbst dann, wenn man sie als das gelindeste, noch zum Ziel der Kriminalitätsbekämpfung führende Mittel ansieht, in keinem angemessenen Verhältnis zum Nachteil für die Einzelnen sowie die Gesellschaft

V.4.4.1 Je fragwürdiger die Eignung und die Notwendigkeit (im Sinne des gelindesten Mittels) erscheinen, desto höher sind die Anforderungen an die Verhältnismäßigkeit des Eingriffs.

V.4.4.2 Die Güterabwägung zeigt - wenn überhaupt - nur einen geringen positiven Effekt in wenigen Einzelfällen gegenüber einem schweren Eingriff in die Privatsphäre praktisch der gesamten Bevölkerung.

V.4.4.3 Die Unverhältnismäßigkeit der VDS ergibt sich auch daraus, dass die Verwendungszwecke viel zu weit gefasst sind und **keine ausreichenden Rechtsschutzmöglichkeiten** zur Verfügung stehen.

V.4.4.4 Sie führt auch zu einer gewissen Umkehr der Unschuldsvermutung: Man muss dann bis zu sechs Monate im Nachhinein erklären können, warum man jemanden kontaktiert hat (oder kontaktiert wurde). Denn die andere Person mag verdächtig sein – man selbst ist es aufgrund der

Kommunikation also auch. Die bloße Behauptung *„ich kann mich nicht erinnern"* wird zwar sehr oft der Wahrheit entsprechen, aber nützen wird sie nichts – bis zur Beseitigung jeglichen Verdachts!

V.4.5 Normierte Zwecke

V.4.5.1 Falls die VDS nicht schon dem Grunde nach als unverhältnismäßig gesehen wird, ergibt sich die mangelnde Verhältnismäßigkeit daraus, dass die Normen, welche die Verwendungszwecke regeln, eine überschießende Verwendungsmöglichkeit einräumen. Die Regelung der Zwecke betrifft die Anordnung der Speicherung (102a TKG) schon im Hinblick auf das Bestimmtheitsgebot, dass nach Datenschutzgrundsätzen über den allgemeinen Maßstab des Artikel 18 B-VG hinausgeht. Die Bindung der Verwaltung ist im Hinblick auf Überwachungsmaßnahmen besonders wichtig, da der Betroffene von solchen Maßnahmen naturgemäß keine Kenntnis und daher auch keine Möglichkeit hat, in einem vorgeschalteten Verfahren Einfluss auf das eingreifende Verhalten der Verwaltung zu nehmen.

Im Falle der Verhütung künftiger Straftaten kann nicht an dieselben Kriterien angeknüpft werden, die für die Gefahrenabwehr oder die Verfolgung begangener Straftaten entwickelt worden sind.

Maßnahmen der **Gefahrenabwehr** setzen eine **konkrete aktuelle Gefahrenlage** voraus, während die **Strafverfolgung** an den Verdacht einer **schon verwirklichten Straftat** anknüpft. Bei der Vorverlagerung des Eingriffs in eine Phase, in der sich noch kein konkreter Straftatbestand abzeichnet, besteht das Risiko, dass der Eingriff lediglich an ein noch schwer fassbares Geschehen anknüpft.

Da der Eingriff sich auf mögliche zukünftige Aktivitäten bezieht, kann er sich häufig nur auf Tatsachen stützen, bei denen noch offen ist, ob sie sich zu einer Rechtsgutverletzung weiterentwickeln (Vgl BVerfGE 110, 33 (59)). Man sondiert Kommunikationsvorgänge, bei denen nicht unbedingt klar sein muss, ob sie überhaupt mit einer Rechtsverletzung in Verbindung stehen. Sieht der Gesetzgeber in solchen Situationen Grundrechtseingriffe vor, so hat er die den Anlass bildenden Straftaten sowie die Anforderungen an Tatsachen, die auf die künftige Begehung hindeuten, derart bestimmt zu umschreiben, dass das besonders hohe Risiko einer Fehlprognose noch innerhalb des verfassungsrechtlichen Rahmens bleibt. Die Norm muss handlungsbegrenzende Tatbestandselemente enthalten, die einen Standard an Vorhersehbarkeit und Kontrollierbarkeit vergleichbar dem schaffen, der für die Aufgaben der Gefahrenabwehr und Strafverfolgung rechtsstaatlich geboten ist (Vgl BVerfGE 110, 33 (56)). Es muss den Betroffenen vorhersehbar und kontrollierbar (d.h. einsehbar) sein, aufgrund welcher ihrer Handlungen ihre Vorratsdaten von den Behörden verwendet werden.

V.4.5.2 In dieser Hinsicht äußerte der VfGH anlässlich eines Bescheidbeschwerdeverfahrens (VfSlg 16.369/ 2001) zur Auskunftsermächtigung des damaligen § 83 Abs 2 TKG entsprechende Bedenken:

„§83 Abs2 TKG ist angesichts der Weite seiner Ermächtigung, Auskünfte zu verlangen, kein nach §1 Abs2 DSG 2000 iVm Art 8 Abs 2 EMRK notwendiges, Eingriffe in das Grundrecht auf Datenschutz legitimierendes Gesetz; die Bestimmung bezeichnet für sich genommen nicht ausreichend präzise, also nicht für jedermann vorhersehbar (vgl. EGMR 16.2.2000 Fall Amann, ÖJZ 2001/1, zu Art 8 EMRK), unter welchen Voraussetzungen Auskünfte über geschützte Daten für die Wahrnehmung konkreter Verwaltungsaufgaben erforderlich sind. Der angefochtene Bescheid, der sich ausdrücklich auf § 83 Abs2 und 3 TKG beruft und in seiner Begründung über eine kursorische Darlegung der "Notwendigkeit der Daten - Einzelne Datenarten" hinaus auch allen Konzessionsinhabern umfassende Detaildaten nach einheitlichen Begriffsbestimmungen zwecks "Ermittlung ... statistischer Kenngrößen" abverlangt, verletzt damit schon wegen des Fehlens der im Sinne des §1 Abs2 DSG 2000 erforderlichen gesetzlichen Grundlage das Grundrecht auf Datenschutz."

V.4.6 Anforderungen an die gesetzlichen Grundlagen

V.4.6.1 Eingriffe in den Schutzbereich des Art 8 EMRK bedürfen einer Rechtfertigung.

Gemäß Art. 8 Abs. 2 EMRK ist zunächst eine gesetzliche Grundlage für Eingriffe erforderlich. Nach dem Urteil des EGMR im Fall *Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien* vom 28.6.2007 (siehe insbesondere § 71 mit Hinweisen auf *Malone gg. das Vereinigte Königreich*, *Kruslin gg. Frankreich*, § 27; *Huvig gg. Frankreich*, § 26; *Kopp gg. die Schweiz*, § 55, und *Amann gg. die Schweiz*, § 50) verlangt der Ausdruck „gesetzlich vorgesehen", wie er in Art. 8 Abs. 2 EMRK verwendet wird, nicht nur, dass die angefochtene Maßnahme eine Grundlage im innerstaatlichen Recht hat. Er bezieht sich darüber hinaus auch auf die Qualität dieses Gesetzes und verlangt, dass es für die betroffenen Personen zugänglich sein muss und diese im Einklang mit dem Rechtsstaatsprinzip auch in der Lage sind, die Konsequenzen vorherzusehen.

V.4.6.2 Aus dem Erfordernis einer gesetzlichen Grundlage in Verbindung mit dem in der Präambel der EMRK verankerten Rechtsstaatsprinzip leitet der EGMR zudem ab, dass das eingreifende innerstaatliche Recht hinreichend bestimmt und für den Bürger zugänglich sein muss (EGMR, *Lambert gg. Frankreich*, 24.08.1998). Dem Einzelnen müsse es möglich sein, sein Verhalten den Vorschriften entsprechend einzurichten, was ein – gemessen an der Schwere des Eingriffs – hinreichendes Maß an Vorhersehbarkeit voraussetze.

Räumt das nationale Recht der Exekutive oder dem zuständigen Richter bei der Durchführung bzw Anordnung von Maßnahmen Ermessen ein, dann verlangt das Bestimmtheitserfordernis – auch und gerade bei geheimen Maßnahmen –, dass der zulässige Zweck der Maßnahme, die Reichweite und Grenzen des Ermessens sowie die Kriterien, nach denen es auszuüben ist, hinreichend erkennbar sind, insbesondere, dass vorhersehbar ist, unter welchen Umständen Eingriffe zulässig sind (EGMR, *Malone gg. Großbritannien*, 27.06. 1984; EGMR, *Kopp gg. die Schweiz*, 25.03. 1998).

Die **Anforderungen an die Vorhersehbarkeit im Einzelnen** hängen von der **Eingriffstiefe** der jeweiligen Maßnahme ab, sodass schwerwiegende Eingriffe eine besonders präzise gesetzliche Regelung erforderlich machen. Für den Fall einer Informationssammlung und -speicherung durch einen Geheimdienst wurde etwa entschieden, dass das nationale Recht detailliert festlegen muss, welche Arten von Informationen gespeichert werden dürfen, gegenüber welchen Personengruppen Überwachungsmaßnahmen ergriffen werden dürfen, unter welchen Umständen Informationen gesammelt werden dürfen, welches Verfahren dabei einzuhalten ist, nach welcher Zeitdauer erlangte Informationen zu löschen sind, welche Personen auf den Datenbestand zugreifen dürfen, die Art und Weise der Speicherung, das Verfahren des Informationsabrufs sowie die zulässigen Verwendungszwecke für die abgerufenen Informationen (EGMR, *Rotaru gg. Rumänien*, 29.03.2000).

Zum Schutz vor Missbrauch durch Telefonüberwachung ohne Wissen des Betroffenen hat der EGMR die detaillierte Festlegung der folgenden Umstände durch das nationale Recht gefordert:

Gegen welche Personen und bei welchen Straftaten das Instrument der Telefonüberwachung eingesetzt werden darf, die maximale Dauer der Überwachungsmaßnahme, das Verfahren, in welchem Abhörprotokolle erstellt werden, die Sicherungsmaßnahmen dafür, dass die Originalbänder intakt und in ihrer Gesamtheit erhalten bleiben, damit sie vom Richter und dem Verteidiger des Beschuldigten untersucht werden können, sowie Fristen für die Löschung der erlangten Informationen (EGMR, *Kruslin gg. Frankreich*, 27.03.1990). Für den Fall, dass unbeteiligte Dritte von einer Überwachungsmaßnahme betroffen sind (zB als Gesprächspartner eines Verdächtigen), müssen Sicherungsvorkehrungen in Bezug auf deren Daten vorgesehen werden (EGMR, *Amann gg. die Schweiz*, 12.01.2000).

V.4.6.3 Auch wenn Strafverfolgungsorgane um die Herausgabe von Daten „bitten", ohne das Telekommunikationsunternehmen dazu zu verpflichtet sind, ist erforderlich, dass die freiwillige Übermittlung der angeforderten Daten nach innerstaatlichem Recht rechtmäßig und die Befugnis der Strafverfolgungsorgane zur Anforderung solcher Daten detailliert geregelt ist (EGMR, *Malone gg. Großbritannien,* 27.06. 1984). In jedem Fall muss der Staat angemessene Maßnahmen ergreifen, um zu verhindern, dass Dritte unbefugt Kenntnis von überwachten Telekommunikationsinhalten erlangen (EGMR, *Craxi gg. Italien*, 26.06.2003).

V.4.6.4 Vor allem in Bezug auf § 99 Abs 5 Z 3 und 4 TKG iVm § 53 Abs 3a und 3b SPG ist der Rechtsschutz äußerst mangelhaft, weil die Auskünfte keine Einschränkungen auf den Schutz höherrangiger Rechtsgüter (zB Leben, Gesundheit oder Freiheit eines Menschen) vorsehen sondern Auskünfte allgemein zur Abwehr gefährlicher Angriffe (§ 16 SPG) zulassen. Ebensowenig vorgesehen ist eine vorherige Genehmigung im Sinne eines 4-Augen-Prinzips, eine unabhängige richterliche Kontrolle ist dem SPG insgesamt fremd.

Ebenso ist für Datenauskünfte gemäß § 99 Abs 5 Z 2 TKG iVm § 76a Abs 2 StPO kein Richtervorbehalt vorgesehen, und auch hier gibt es keine Einschränkung auf „schwere Straftaten" mit einem bestimmten Mindestmaß an Strafdrohung.

Trotz Richtervorbehalt ist aber auch die Grundregel zur Verwendung von Vorratsdaten in § 102b TKG iVm § 135 Abs 2a StPO zu weit gehend, weil die Delikte, für deren Aufklärung eine Auskunft zulässig ist, lediglich eine Höchststrafdrohung von mehr als einem Jahr Freiheitsstrafe beinhalten müssen. Eine Durchsicht des StGB zeigt, dass hier Delikte erfasst sind, die doch weit entfernt von der ursprünglichen Rechtfertigung der VDS – Bekämpfung von organisierter Kriminalität und Terrorismus – erscheinen, beispielsweise § 123 StGB (Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses, Strafdrohung bis 2 Jahre Freiheitsstrafe).

V.4.7 Praxis der VDS und Schlussfolgerungen in Bezug auf die angefochtenen Normen

V.4.7.1 <u>Bezüglich IP-Adressen</u>: Hier sehen die Regelungen überhaupt keine Einschränkung vor, Ermittlung bzw. Gefahrenabwehr bezüglich **<u>jeder</u>** gerichtlich strafbaren Handlung, es sind keine Einschränkungen vorgesehen auf überragende Rechtsgüter, zB Leben, Gesundheit, Freiheit (§ 99 Abs. 5 Z 2 und 4 iVm § 76a Abs. 2; § 53 Abs. 3a SPG).

Ermittlungsrelevante IP-Adressen „fallen nicht vom Himmel", sondern man kommt an sie nur (außer: Verschlüsselung) heran, **wenn man vorher den Inhalt einer Kommunikation (= aufgerufener Dienst, besuchte Website, etc) kennt** und von dort die IP-Adresse eines Nutzers erfährt.

Sie können daher nicht einfach als „harmlose Zugangsdaten" angesehen werden, da mit ihnen immer ein Zusammenhang zwischen Inhalt und Person hergestellt wird. Die Auskunft über Zugangsdaten ist immer erst ein weiterer Ermittlungsschritt, bei dem eine inhaltlich bestimmte Kommunikation auf einen bestimmten Teilnehmer zurückgeführt werden soll.

Problematisch ist auch, dass die IP-Adressen sich oft **lange nicht ändern** (statische sowieso nicht, aber auch dynamische): Die Polizei kann also eine **„Registratur"** für die Zukunft aufbauen, da es **keine klare Bestimmungen gibt, die Daten nachher zu löschen**, solange nicht völlig eindeutig ist, dass die Daten für die Strafverfolgung oder Gefahrenabwehr unbrauchbar sind (dies wird aber sehr selten zu argumentieren sein, vor allem im Zusammenhang mit Ermittlungen im Umfeld von organisierter Kriminalität.)

Hierzu kann vergleichend die **Rechtslage in Deutschland** herangezogen werden. Das BVerfG hat in seinem Grundsatzurteil zur Vorratsdatenspeicherung festgestellt, dass diese auf besonders schwere Straftaten zu beschränken ist. Diese sind in Deutschland in § 100a Abs. 2 StPO aufgezählt. Zwar ist es dem Gesetzgeber **möglich, auch weitere Straftaten in den Katalog** des § 100a Abs. 2 StPO aufzunehmen, was in manchen Fälle sicher auch gerechtfertigt ist (das BVerfG geht z.B. auf das sog. „Cyber-Stalking", das - noch - nicht umfasst ist, ein).

Dazu stellt der 4. Senat des BVerfG folgendes fest:

*„Es erscheint zwar vorstellbar, dass der Gesetzgeber einzelne dieser Tatbestände in den vom Senat geforderten Katalog schwerer Straftaten aufnimmt. Dabei wird er allerdings an die **Grenzen einer dem Schuldprinzip verpflichteten angemessenen Strafdrohung** stoßen, die dies zu*

rechtfertigen vermag. Delikte, die etwa nicht gewerbsmäßig begangen werden oder keinen besonders hohen Schaden im Einzelfall auslösen, werden so kaum in einen solchen Katalog aufgenommen werden dürfen, wie er dem Senat vorschwebt." (BVerfG, Urt. v. 02.03.2010, Az. 1 BvR 256/08, Rn. 332).

Schwere Straftaten werden von der EU-Richtlinie nicht vorgegeben.

V.4.7.2 <u>Bezüglich Standortdaten</u> nach § 53 Abs. 3b SPG: es besteht kein effektiver Rechtsschutz, keine Sicherstellung, dass das Abfragen tatsächlich auf den von § 53 Abs. 3b SPG beschriebenen Zweck beschränkt bleibt (andere mögliche Zwecke: Abwehr einer Gefahr vom Inhaber der lokalisierten Endeinrichtung, zB Tourengeher, Lawinenopfer).

Nur die Information durch den Anbieter selbst wäre ein effektiver Schutzmechanismus (Ermittlungszweck kann bei Hilfeleistung kaum gefährdet werden; Argumentation zum **Sonderfall der Entführung** – Zeitverzögerung reicht dort bereits aus bzw. „offensichtlich ohnehin bekannt, das abgefragt wurde")

Ebenso wiegt das BVerfG im **Bereich der Gefahrenabwehr** ab. Auch im sicherheitsrechtlichen Bereich hat der Gesetzgeber die Vorratsdatenspeicherung klar zu beschränken (BVerfG, Urt. v. 02.03.2010, Az. 1 BvR 256/08, Rn. 334).

V.4.7.3 <u>Bezüglich E-Mail Adressen</u> (ev. auch Telefon) wäre eine Benachrichtigung der Betroffenen problemlos (E-Mail senden!) möglich.

V.4.8 Die Praxis der VDS und die Verletzung materieller Grundrechte

V.4.8.1 Verletzung des Rechts auf Datenschutz gemäß **§ 1 DSG 2000** durch die angefochtenen Bestimmungen.

Mittels elektronischer Datenverarbeitung sind Einzelangaben über persönliche oder sachliche Verhältnisse einer Person unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar. Sie können darüber hinaus **mit anderen Datensammlungen zusammengefügt** werden, wodurch vielfältige Nutzungs- und Verknüpfungsmöglichkeiten entstehen. **Dadurch können weitere Informationen erzeugt und Schlüsse gezogen werden, die sowohl die grundrechtlich geschützten Geheimhaltungsinteressen des Betroffenen beeinträchtigen als auch anschließende Eingriffe in seine Privatsphäre nach sich ziehen können.**

Eine weitere Besonderheit des Eingriffspotentials von Maßnahmen der elektronischen Datenverarbeitung liegt in der **Menge** der potentiell verarbeitbaren Daten, die auf konventionellem Wege nicht bewältigt werden könnten. Der mit solchen technischen Möglichkeiten einhergehenden **gesteigerten Gefährdungslage** entspricht der Steigerung des Bedürfnisses nach einem hierauf bezogenen, verbesserten Grundrechtsschutz.

V.4.8.2 Mit in den Blick zu nehmen ist zum anderen auch die Persönlichkeitsrelevanz **der Informationen, die durch eine weitergehende Verarbeitung und Verknüpfung der erfassten Informationen gewonnen werden sollen** oder auch nur können. Ferner ist bedeutsam, ob der Betroffene, etwa durch eine Rechtsverletzung, einen ihm zurechenbaren **Anlass** für eine Datenerhebung geschaffen hat oder ob die Erhebung **anlasslos** erfolgt und damit praktisch auch jeden anderen hätte treffen können. Informationserhebungen gegenüber Personen, die den Eingriff durch ihr Verhalten nicht veranlasst haben, sind grundsätzlich **von höherer Eingriffsintensität als anlassbezogene**.

Werden Personen, die keinen Erhebungsanlass gegeben haben, in großer Zahl in den Wirkungsbereich einer Maßnahme einbezogen, können von ihr auch allgemeine **Einschüchterungseffekte** ausgehen, die zu Beeinträchtigungen bei der Ausübung von Grundrechten führen können (Vgl BVerfGE 65, 1 (42); 113, 29 (46)).

Dies trifft exakt zu auf das *„diffuse Gefühl ständiger Überwachung der heutigen Situation"*.

Die Unbefangenheit des Verhaltens wird insbesondere gefährdet, wenn die Streubreite von Ermittlungsmaßnahmen dazu beiträgt, dass **Risiken des Missbrauchs** und ein **Gefühl des Überwachtwerdens** entstehen.

V.4.8.3 Aus der Judikatur des EGMR ergibt sich explizit, dass auch „äußere Gesprächsdaten", also gewählte Nummer, Zeitpunkt und Dauer, vom Schutzbereich des Art 8 Abs 1 EMRK umfasst sind und ein Eingriff in dieses Grundrecht insbesondere auch dann vorliegt, wenn solche Daten **ohne Zustimmung des Betroffenen** an staatliche Behörden übermittelt werden (EGMR, *Malone gg. Großbritannien,* 27.06. 1984. Abs. 83f.) Der EGMR selbst hat im Zusammenhang mit ähnlich gelagerten Fällen bereits mehrfach ausgesprochen, dass schon das bloße Bestehen eines Gesetzes, das eine geheime Überwachung der Telekommunikation erlaubt, für alle Personen, auf die es Anwendung findet, die Gefahr der Überwachung mit sich bringt. Diese Gefahr greife notwendigerweise in die Freiheit der Kommunikation zwischen Benützern von Telekommunikationseinrichtungen ein und stelle daher unabhängig von irgendwelchen tatsächlich gegen sie ergriffenen Maßnahmen einen Eingriff in die durch Art 8 EMRK geschützten Rechte dar (EGMR, *Weber und Saravia gg. Deutschland*, App. Nr. 54934/00, Abs 78 mit Hinweisen auf frühere Rechtsprechung in Klass, Malone).

V.4.9 Eingriffe in den Schutzbereich

Im Urteil *Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien* entschied der EGMR im Hinblick auf Entscheidungen in anderen Fällen (siehe *Klass u.a. gg. Deutschland,* § 41; *Malone gg. das Vereinigte Königreich*, § 64; *Weber und Saravia gg. Deutschland*, §§ 77-79), dass das Bestehen von Rechtsvorschriften, die eine geheime Überwachung erlauben, selbst einen Eingriff in das Recht nach Art 8 EMRK darstellt.

Im Urteil *Copland gg. das Vereinigte Königreich* entschied der Gerichtshof überdies, dass die Erhebung von Verbindungsdaten ohne Einwilligung des Betroffenen einen Eingriff in dessen

Rechte auf Achtung des Privatlebens und des Briefverkehrs darstellt. Dies gilt neben Telefonaten auch für die Erhebung von näheren Umständen der E-Mail-Nutzung und der Internetnutzung (EGMR Urteil *Copland gg. das Vereinigte Königreich).* Sowohl in der Erhebung wie auch in der Speicherung dieser Daten liegt ein Grundrechtseingriff, selbst wenn die Daten auf legalem Wege erlangt werden. (EGMR Urteil *Rotaru gg. Rumänien).*

Es lässt sich also festhalten, dass jede staatliche Verwendung (Erhebung, Speicherung, Verarbeitung und Weitergabe) von personenbezogenen Informationen einen Eingriff in Art. 8 EMRK darstellt. Der EGMR entschied ebenso bereits wiederholt, dass auch Telefongespräche als „Briefverkehr/Korrespondenz" iSd Art. 8 EMRK anzusehen sind (EGMR Urteil *Niemietz gg. Deutschland).* Art. 8 EMRK schützt dabei sowohl geschäftliche als auch private Kommunikation (EGMR Urteil *Leander gg. Schweden,* 25.02.1987*)* . Eine Subsumtion unter den Begriff des „Privatlebens" fällt insofern leichter, als der Gerichtshof unter Bezugnahme auf die Europäische Datenschutzkonvention (EGMR Urteil *Silver gg. Großbritannien*, 25.02.1983) allgemein anerkennt, dass die Sammlung und Speicherung personenbezogener Daten einen Eingriff in das Privatleben des Einzelnen darstellt (EGMR Urteil *Leander gg. Schweden,* 25.02.1987), ebenso wie die Verwendung solcher Daten und die Verweigerung ihrer Löschung.

Dass sich der Staat zur Speicherung solcher Daten privater Unternehmen bedient, kann keinen Unterschied machen, wenn er sich gleichzeitig selbst Zugriff auf die gespeicherten Daten eröffnet. Andernfalls könnte der Staat seine Grundrechtsbindung durch ein bloßes „Outsourcing" von Maßnahmen umgehen. Die Inanspruchnahme Privater erhöht das Gewicht des Eingriffs sogar noch, da sich der Kreis von – weitgehend ohne Schuld – beeinträchtigten Personen durch den zusätzlichen Eingriff entsprechend vergrößert. Zudem ist das Risiko, dass gespeicherte Daten missbraucht werden, durch eine Vielzahl von Daten erfassende Privatunternehmen erheblich höher einzuschätzen als im Fall einer Speicherung durch staatliche Stellen.

In einer demokratischen Gesellschaft ist eine Maßnahme nur erforderlich, wenn ein in Anbetracht des Stellenwerts des garantierten Freiheitsrechts hinreichend dringendes soziales Bedürfnis nach ihr besteht, sie einen legitimen Zweck verfolgt und ihre Belastungsintensität nicht außer Verhältnis zu dem Gewicht des Zwecks steht (EGMR Urteil *Silver gg. Großbritannien,* 25.02.1983). Der EGMR hat dazu eindeutig erklärt, dass das Interesse des Staates gegenüber den Interessen des Einzelnen an der Achtung seiner Privatsphäre abgewogen werden müsse (EGMR Urteil *Leander gg. Schweden,* 25.02.1987). Eingriffe sind zwar nicht auf das unerlässliche Maß beschränkt, aber ein bloßes Nützlichsein oder Wünschenswertsein genügt nicht (EGMR Urteil, *Silver gg. Großbritannien,* 25.02.1983). Sind die genannten Kriterien erfüllt, dann liegt keine Verletzung von Art 8 EMRK vor.

In Bezug auf die Vorratsdatenspeicherung von Telekommunikationsdaten ist nach Ansicht der Antragsteller/innen die Rechtssprechung des EGMR so zu interpretieren, dass jede Form einer groß angelegten, allgemeinen oder sondierenden elektronischen Überwachung unzulässig ist, insbesondere, wenn nicht wegen einer bestimmten Tat oder Gefahr ermittelt wird, sondern nach möglichen Taten oder Gefährdungen gesucht werden soll.

V.4.10 Unverhältnismäßigkeit

Eine Beschränkung von Grundrechten ist nur insoweit zulässig, als sie zur Erreichung des angestrebten Zweckes geeignet und erforderlich ist, und der mit ihr verbundene Eingriff seiner Intensität nach nicht außer Verhältnis zur Bedeutung der Sache und den von den Betroffenen hinzunehmenden Einbußen steht. Einbußen an grundrechtlich geschützter Freiheit dürfen nicht in unangemessenem Verhältnis zu den Zwecken stehen, denen die Grundrechtsbeschränkung dient.

Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person führen zwar dazu, dass der Einzelne Einschränkungen seiner Grundrechte hinzunehmen hat, wenn überwiegende Allgemeininteressen dies rechtfertigen. Der Gesetzgeber muss aber zwischen Allgemein- und Individualinteressen einen angemessenen Ausgleich herstellen. Dabei spielt auf grundrechtlicher Seite eine Rolle, unter welchen Voraussetzungen welche und wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind. Maßgebend sind also insbesondere die Gestaltung der Einschreitschwellen, die Zahl der Betroffenen und die Intensität der Beeinträchtigungen.

Im **Bereich der Telekommunikationsüberwachung** ist von Bedeutung, ob die Betroffenen als Personen anonym bleiben, welche Informationen erfasst werden können und welche Nachteile den Grundrechtsträgern aufgrund der Überwachungsmaßnahme drohen. Auf Seiten der mit dem Eingriff verfolgten Zwecke ist das Gewicht der Ziele maßgeblich, denen die Telekommunikationsüberwachung dient. Es hängt unter anderem davon ab, wie bedeutsam die Rechtsgüter sind, die mit Hilfe der Maßnahme geschützt werden sollen und wie wahrscheinlich der Eintritt einer Rechtsgutverletzung ist [vgl BVerfGE 100, 313 (375f.)].

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 genügt den Anforderungen der Verhältnismäßigkeit im engeren Sinne nicht.

Die Standortkennung eingeschalteter Mobilfunkendeinrichtungen kann zur Erstellung eines Bewegungsbildes führen, über das gegebenenfalls auf Gewohnheiten der betroffenen Personen oder auf Abweichungen hiervon geschlossen werden kann. Schließlich ist zu bedenken, dass die Zuordnung von Verbindungs- und Bestanddaten, insbesondere von IP-Adressen, zu einer bestimmten Person selbst keine Rückschlüsse darüber zulässt, ob diese Person auch am interessierenden Kommunikationsvorgang beteiligt war. Hierzu bedarf es weiterer konkretisierender Indizien, welche gerade bei der Erforschung von Kommunikationsvorgängen im Internet häufig nur schwer fassbar sind.

Anschaulich lässt sich eine IP-Adresse als eine Art KFZ-Kennzeichen auf dem „Datenhighway" beschreiben. Vielfach wird daher eine Art „IT-Lenkererhebung" erforderlich sein, um Aussagekraft und Zuverlässigkeit der ermittelten Daten beurteilen zu können; denn eine reine Gefährdungshaftung für Inhaber von Internet- oder Telefonanschlüssen ist der österreichischen Rechtsordnung bislang nicht bekannt. Der Aussagekraft und mit ihr verbunden dem tatsächlich Nutzen der Daten für den angestrebten Zweck kommen für die Verhältnismäßigkeit der

behördlichen Befugnisse entscheidende Bedeutung zu, die bereits abstrakt in jeden Abwägungsvorgang mit einzubeziehen sind. Grundrechtlich bedeutsam ist ferner die große Streubreite der möglichen Eingriffe. Die Erhebung von Verbindungsdaten kann eine große Zahl von Personen treffen. Erfasst werden nicht nur potenzielle Straftäter, sondern auch sämtliche Personen, mit denen diese im betreffenden Zeitraum Telekommunikationsverbindungen nutzen. Dazu können etwa auch Personen gehören, die in keiner Beziehung zu einer möglicherweise zu verhütenden oder später zu verfolgenden Straftat stehen, wie etwa Kontakt- und Begleitpersonen oder gänzlich unbeteiligte Dritte.

Eingriffe dieser Art bergen darüber hinaus auch deshalb hohe Risiken für die Rechte der Betroffenen in sich. Gegen die angesprochenen Maßnahmen können Betroffene frühestens dann mit rechtlichen Mitteln vorgehen, wenn die Maßnahmen bereits vollzogen sind und sie über die Tatsache, dass solche Maßnahmen getroffen wurden, informiert wurden oder davon auf andere Weise Kenntnis erlangen konnten. Bei Maßnahmen der Vorfeldermittlung ist aufgrund der Ungewissheit, ob und wann Straftaten begangen werden, regelmäßig mit einer längeren Zeitdauer bis zu einer (allfälligen) Unterrichtung zu rechnen als bei sonstigen Überwachungsmaßnahmen.

Die Eingriffsschwere wird durch die Möglichkeit der Behörden, die erhobenen Daten - wie in § 53 Abs. 2 SPG vorgesehen - allgemein zu Zwecken der Gefahrenabwehr und zu weiteren Zwecken nach Abs 1 leg cit zu speichern, zu verändern oder zu nutzen, noch weiter verstärkt.

Die Verwertung in anderen Zusammenhängen ist ein eigenständiger Eingriff. Die Datenerhebung im Vorfeld der Begehung von Straftaten kann aufgrund der fehlenden Begrenzung auf eine konkret in Verwirklichung begriffene oder schon begangene Straftat vielfältig nutzbare Informationen ergeben. Die Bindung an den Zweck, den das zur Kenntnisnahme der Daten ermächtigende Gesetz festgelegt hat, wird bei der weiteren Verwertung der erlangten Informationen praktisch kaum haltbar sein. Die Möglichkeit der Verwendung der erhobenen Daten zu unbestimmten oder noch nicht bestimmbaren Zwecken erhöht damit die Schwere des Eingriffs schon in der Phase der Erhebung.

Das Urteil EGMR *S. und Marper vs UK* ist im vorliegenden Zusammenhang von besonderem Gewicht, weil selbst die Speicherung personenbezogener Daten von Personen, die einmal im Verdacht standen, eine strafbare Handlung begangen zu haben, vom EGMR als Verletzung des Art. 8 EMRK betrachtet wird. Umso mehr wirft die völlig verdachtsunabhängige Speicherung von Vorratsdaten die Frage nach einer Verletzung dieses Konventionsrechts auf.

Die durch die anfechtungsgegenständlichen Normen vorgesehenen Eingriffe in die geltend gemachten Grundrechte sind daher im engeren Sinne nicht verhältnismäßig.

VI. ANTRÄGE:

Die Antragsteller beantragen daher die Aufhebung folgender gesetzlicher Bestimmungen wegen Verletzung verfassungsgesetzlich gewährleisteter Rechte:

Den Antragsgegenstand bilden § 102 a TKG 2003 (Telekommunikationsgesetz 2003, Stammfassung BGBl. I Nr. 70/2003 in der Fassung von BGBl. I Nr. 102/2011) **und andere Bestimmungen des TKG 2003** (Telekommunikationsgesetz 2003, Stammfassung BGBl. I Nr. 70/2003 in der Fassung von BGBl. I Nr. 102/2011), **der StPO** (Strafprozessordnung 1975, Stammfassung BGBl. Nr. 631/1975 in der Fassung von BGBl. I Nr. 53/2012) **und des SPG** (Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei, Stammfassung BGBl. Nr. 566/1991 in der Fassung von BGBl. I Nr. 13/2012).

Der Hauptantrag geht davon aus, dass das gesamte Konzept der Vorratsdatenspeicherung verfassungs- / EMRK- /GRC- widrig ist.

Die Eventualanträge gelten insbesondere für den Fall, dass der VfGH den Antragsteller/innen nicht in ihrer Argumentation, dass die Vorratsdatenspeicherung an sich verfassungswidrig ist, folgt, sondern nur die konkrete österreichische Umsetzung für unverhältnismäßig hält.

Dies vorausgeschickt stellen die Antragsteller/innen nachstehende

ANTRÄGE:

VI.1 Der VfGH möge

- § 102a TKG 2003 **zur Gänze,**

weiters, wegen untrennbaren Zusammenhanges mit § 102a TKG 2003

- § 102b TKG 2003 **zur Gänze,**
- § 102c TKG 2003 **zur Gänze,**
- 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" (...) „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 TKG 2003 **zur Gänze**
- 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 2 TKG 2003 die Wortfolgen ***„einschließlich der Übermittlung von Vorratsdaten,"*** und ***„sowie die näheren Bestimmungen betreffend die Speicherung der gemäß § 102 c angefertigten Protokolle"***
- in § 98 Abs 2 TKG 2003 die Wortfolge ***„, auch wenn hierfür ein Zugriff auf gemäß § 102 a Ab.s 3 Z 6 lit. D gespeicherte Vorratsdaten erforderlich ist"***,
- in § 109 Abs. 3 TKG 2003 dessen Z 22 **zur Gänze**
- in § 109 Abs. 3 TKG 2003 dessen Z 23 **zur Gänze**
- in § 109 Abs. 3 TKG 2003 dessen Z 24 **zur Gänze**
- in § 109 Abs. 3 TKG 2003 dessen Z 25 **zur Gänze**
- in § 109 Abs. 3 TKG 2003 dessen Z 26 **zur Gänze**

weiters

- § 135 Abs 2a StPO **zur Gänze**
- In § 134 StPO die Z 2a **zur Gänze**

schließlich

- in § 53 Abs 3a Z 3 SPG 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 SPG die Wortfolge ***„„auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 iVm § 102a TKG 2003 erforderlich ist,"***

wegen Verletzung des Rechts auf Privatleben und Familienleben, Schutz der Korrespondenz gemäß **Art. 8 EMRK/Art. 7 GRC**, des Rechts auf Datenschutz gemäß **§ 1 DSG 2000/Art. 8 GRC,** des Rechts auf Meinungs- und Informationsfreiheit gemäß **Art. 10 EMRK/Art. 11 GRC,** des Rechts auf Versammlungs- und Vereinigungsfreiheit gemäß **Art. 11 EMRK/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/Art. 48 GRC**

im jeweils beantragten Umfang aufheben.

VI.2. In eventu möge der VfGH

- 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" (...) „als Vorratsdaten gemäß § 102a Abs. 2 Z 1 oder § 102a Abs. 4 Z 1, 2,3 und 5",***

weiters

- in § 53 Abs 3a Z 3 SPG 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 SPG die Wortfolge ***„„auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 iVm § 102a TKG 2003 erforderlich ist,",***

weiters

- § 135 Abs 2a StPO **zur Gänze,**
- in § 134 StPO die Z 2a **zur Gänze,**

wegen Verletzung, des Rechts auf Privatleben und Familienleben, Schutz der Korrespondenz gemäß **Art. 8 EMRK/Art 7 GRC**, des Rechts auf Datenschutz gemäß **§ 1 DSG 2000/Art. 8 GRC**, des Rechts auf Meinungs- und Informationsfreiheit gemäß **Art. 10 EMRK/Art. 11 GRC,** des Rechts auf Versammlungs- und Vereinigungsfreiheit gemäß **Art. 11 EMRK/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/Art. 48 GRC**

im jeweils beantragten Umfang aufheben.

VI.3. In eventu möge der VfGH

- 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" (...) „als Vorratsdaten gemäß § 102a Abs. 2 Z 1 oder § 102a Abs. 4 Z 1, 2,3 und 5",***

weiters

- in § 53 Abs 3a Z 3 SPG 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 SPG die Wortfolge ***„„auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 iVm § 102a TKG 2003 erforderlich ist,".***

wegen Verletzung, des Rechts auf Privatleben und Familienleben, Schutz der Korrespondenz gemäß **Art. 8 EMRK/Art. 7 GRC**, des Rechts auf Datenschutz gemäß **§ 1 DSG 2000/Art. 8 GRC**, des Rechts auf Meinungs- und Informationsfreiheit gemäß **Art. 10 EMRK/Art. 11 GRC,** des Rechts auf Versammlungs- und Vereinigungsfreiheit gemäß **Art. 11 EMRK/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/Art. 48 GRC**

im jeweils beantragten Umfang aufheben.

VI.4. In eventu möge der VfGH

- 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" (...) „als Vorratsdaten gemäß § 102a Abs. 2 Z 1 oder § 102a Abs. 4 Z 1, 2,3 und 5",***

weiters

- § 135 Abs 2a StPO **zur Gänze,**
- in § 134 StPO die Z 2a **zur Gänze,**

wegen Verletzung, des Rechts auf Privatleben und Familienleben, Schutz der Korrespondenz gemäß **Art. 8 EMRK/Art. 7 GRC**, des Rechts auf Datenschutz gemäß **§ 1 DSG 2000/Art. 8 GRC**, des Rechts auf Meinungs- und Informationsfreiheit gemäß **Art. 10 EMRK/Art. 11 GRC,** des Rechts auf Versammlungs- und Vereinigungsfreiheit gemäß **Art. 11 EMRK / 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 / Art. 48 GRC**

im jeweils beantragten Umfang aufheben.

VI.5. In eventu möge der VfGH

- 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" (...) „als Vorratsdaten gemäß § 102a Abs. 2 Z 1 oder § 102a Abs. 4 Z 1, 2,3 und 5",***

wegen Verletzung, des Rechts auf Privatleben und Familienleben, Schutz der Korrespondenz gemäß **Art. 8 EMRK/Art. 7 GRC**, des Rechts auf Datenschutz gemäß **§ 1 DSG 2000/Art. 8 GRC**, des Rechts auf Meinungs- und Informationsfreiheit gemäß **Art. 10 EMRK/Art. 11 GRC,** des Rechts auf Versammlungs- und Vereinigungsfreiheit

gemäß **Art. 11 EMRK/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/Art 48 GRC**

im jeweils beantragten Umfang aufheben.

VI.6. In eventu möge der VfGH

- in § 53 Abs 3a Z 3 SPG 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 SPG die Wortfolge ***„„auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 iVm § 102a TKG 2003 erforderlich ist,".***

weiters

- § 135 Abs 2a StPO **zur Gänze,**
- in § 134 StPO die Z 2a **zur Gänze,**

schließlich

- in § 76a Abs 2 StPO die Z 2 **zur Gänze,**
- in § 76a Abs 2 StPO die Z 4 **zur Gänze,**

wegen Verletzung des Rechts auf Privatleben und Familienleben, Schutz der Korrespondenz gemäß **Art. 8 EMRK/Art. 7 GRC**, des Rechts auf Datenschutz gemäß **§ 1 DSG 2000/Art. 8 GRC**, des Rechts auf Meinungs- und Informationsfreiheit gemäß **Art. 10 EMRK/Art. 11 GRC,** des Rechts auf Versammlungs- und Vereinigungsfreiheit gemäß **Art. 11 EMRK/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 / Art. 48 GRC**

im jeweils beantragten Umfang aufheben.

VI.7. In eventu möge der VfGH

- in § 53 Abs 3a Z 3 SPG 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 SPG die Wortfolge ***„„auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 iVm § 102a TKG 2003 erforderlich ist,".***

weiters

- § 135 Abs 2a StPO **zur Gänze,**
- in § 134 StPO die Z 2a **zur Gänze,**

wegen Verletzung, des Rechts auf Privatleben und Familienleben, Schutz der Korrespondenz gemäß **Art. 8 EMRK/Art 7 GRC**, des Rechts auf Datenschutz gemäß **§ 1 DSG 2000/Art. 8 GRC**, des Rechts auf Meinungs- und Informationsfreiheit gemäß **Art. 10 EMRK/Art. 11 GRC,** des Rechts auf Versammlungs- und Vereinigungsfreiheit gemäß **Art. 11 EMRK/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/Art. 48 GRC**

im jeweils beantragten Umfang aufheben.

VI.8. In eventu möge der VfGH

- in § 53 Abs 3a Z 3 SPG 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 SPG die Wortfolge ***„„auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 iVm § 102a TKG 2003 erforderlich ist,".***

wegen Verletzung, des Rechts auf Privatleben und Familienleben, Schutz der Korrespondenz gemäß **Art. 8 EMRK/Art. 7 GRC**, des Rechts auf Datenschutz gemäß **§ 1 DSG 2000/Art 8 GRC**, des Rechts auf Meinungs- und Informationsfreiheit gemäß **Art. 10 EMRK/Art. 11 GRC,** des Rechts auf Versammlungs- und Vereinigungsfreiheit gemäß **Art. 11 EMRK/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/Art. 48 GRC**

im jeweils beantragten Umfang aufheben.

VI.9. In eventu möge der VfGH

- § 135 Abs 2a StPO **zur Gänze,**
- in § 134 StPO die Z 2a **zur Gänze,**

wegen Verletzung, des Rechts auf Privatleben und Familienleben, Schutz der Korrespondenz gemäß **Art. 8 EMRK/Art. 7 GRC**, des Rechts auf Datenschutz gemäß **§ 1 DSG 2000/Art. 8 GRC**, des Rechts auf Meinungs- und Informationsfreiheit gemäß **Art. 10 EMRK/Art.11 GRC,** des Rechts auf Versammlungs- und Vereinigungsfreiheit gemäß **Art. 11 EMRK/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/Art. 48 GRC**

im jeweils beantragten Umfang aufheben.

VI.10. In eventu möge der VfGH

- in § 76a Abs 2 StPO die Z 2 **zur Gänze**,
- in § 76a Abs 2 StPO die Z 4 **zur Gänze**,

wegen Verletzung, des Rechts auf Privatleben und Familienleben, Schutz der Korrespondenz gemäß **Art. 8 EMRK/Art. 7 GRC**, des Rechts auf Datenschutz gemäß **§ 1 DSG 2000/Art. 8 GRC**, des Rechts auf Meinungs- und Informationsfreiheit gemäß **Art. 10 EMRK/Art. 11 GRC,** des Rechts auf Versammlungs- und Vereinigungsfreiheit gemäß **Art. 11 EMRK/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/Art. 48 GRC**

im jeweils beantragten Umfang aufheben.

VI.11. Schließlich wird **angeregt**, der VfGH möge eine **Vorabentscheidung gemäß Artikel 267 AEUV** einholen, wobei dem Gerichtshof der Europäischen Union beispielsweise folgende Fragen vorgelegt werden könnten:

- Ist die Richtlinie 2006/24/EG vereinbar mit dem in Art. 7 GRC und Art. 8 EMRK enthaltenen Recht auf Schutz des Privat- und Familienlebens?
- Ist die Richtlinie 2006/24/EG vereinbar mit dem in Art. 8 GRC garantierten Recht auf Schutz personenbezogener Daten?
- Ist die Richtlinie 2006/24/EG vereinbar mit dem in Art. 11 GRC und Art. 10 EMRK garantierten Recht auf freie Meinungsäußerung?
- Inwieweit fordern die Verträge – speziell der Grundsatz der loyalen Zusammenarbeit des Art. 4 Abs. 3 EUV – die nationalen Gerichte dazu auf, die Vereinbarkeit der nationalen Umsetzungen der Richtlinie 2006/24/EG mit dem von der Grundrechtscharta gewährleisteten Schutz, einschließlich deren Art. 7 (sowie Art. 8 EMRK), zu prüfen und zu beurteilen?

VII. Kosten

Weiters beantragen die Antragsteller den Zuspruch der regelmäßig anfallenden Kosten iSd § 27 VfGG zuzüglich USt.

Wien, am 15. Juni 2012 für die Antragsteller/innen