VERFASSUNGSGERICHTSHOF
G 223/2016-23
29. November 2017

# IM NAMEN DER REPUBLIK!

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

in Anwesenheit der Vizepräsidentin
Dr. Brigitte BIERLEIN

und der Mitglieder
Dr. Markus ACHATZ,
Mag. Dr. Eleonore BERCHTOLD-OSTERMANN,
Dr. Sieglinde GAHLEITNER,
DDr. Christoph GRABENWARTER,
Dr. Christoph HERBST,
Dr. Michael HOLOUBEK,
Dr. Helmut HÖRTENHUBER,
Dr. Claudia KAHR,
Dr. Georg LIENBACHER,
Dr. Rudolf MÜLLER und
Dr. Ingrid SIESS-SCHERZ

sowie des Ersatzmitgliedes
Dr. Angela JULCHER

als Stimmführer, im Beisein der verfassungsrechtlichen Mitarbeiterin
Dr. Laura PAVLIDIS
als Schriftführerin,

über den Antrag der Abgeordneten zum Nationalrat 1. Dr. Peter PILZ, 2. Dr. Walter ROSENKRANZ, 3. Erwin ANGERER, 4. Dr. Dagmar BELAKOWITSCH-JENEWEIN, 5. Dr. Reinhard Eugen BÖSCH, 6. Hermann BRÜCKL, 7. Dipl.-Ing. Gerhard DEIMEK, 8. MMag. DDr. Hubert FUCHS, 9. Ing. Heinz-Peter HACKL, 10. Christian HAFENECKER, MA, 11. Mag. Roman HAIDER, 12. Mag. Gerald HAUSER, 13. Ing. Christian HÖBART, 14. Ing. Norbert HOFER, 15. Dr. Johannes HÜBNER, 16. Harald JANNACH, 17. Dr. Andreas F. KARLSBÖCK, 18. MMMag. Dr. Axel KASSEGGER, 19. Herbert KICKL, 20. Anneliese KITZMÜLLER, 21. Mag. Günther KUMPITSCH, 22. Christian LAUSCH, 23. Dr. Jessi LINTL, 24. Wendelin MÖLZER, 25. Edith MÜHLBERGHUBER, 26. Werner NEUBAUER, 27. Walter RAUCH, 28. Josef A. RIEMER, 29. Barbara ROSENKRANZ, 30. Ing. Thomas SCHELLENBACHER, 31. Carmen SCHIMANEK, 32. Mag. Philipp SCHRANGL, 33. Mag. Harald STEFAN, 34. Petra STEGER, 35. Heinz-Christian STRACHE, 36. Bernhard THEMESSL, 37. Peter WURM, 38. Wolfgang ZANGER, 39. Mag. Aygül Berivan ASLAN, 40. Dieter BROSZ, MSc, 41. Mag. Christiane BRUNNER, 42. Dr. Eva GLAWISCHNIG-PIESCZEK, 43. Mag. Helene JARMER, 44. Matthias KÖCHL, 45. Mag. Werner KOGLER, 46. Mag. Alev KORUN, 47. Dr. Ruperta LICHTENECKER, 48. Sigrid MAURER, 49. Dr. Gabriela MOSER, 50. Dr. Eva MÜCKSTEIN, 51. Karl ÖLLINGER, 52. Dipl.-Ing. Dr. Wolfgang PIRKLHUBER, 53. Mag. Bruno ROSSMANN, 54. Mag. Birgit SCHATZ, 55. Julian SCHMID, BA, 56. Mag. Judith SCHWENTNER, 57. Mag. Albert STEINHAUSER, 58. Dr. Harald WALSER, 59. Georg WILLI, 60. Tanja WINDBÜCHLER-SOUSCHILL sowie 61. Mag. Dr. Wolfgang ZINGGL, alle vertreten durch die SCHEUCHER Rechtsanwalt GmbH, Lindengasse 39, 1070 Wien, auf Aufhebung (von Teilen) des Bundesgesetzes, mit dem das Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz – PStSG), erlassen und das Sicherheitspolizeigesetz geändert werden, BGBl. I 5/2016, sowie von näher bezeichneten Bestimmungen im Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz – PStSG) in seiner heutigen nichtöffentlichen Sitzung gemäß Art. 140 B-VG zu Recht erkannt:

I. Der Antrag wird abgewiesen, soweit er sich gegen § 6 Abs. 1 Z 1 und Z 2, § 10 Abs. 5 sowie § 11 Abs. 1 Z 2, Z 3, Z 5 und Z 7 des Bundesgesetzes über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz – PStSG) BGBl. I Nr. 5/2016, richtet.

II. Im Übrigen wird der Antrag zurückgewiesen.

## Entscheidungsgründe

# I. Antrag

Mit dem vorliegenden, auf Art. 140 Abs. 1 Z 2 B-VG gestützten Antrag beantragen 61 Abgeordnete zum Nationalrat, die im Folgenden näher bezeichneten Bestimmungen, nämlich 1

"1. im Bundesgesetz vom 26.02.2016, BGBl. I Nr. 5/2016, mit dem das Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz — PStSG) erlassen und das Sicherheitspolizeigesetz geändert werden, Artikel 1, zur Gänze;

Artikel 2, Ziffer 10., 13., und 27. zur Gänze; in Ziffer 15., 16., 24. und 30. näher bestimmte Wortfolgen; in eventu zusätzlich in Ziffer 1., 6. und 29. näher bestimmte Wortfolgen;

[…]

in eventu

2. im Bundesgesetz vom 26.02.2016, BGBl. I Nr. 5/2016, mit dem das Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz — PStSG) erlassen und das Sicherheitspolizeigesetz geändert werden, Artikel 1, zur Gänze;

Artikel 2, Ziffer 27. zur Gänze; in eventu zusätzlich in Ziffer 6., 24. und 29. näher bestimmte Wortfolgen;

[…]

in eventu

3. im Bundesgesetz vom 26.02.2016, BGBl. I Nr. 5/2016, mit dem das Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz — PStSG) erlassen und das Sicherheitspolizeigesetz geändert werden, Artikel I, zur Gänze;

Artikel 2, Ziffer 6., 8., 14. und 27. zur Gänze; in Ziffer 1., 24. und 29. näher bestimmte Wortfolgen;

[…]

in eventu

4. im Bundesgesetz vom 26.02.2016, BGBl. I Nr. 5/2016, mit dem das Bundesgesetz über die Organisation. Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz — PStSG) erlassen und das Sicherheitspolizeigesetz geändert werden, Artikel 1 zur Gänze; Artikel 2, in Ziffer 24 näher bestimmte Wortfolgen;

[…]

in eventu

5. das Bundesgesetz vom 26.02.2016, BGBl. I Nr. 5/2016, mit dem das Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz — PStSG) erlassen und das Sicherheitspolizeigesetz geändert werden, zur Gänze;

[…]

in eventu

6. im Bundesgesetzes über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz — PStSG), BGBl. I Nr. 5/2016, nachstehende Bestimmungen:

6.1 § 4 Ziffer 1. zur Gänze;

6.2 § 6 Absatz 1 Ziffer 1 zur Gänze;

sowie wegen untrennbarer Verbundenheit

- § 10 Absatz 1 Ziffer 1;

- in § 11 Absatz 1 erster Satz die Wortfolge 'Zur erweiterten Gefahrenerforschung (56 Abs. 1 Z 1,) und';

- in § 12 Absatz 7 die Wortfolge 'der erweiterten Gefahrenerforschung (§ 6 Abs. 1 Z 1),';

6.3 § 6 Absatz 1 Ziffer 2 zur Gänze;

sowie wegen untrennbarer Verbundenheit

- § 10 Absatz 1 Ziffer 2 zur Gänze;

- in § 11 Absatz 1 erster Satz die Wortfolge 'zum vorbeugenden Schutz vor verfassungsgefährdenden Angriffen (§ 6 Abs. 1 Z 2)';

- in § 12 Absatz 7 die Wortfolge 'des vorbeugenden Schutzes vor verfassungsgefährdenden Angriffen (§ 6 Abs. 1 Z 2),';

6.4 § 6 Absatz 1 Ziffer 3 zur Gänze;

sowie wegen untrennbarer Verbundenheit § 10 Absatz 1 Ziffer 3 zur Gänze;

6.5 § 6 Absatz 2 Z 2 die Wortfolge '274 Abs. 2 erster Fall,';

6.6 § 6 Absatz 2 Z 2 clic Wortfolge 'oder in 278c StGB genannten';

6.7 § 6 Absatz 2 Z 4 die Zeichenfolge ' 124,';

6.8 § 9 Absatz 1 zweiter Satz zur Gänze: 'Beim Verwenden sensibler und strafrechtlich relevanter Daten haben sie angemessene Vorkehrungen zur Wahrung der Geheimhaltungsinteressen der Betroffenen zu treffen.';

6.9 § 10 Absatz 1 letzter Satz: 'wobei sensible Daten gemäß § 4 Z 2 Datenschutzgesetz 2000 — DSG 2000, BGBl. I Nr. 165/1999, nur insoweit ermittelt und weiterverarbeitet werden dürfen, als diese für die Erfüllung der Aufgabe unbedingt erforderlich sind.';

6.10 § 10 Absatz 5 zur Gänze: 'Abgesehen von den Fällen der Abs. 2 bis 4 sowie den Ermittlungen nach § 11 sind die Organisationseinheiten gemäß § 1 Abs. 3 für Zwecke des Abs. 1 berechtigt, personenbezogene Daten aus allen anderen verfügbaren Quellen durch Einsatz geeigneter Mittel, insbesondere durch Zugriff etwa auf im Internet öffentlich zugängliche Daten, zu ermitteln und weiterzuverarbeiten. Abs. 2 zweiter Satz gilt';

6.11 § 11 Absatz 1 Z 1 zur Gänze;

6.12 § 11 Absatz 1 Z 2 zur Gänze;

6.13 § 11 Absatz 1 Z 3 zur Gänze;

6.14 § 11 Absatz 1 Z 5 zur Gänze;

6.15 § 11 Absatz 1 Z 6 zur Gänze;

6.16 § 11 Absatz 1 Z 7 zur Gänze;

in eventu zu 6.11 bis 6.16: § 11 zur Gänze;

6.17 § 12 zur Gänze;

in eventu zu 6.17

- § 12 Absatz 1 Z 1 zur Gänze;

- § 12 Absatz 1 Z 4 zur Gänze;

- § 12 Absatz 1 letzter Satz zur Gänze: 'Soweit dies zur Erfüllung des Zwecks (Abs. 1) unbedingt erforderlich ist, dürfen auch sensible Daten im Sinne des § 4 Z 2 DSG 2000 verarbeitet werden.'

6.18 § 15 Absatz 1 letzter Satz zur Gänze 'Dies gilt jedoch nicht für Auskünfte über die Identität von Personen nach Maßgabe des i162 StP0.';

sowie

7. im Bundesgesetz vom 26.02.2016, BGBl. I Nr. 5/2016, mit dem das Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz - PStSG) erlassen und das Sicherheitspolizeigesetz geändert werden, Artikel 2

7.1 Ziffer 10 zur Gänze;

7.2 Ziffer 13 zur Gänze;

7.3 in Ziffer 15. die Wortfolge 'oder im Auftrag der Sicherheitsbehörde durch andere Personen (Vertrauenspersonen),die ihren Auftrag weder offen legen noch erkennen lassen,'; sowie in Ziffer 16. den letzten Satz '§ 54a gilt für verdeckte Ermittlungen durch Vertrauenspersonen nicht.';

7.4 Ziffer 27 zur Gänze;

7.5 In Ziffer 30 die Wortfolge 'sowie unter den Voraussetzungen des § 53a Abs. 3a in der Fassung BGBl. I Nr. 5/2016 auch im Informationsverbundsystem geführt'[…]"

als verfassungswidrig aufzuheben (Zitat ohne die im Original enthaltenen Hervorhebungen). 2

## II. Rechtslage

Das Bundesgesetz, mit dem das Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz – PStSG) erlassen und das Sicherheitspolizeigesetz geändert werden, BGBl. I 5/2016, lautet wie folgt: 3

"Artikel 1
Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz – PStSG)

1. Hauptstück
Allgemeines

Anwendungsbereich; Polizeilicher Staatsschutz

§ 1. (1) Dieses Bundesgesetz regelt den polizeilichen Staatsschutz. Dieser erfolgt in Ausübung der Sicherheitspolizei.
(2) Der polizeiliche Staatsschutz dient dem Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit sowie von Vertretern ausländischer Staaten, internationaler Organisationen und anderer Völkerrechtssubjekte nach Maßgabe völkerrechtlicher Verpflichtungen, kritischer Infrastruktur und der Bevölkerung vor terroristisch, ideologisch oder religiös motivierter Kriminalität, vor Gefährdungen durch Spionage, durch nachrichtendienstliche Tätigkeit und durch Proliferation sowie der Wahrnehmung zentraler Funktionen der internationalen Zusammenarbeit in diesen Bereichen.
(3) Für die Wahrnehmung der in Abs. 2 genannten Angelegenheiten bestehen als Organisationseinheit der Generaldirektion für die öffentliche Sicherheit das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (Bundesamt) und in jedem Bundesland eine für Verfassungsschutz zuständige Organisationseinheit der Landespolizeidirektion.
(4) Der Bundesminister für Inneres kann bestimmte Angelegenheiten nach Abs. 2 dem Bundesamt vorbehalten. Diesfalls kann das Bundesamt die für Verfassungsschutz zuständige Organisationseinheit der Landespolizeidirektion mit der Durchführung einzelner Maßnahmen beauftragen. Auch kann das Bundesamt anordnen, dass ihm direkt über den Fortgang einer Angelegenheit laufend oder zu bestimmten Zeitpunkten zu berichten ist.
(5) Das Bundesamt wird bei Vollziehung dieses Bundesgesetzes für den Bundesminister für Inneres, die für Verfassungsschutz zuständige Organisationseinheit für die jeweilige Landespolizeidirektion tätig.

Organisation

§ 2. (1) Dem Bundesamt steht ein Direktor vor. Der Direktor nimmt die Funktion als Informationssicherheitsbeauftragter für den Wirkungsbereich des Bundesministeriums für Inneres nach § 7 des Informationssicherheitsgesetzes – InfoSiG, BGBl. I Nr. 23/2002, wahr.

(2) Zum Direktor kann nur ernannt werden, wer ein abgeschlossenes Studium der Rechtswissenschaften und besondere Kenntnisse auf dem Gebiet des polizeilichen Staatsschutzes aufweist.
(3) Sonstige Bedienstete der Organisationseinheiten gemäß § 1 Abs. 3 haben innerhalb von zwei Jahren nach Dienstbeginn eine spezielle Ausbildung für Verfassungsschutz und Terrorismusbekämpfung zu absolvieren, deren näherer Inhalt durch Verordnung des Bundesministers für Inneres festzusetzen ist.
(4) Sofern es sich bei Bediensteten in Leitungsfunktionen nicht bereits um Organe des öffentlichen Sicherheitsdienstes handelt, können sie nach erfolgreicher Absolvierung der Ausbildung (Abs. 3) zur Ausübung unmittelbarer Befehls- und Zwangsgewalt ermächtigt werden. Diesfalls gelten sie als Organe des öffentlichen Sicherheitsdienstes nach § 5 Abs. 2 Sicherheitspolizeigesetz – SPG, BGBl. Nr. 566/1991.
(5) Vor Beginn der Tätigkeit muss sich jeder Bedienstete einer Sicherheitsüberprüfung (§ 55 SPG) für den Zugang zu geheimer Information unterziehen. Strebt der Bedienstete eine Leitungsfunktion an, muss er sich einer Sicherheitsüberprüfung für den Zugang zu streng geheimer Information unterziehen. Die Sicherheitsüberprüfungen sind nach drei Jahren zu wiederholen. Bei Vorliegen von Anhaltspunkten, wonach ein Bediensteter nicht mehr vertrauenswürdig sein könnte, ist die Sicherheitsüberprüfung vor Ablauf dieser Frist zu wiederholen.

Geschäftsordnung des Bundesamtes

§ 3. Der Direktor des Bundesamtes hat festzulegen, wem die Genehmigung von Entscheidungen für den Bundesminister für Inneres im Rahmen der Geschäftseinteilung zukommt, in welchen Fällen ihm die Genehmigung vorbehalten ist und wem diese im Fall der Verhinderung obliegt (Geschäftsordnung). Vor Erlassung und vor jeder Änderung der Geschäftsordnung ist der Generaldirektor für die öffentliche Sicherheit zu befassen.

Bundesamt als Zentralstelle

§ 4. Das Bundesamt erfüllt für den Bundesminister für Inneres folgende zentrale Funktionen:
1. Operative Koordinierungsstelle für Meldungen über jede Form von Angriffen auf Computersysteme (§ 74 Abs. 1 Z 8 Strafgesetzbuch – StGB, BGBl. Nr. 60/1974) von verfassungsmäßigen Einrichtungen (§ 22 Abs. 1 Z 2 SPG) sowie kritischen Infrastrukturen (§ 22 Abs. 1 Z 6 SPG) nach den §§ 118a, 119, 119a, 126a, 126b und 126c StGB;
2. Meldestelle für jede Form der Betätigung im nationalsozialistischen Sinn nach dem Verbotsgesetz – VerbotsG, StGBl. Nr. 13/1945 (Meldestelle NS-Wiederbetätigung);
3. die Durchführung von Sicherheitsüberprüfungen (§ 55 SPG);
4. die Organisation der Gebäudesicherheit der vom Bundesministerium für Inneres genutzten Gebäude;
5. die internationale Zusammenarbeit auf dem Gebiet des Staatsschutzes; davon unberührt bleibt die Zusammenarbeit der für Verfassungsschutz zuständigen Organisationseinheiten der Landespolizeidirektionen mit benachbarten regionalen Sicherheitsdienststellen.

Anwendbarkeit des Sicherheitspolizeigesetzes

§ 5. Soweit in diesem Bundesgesetz nicht Besonderes bestimmt ist, gilt das Sicherheitspolizeigesetz.

## 2. Hauptstück
## Aufgaben auf dem Gebiet des polizeilichen Staatsschutzes

Erweiterte Gefahrenerforschung und Schutz vor verfassungsgefährdenden Angriffen

§ 6. (1) Den Organisationseinheiten gemäß § 1 Abs. 3 obliegen

1. die erweiterte Gefahrenerforschung; das ist die Beobachtung einer Gruppierung, wenn im Hinblick auf deren bestehende Strukturen und auf zu gewärtigende Entwicklungen in deren Umfeld damit zu rechnen ist, dass es zu mit schwerer Gefahr für die öffentliche Sicherheit verbundener Kriminalität, insbesondere zu ideologisch oder religiös motivierter Gewalt kommt;
2. der vorbeugende Schutz vor verfassungsgefährdenden Angriffen durch eine Person, sofern ein begründeter Gefahrenverdacht für einen solchen Angriff besteht (§ 22 Abs. 2 SPG);
3. der Schutz vor verfassungsgefährdenden Angriffen aufgrund von Informationen von Dienststellen inländischer Behörden, ausländischen Sicherheitsbehörden oder Sicherheitsorganisationen (§ 2 Abs. 2 und 3 Polizeikooperationsgesetz – PolKG, BGBl. I Nr. 104/1997) sowie von Organen der Europäischen Union oder Vereinten Nationen zu Personen, die im Verdacht stehen, im Ausland einen Sachverhalt verwirklicht zu haben, der einem verfassungsgefährdenden Angriff entspricht.

(2) Ein verfassungsgefährdender Angriff ist die Bedrohung von Rechtsgütern

1. durch die rechtswidrige Verwirklichung des Tatbestandes einer nach §§ 278b bis 278f oder, soweit es der Verfügungsmacht einer terroristischen Vereinigung unterliegende Vermögensbestandteile betrifft, nach § 165 Abs. 3 StGB strafbaren Handlung;
2. durch die rechtswidrige Verwirklichung des Tatbestandes einer nach §§ 274 Abs. 2 erster Fall, 279, 280, 283 Abs. 3 oder in § 278c StGB genannten strafbaren Handlung, sofern diese ideologisch oder religiös motiviert ist;
3. durch die rechtswidrige Verwirklichung des Tatbestandes einer nach §§ 242 und 246 StGB, dem fünfzehnten Abschnitt des StGB oder nach dem VerbotsG strafbaren Handlung;
4. durch die rechtswidrige und vorsätzliche Verwirklichung des Tatbestandes einer nach §§ 175, 177a, 177b StGB, §§ 79 bis 82 Außenwirtschaftsgesetz 2011 – AußWG 2011, BGBl. I Nr. 26/2011, § 7 Kriegsmaterialgesetz – KMG, BGBl. Nr. 540/1977, § 11 Sanktionengesetz 2010 – SanktG, BGBl. I Nr. 36/2010, nach §§ 124, 316, 319 oder 320 StGB sowie nach dem sechzehnten Abschnitt des StGB strafbaren Handlung;
5. durch die rechtswidrige Verwirklichung des Tatbestandes einer nach §§ 118a, 119, 119a, 126a, 126b oder 126c StGB strafbaren Handlung gegen verfassungsmäßige Einrichtungen und ihre Handlungsfähigkeit (§ 22 Abs. 1 Z 2 SPG) sowie kritische Infrastrukturen (§ 22 Abs. 1 Z 6 SPG).

Polizeilich staatsschutzrelevante Beratung

§ 7. Den Organisationseinheiten gemäß § 1 Abs. 3 obliegen zur Vorbeugung verfassungsgefährdender Angriffe, insbesondere auf dem Gebiet der Cybersicherheit, die Förderung der Bereitschaft und Fähigkeit des Einzelnen, sich über eine Bedrohung seiner Rechtsgüter Kenntnis zu verschaffen und Angriffen entsprechend vorzubeugen.

Information verfassungsmäßiger Einrichtungen

§ 8. (1) Die Wahrnehmung der Aufgabenerfüllung nach diesem Bundesgesetz umfasst ferner die Analyse und Beurteilung von staatsschutzrelevanten Bedrohungslagen, die sich auch aus verfassungsgefährdenden Entwicklungen im Ausland ergeben können, zur Information verfassungsmäßiger Einrichtungen, sofern nicht der Vollziehungsbereich des Bundesministers für Landesverteidigung und Sport betroffen ist.

(2) Über staatsschutzrelevante Bedrohungen sind die obersten Organe der Vollziehung (Art. 19 B-VG) sowie die mit der Leitung der gesetzgebenden Körperschaften des Bundes und der Länder betrauten Organe zu unterrichten, soweit diese Information für die Wahrnehmung der gesetzlichen Aufgaben in deren Zuständigkeitsbereich von Bedeutung ist. Ebenso sind die Genannten über Umstände zu unterrichten, die für die Ausübung ihres Amtes von wesentlicher Bedeutung sind.

## 3. Hauptstück
## Verwenden personenbezogener Daten auf dem Gebiet des polizeilichen Staatsschutzes

Allgemeines

§ 9. (1) Die Organisationseinheiten gemäß § 1 Abs. 3 haben beim Verwenden (Verarbeiten und Übermitteln) personenbezogener Daten die Verhältnismäßigkeit (§ 29 SPG) zu beachten. Beim Verwenden sensibler und strafrechtlich relevanter Daten haben sie angemessene Vorkehrungen zur Wahrung der Geheimhaltungsinteressen der Betroffenen zu treffen. Bei Ermittlungen von personenbezogenen Daten nach diesem Bundesgesetz ist ein Eingriff in das von § 157 Abs. 1 Z 2 bis 4 Strafprozessordnung – StPO, BGBl. Nr. 631/1975, geschützte Recht nicht zulässig. § 157 Abs. 2 StPO gilt sinngemäß.

(2) Personenbezogene Daten dürfen von den Organisationseinheiten gemäß § 1 Abs. 3 gemäß diesem Hauptstück nur verwendet werden, soweit dies zur Erfüllung der ihnen übertragenen Aufgaben erforderlich ist. Ermächtigungen nach anderen Bundesgesetzen bleiben unberührt.

Ermittlungsdienst für Zwecke des polizeilichen Staatsschutzes

§ 10. (1) Die Organisationseinheiten gemäß § 1 Abs. 3 dürfen personenbezogene Daten ermitteln und weiterverarbeiten für

1. die erweiterte Gefahrenerforschung (§ 6 Abs. 1 Z 1),
2. den vorbeugenden Schutz vor verfassungsgefährdenden Angriffen (§ 6 Abs. 1 Z 2),
3. den Schutz vor verfassungsgefährdenden Angriffen aufgrund von Informationen von Dienststellen inländischer Behörden, ausländischen Sicherheitsbehörden

oder Sicherheitsorganisationen sowie von Organen der Europäischen Union oder Vereinten Nationen (§ 6 Abs. 1 Z 3) und
4. die Information verfassungsmäßiger Einrichtungen (§ 8),
wobei sensible Daten gemäß § 4 Z 2 Datenschutzgesetz 2000 – DSG 2000, BGBl. I Nr. 165/1999, nur insoweit ermittelt und weiterverarbeitet werden dürfen, als diese für die Erfüllung der Aufgabe unbedingt erforderlich sind.
(2) Die Organisationseinheiten gemäß § 1 Abs. 3 dürfen Daten, die sie in Vollziehung von Bundes- oder Landesgesetzen rechtmäßig verarbeitet haben, für die Zwecke des Abs. 1 ermitteln und weiterverarbeiten. Ein automationsunterstützter Datenabgleich im Sinne des § 141 StPO ist davon nicht umfasst. Bestehende Übermittlungsverbote bleiben unberührt.
(3) Die Organisationseinheiten gemäß § 1 Abs. 3 sind berechtigt, von den Dienststellen der Gebietskörperschaften, den anderen Körperschaften des öffentlichen Rechtes und den von diesen betriebenen Anstalten Auskünfte zu verlangen, die sie zur Erfüllung ihrer Aufgaben nach Abs. 1 Z 1 und 2 benötigen. Eine Verweigerung der Auskunft ist nur zulässig, soweit andere öffentliche Interessen überwiegen oder eine über die Amtsverschwiegenheit (Art. 20 Abs. 3 B-VG) hinausgehende sonstige gesetzliche Verpflichtung zur Verschwiegenheit besteht.
(4) Die Organisationseinheiten gemäß § 1 Abs. 3 sind im Einzelfall ermächtigt, für die Erfüllung ihrer Aufgaben nach Abs. 1 Z 1 und 2 personenbezogene Bilddaten zu verwenden, die Rechtsträger des öffentlichen oder privaten Bereichs mittels Einsatz von Bild- und Tonaufzeichnungsgeräten rechtmäßig ermittelt und den Sicherheitsbehörden übermittelt haben, wenn ansonsten die Aufgabenerfüllung gefährdet oder erheblich erschwert wäre. Dabei ist besonders darauf zu achten, dass Eingriffe in die Privatsphäre der Betroffenen die Verhältnismäßigkeit (§ 29 SPG) zum Anlass wahren. Nicht zulässig ist die Verwendung von Daten über nichtöffentliches Verhalten.
(5) Abgesehen von den Fällen der Abs. 2 bis 4 sowie den Ermittlungen nach § 11 sind die Organisationseinheiten gemäß § 1 Abs. 3 für Zwecke des Abs. 1 berechtigt, personenbezogene Daten aus allen anderen verfügbaren Quellen durch Einsatz geeigneter Mittel, insbesondere durch Zugriff etwa auf im Internet öffentlich zugängliche Daten, zu ermitteln und weiterzuverarbeiten. Abs. 2 zweiter Satz gilt.

Besondere Bestimmungen für die Ermittlungen

§ 11. (1) Zur erweiterten Gefahrenerforschung (§ 6 Abs. 1 Z 1) und zum vorbeugenden Schutz vor verfassungsgefährdenden Angriffen (§ 6 Abs. 1 Z 2) ist die Ermittlung personenbezogener Daten nach Maßgabe des § 9 und unter den Voraussetzungen des § 14 zulässig durch
1. Observation (§ 54 Abs. 2 SPG), sofern die Observation ansonsten aussichtslos oder wesentlich erschwert wäre unter Einsatz technischer Mittel (§ 54 Abs. 2a SPG);
2. verdeckte Ermittlung (§ 54 Abs. 3 und 3a SPG), wenn die Erfüllung der Aufgabe durch Einsatz anderer Ermittlungsmaßnahmen aussichtslos wäre;
3. Einsatz von Bild- und Tonaufzeichnungsgeräten (§ 54 Abs. 4 SPG); dieser darf verdeckt erfolgen, wenn die Erfüllung der Aufgabe ansonsten aussichtslos wäre;
4. Einsatz von Kennzeichenerkennungsgeräten (§ 54 Abs. 4b SPG) zum automatisierten Abgleich mit KFZ-Kennzeichen, die nach § 12 Abs. 1 verarbeitet werden;

5. Einholen von Auskünften nach §§ 53 Abs. 3a Z 1 bis 3 und 53 Abs. 3b SPG zu einer Gruppierung nach § 6 Abs. 1 Z 1 oder einem Betroffenen nach § 6 Abs. 1 Z 2 sowie zu deren jeweiligen Kontakt- oder Begleitpersonen (§ 12 Abs. 1 Z 4) von Betreibern öffentlicher Telekommunikationsdienste (§ 92 Abs. 3 Z 1 Telekommunikationsgesetz 2003 – TKG 2003, BGBl. I Nr. 70/2003) und sonstigen Diensteanbietern (§ 3 Z 2 E-Commerce-Gesetz – ECG, BGBl. I Nr. 152/2001), wenn die Erfüllung der Aufgabe durch Einsatz anderer Ermittlungsmaßnahmen aussichtslos wäre;
6. Einholen von Auskünften zu Kontaktdaten, Nummer und Art des Reisedokuments sowie Zahlungsinformationen eines Betroffenen nach § 6 Abs. 1 Z 2, Datum der Buchung, Reiseverlauf, Reisestatus, Flugscheindaten, Zahl und Namen von Mitreisenden im Rahmen einer Buchung von Personenbeförderungsunternehmen zu einer von ihnen erbrachten Leistung;
7. Einholen von Auskünften über Verkehrsdaten (§ 92 Abs. 3 Z 4 TKG 2003), Zugangsdaten (§ 92 Abs. 3 Z 4a TKG 2003) und Standortdaten (§ 92 Abs. 3 Z 6 TKG 2003), die nicht einer Auskunft nach Abs. 1 Z 5 unterliegen, zu einer Gruppierung nach § 6 Abs. 1 Z 1 oder einem Betroffenen nach § 6 Abs. 1 Z 2 von Betreibern öffentlicher Telekommunikationsdienste (§ 92 Abs. 3 Z 1 TKG 2003) und sonstigen Diensteanbietern (§ 3 Z 2 ECG), wenn dies zur Vorbeugung eines verfassungsgefährdenden Angriffs, dessen Verwirklichung mit beträchtlicher Strafe (§ 17 SPG) bedroht ist, erforderlich erscheint und die Erfüllung der Aufgabe durch Einsatz anderer Ermittlungsmaßnahmen aussichtslos wäre. Eine Ermächtigung darf nur für jenen künftigen oder auch vergangenen Zeitraum erteilt werden, der zur Erreichung des Zwecks voraussichtlich erforderlich ist.
Die Ermittlung ist zu beenden, sobald ihre Voraussetzungen wegfallen.
(2) In den Fällen des Abs. 1 Z 5 bis 7 ist die ersuchte Stelle verpflichtet, die Auskünfte zu erteilen. Der Ersatz von Kosten in den Fällen des Abs. 1 Z 5 hinsichtlich § 53 Abs. 3b SPG und des Abs. 1 Z 7 richtet sich nach der Überwachungskostenverordnung – ÜKVO, BGBl. II Nr. 322/2004.
(3) Beim Einholen von Auskünften nach Abs. 1 Z 7 hat das Bundesamt der um Auskunft ersuchten Stelle die Verpflichtung nach Abs. 2 und ihren Umfang sowie die Verpflichtung, mit der Ermächtigung verbundene Tatsachen und Vorgänge gegenüber Dritten geheim zu halten, aufzutragen und die entsprechende Ermächtigung des Rechtsschutzsenats anzuführen.

Datenanwendungen

§ 12. (1) Der Bundesminister für Inneres und die Landespolizeidirektionen dürfen als datenschutzrechtliche Auftraggeber in einem vom Bundesamt betriebenen Informationsverbundsystem zum Zweck der Bewertung von wahrscheinlichen Gefährdungen sowie zum Erkennen von Zusammenhängen und Strukturen mittels operativer oder strategischer Analyse
1. zu einer Gruppierung nach § 6 Abs. 1 Z 1
a) Namen,
b) frühere Namen,
c) Aliasdaten,
d) Anschrift/Aufenthalt,
e) Rechtsform/-status,

f) sachbezogene Daten zu Kommunikations- und Verkehrsmittel einschließlich Registrierungsnummer/Kennzeichen und
g) Informationen über wirtschaftliche und finanzielle Verhältnisse einschließlich damit im Zusammenhang stehender Daten juristischer Personen,
2. zu Betroffenen nach § 6 Abs. 1 Z 2
a) Namen,
b) frühere Namen,
c) Aliasdaten,
d) Namen der Eltern,
e) Geschlecht,
f) Geburtsdatum und Ort,
g) Staatsangehörigkeit,
h) Wohnanschrift/Aufenthalt,
i) Dokumentendaten,
j) Beruf, Qualifikation und Funktion/Beschäftigung/Lebensverhältnisse,
k) Daten, die für die Einreise- und Aufenthaltsberechtigung maßgeblich sind,
l) sachbezogene Daten zu Kommunikations- und Verkehrsmittel sowie Waffen einschließlich Registrierungsnummer/Kennzeichen,
m) Lichtbild und sonstige zur Personenbeschreibung erforderliche Daten,
n) erkennungsdienstliche Daten und
o) Informationen über wirtschaftliche und finanzielle Verhältnisse einschließlich damit im Zusammenhang stehender Daten juristischer Personen,
3. zu Verdächtigen eines verfassungsgefährdenden Angriffs die Datenarten nach Z 2 a) bis o),
4. zu Kontakt- oder Begleitpersonen, die unmittelbar und nicht nur zufällig mit einer Gruppierung nach Z 1, Betroffenen nach Z 2 oder Verdächtigen nach Z 3 in Verbindung stehen und bei denen ausreichende Gründe für die Annahme bestehen, dass über sie für die Erfüllung der Aufgabe relevante Informationen beschafft werden können, die Datenarten nach Z 2 a) bis m) bis zur möglichst rasch vorzunehmenden Klärung der Beziehung zu diesen Personen,
5. zu Informanten und sonstigen Auskunftspersonen die Datenarten nach Z 2 a) bis j)
sowie tat- und fallbezogene Informationen und Verwaltungsdaten verarbeiten, die gemäß §§ 10 oder 11 oder auf Grundlage des SPG oder der StPO ermittelt wurden. Soweit dies zur Erfüllung des Zwecks (Abs. 1) unbedingt erforderlich ist, dürfen auch sensible Daten im Sinne des § 4 Z 2 DSG 2000 verarbeitet werden.
(2) Die Daten sind vor der Verarbeitung in der Datenanwendung auf ihre Erheblichkeit und Richtigkeit zu prüfen sowie während der Verwendung zu aktualisieren. Erweisen sich Daten als unrichtig, dann sind diese richtigzustellen oder zu löschen, es sei denn, die Weiterverarbeitung von Falschinformationen mit der Kennzeichnung 'unrichtig' ist zur Erfüllung des Zwecks (Abs. 1) erforderlich. Bei Einstellung von Ermittlungen oder Beendigung eines Verfahrens einer Staatsanwaltschaft oder eines Strafgerichtes sind die Daten durch Anmerkung der Einstellung oder Verfahrensbeendigung und des bekannt gewordenen Grundes zu aktualisieren. Eine Aktualisierung oder Richtigstellung von Daten nach Abs. 1 Z 1 lit. a bis d und Z 2 lit. a bis i darf jeder Auftraggeber vornehmen. Hievon ist jener Auftraggeber, der die Daten verarbeitet hat, zu informieren.

(3) Daten sind nach Maßgabe des § 13 zu löschen. Daten zu Verdächtigen gemäß Abs. 1 Z 3 und damit in Zusammenhang stehenden Personen gemäß Abs. 1 Z 5 sind längstens nach fünf Jahren, Personen gemäß Abs. 1 Z 4 längstens nach drei Jahren zu löschen. Daten zu Kontakt- und Begleitpersonen gemäß Abs. 1 Z 4 sind jedenfalls zu löschen, wenn keine Gründe für die Annahme mehr vorliegen, dass über sie für die Erfüllung der Aufgabe relevante Informationen beschafft werden können.
(4) Übermittlungen sind an Sicherheitsbehörden für Zwecke der Sicherheitspolizei und Strafrechtspflege, an Staatsanwaltschaften und ordentliche Gerichte für Zwecke der Strafrechtspflege, an verfassungsmäßige Einrichtungen nach Maßgabe des § 8 und darüber hinaus an Dienststellen inländischer Behörden, soweit dies eine wesentliche Voraussetzung zur Wahrnehmung einer ihr gesetzlich übertragenen Aufgabe ist, an ausländische Sicherheitsbehörden und Sicherheitsorganisationen (§ 2 Abs. 2 und 3 PolKG) sowie Organe der Europäischen Union oder Vereinten Nationen entsprechend den Bestimmungen über die internationale polizeiliche Amtshilfe zulässig.
(5) Jede Abfrage und Übermittlung personenbezogener Daten ist so zu protokollieren, dass eine Zuordnung der Abfrage oder Übermittlung zu einem bestimmten Organwalter möglich ist. Die Protokollaufzeichnungen sind drei Jahre aufzubewahren und danach zu löschen.
(6) Die Kontrolle der Datenanwendung nach Abs. 1 obliegt dem Rechtsschutzbeauftragten nach Maßgabe des § 91c Abs. 2 SPG sowie § 15 Abs. 1.
(7) Darüber hinaus ist das Bundesamt nach Maßgabe des § 54b SPG ermächtigt, personenbezogene Daten von Menschen, die Informationen zur Erfüllung der Aufgabe der erweiterten Gefahrenerforschung (§ 6 Abs. 1 Z 1), des vorbeugenden Schutzes vor verfassungsgefährdenden Angriffen (§ 6 Abs. 1 Z 2), zur Abwehr gefährlicher Angriffe oder krimineller Verbindungen (§ 21 Abs. 1 SPG) weitergeben, zu verarbeiten.

Besondere Löschungsverpflichtung

§ 13. (1) Soweit sich eine Aufgabe nach § 6 Abs. 1 Z 1 oder 2 gestellt hat, sind die nach diesem Bundesgesetz ermittelten personenbezogenen Daten zu löschen, wenn sich nach Ablauf der Zeit, für die die Ermächtigung dazu erteilt wurde, keine Aufgabe für die Organisationseinheiten gemäß § 1 Abs. 3 stellt. Überdies kann die unverzügliche Löschung unterbleiben, wenn in Hinblick auf die Gruppierung oder den Betroffenen aufgrund bestimmter Tatsachen, insbesondere aufgrund von verfassungsgefährdenden Aktivitäten im Ausland, erwartet werden kann, dass sie neuerlich Anlass zu einer Aufgabe nach § 6 Abs. 1 Z 1 oder 2 geben wird. Die Organisationseinheiten gemäß § 1 Abs. 3 haben diese Daten einmal jährlich daraufhin zu prüfen, ob ihre Weiterverarbeitung erforderlich ist. Wenn sich zwei Jahre nach Ablauf der Zeit, für die die Ermächtigung dazu erteilt wurde, keine Aufgabe für die Organisationseinheiten gemäß § 1 Abs. 3 stellt, bedarf die Weiterverarbeitung für jeweils ein weiteres Jahr der Ermächtigung des Rechtsschutzbeauftragten (§ 15). Nach Ablauf von sechs Jahren sind die Daten jedenfalls zu löschen.
(2) Wird der Betroffene nach Ende der Ermächtigung gemäß § 16 Abs. 2 von den Organisationseinheiten gemäß § 1 Abs. 3 informiert, sind die nach diesem Bundesgesetz ermittelten personenbezogenen Daten unbeschadet von Abs. 1 für

sechs Monate aufzubewahren; diese Frist verlängert sich um jenen Zeitraum, als die Information des Betroffenen nach § 16 Abs. 3 aufgeschoben wird. Darüber hinaus sind die Daten nicht vor Abschluss eines Rechtsschutzverfahrens zu löschen. Diesfalls sind die Daten für den Zugriff zu sperren und dürfen nur zum Zweck der Information Betroffener oder in einem Rechtsschutzverfahren verwendet werden.

## 4. Hauptstück
## Rechtsschutz auf dem Gebiet des polizeilichen Staatsschutzes

### Rechtsschutzbeauftragter

§ 14. (1) Dem Rechtsschutzbeauftragten (§ 91a SPG) obliegt der besondere Rechtsschutz bei den Aufgaben nach § 6 Abs. 1 Z 1 und 2 sowie die Kontrolle der Datenanwendung nach § 12 Abs. 6.

(2) Die Organisationseinheiten gemäß § 1 Abs. 3, denen sich eine Aufgabe gemäß § 6 Abs. 1 Z 1 oder 2 stellt, haben vor der Durchführung der Aufgabe die Ermächtigung des Rechtsschutzbeauftragten im Wege des Bundesministers für Inneres einzuholen. Dasselbe gilt, wenn beabsichtigt ist, besondere Ermittlungsmaßnahmen nach § 11 zu setzen oder gemäß § 10 Abs. 4 ermittelte Daten weiterzuverarbeiten. Jede Einholung einer Ermächtigung ist entsprechend zu begründen, insbesondere sind darin die Gründe für den Einsatz einer Vertrauensperson (§ 11 Abs. 1 Z 2 iVm § 54 Abs. 3 und 3a SPG) anzuführen. Eine Ermächtigung darf nur in jenem Umfang und für jenen Zeitraum erteilt werden, der zur Erfüllung der Aufgabe voraussichtlich erforderlich ist, höchstens aber für die Dauer von sechs Monaten; Verlängerungen sind zulässig.

(3) Über die Erteilung der Ermächtigung zu Ermittlungsmaßnahmen gemäß § 11 Abs. 1 Z 2 iVm § 54 Abs. 3 und 3a SPG und § 11 Abs. 1 Z 7 entscheiden der Rechtsschutzbeauftragte und zwei seiner Stellvertreter mit Stimmenmehrheit (Rechtsschutzsenat). Bei Gefahr im Verzug kann der Rechtsschutzbeauftragte die Ermächtigung vorläufig erteilen. In diesem Fall hat er die dem Rechtsschutzsenat angehörenden Stellvertreter unverzüglich zu befassen; wird die Ermächtigung nicht bestätigt, ist die Ermittlungsmaßnahme sogleich zu beenden und die bislang ermittelten Daten sind zu löschen.

### Rechte und Pflichten des Rechtsschutzbeauftragten

§ 15. (1) Die Organisationseinheiten gemäß § 1 Abs. 3 haben dem Rechtsschutzbeauftragten bei der Wahrnehmung seiner Aufgaben jederzeit Einblick in alle erforderlichen Unterlagen und Aufzeichnungen sowie in die Datenanwendung nach § 12 Abs. 1 zu gewähren, ihm auf Verlangen Abschriften (Ablichtungen) einzelner Aktenstücke unentgeltlich auszufolgen und alle erforderlichen Auskünfte zu erteilen; insofern kann ihm gegenüber Amtsverschwiegenheit nicht geltend gemacht werden. Dies gilt jedoch nicht für Auskünfte über die Identität von Personen nach Maßgabe des § 162 StPO.

(2) Dem Rechtsschutzbeauftragten ist jederzeit Gelegenheit zu geben, die Durchführung der in § 14 Abs. 2 genannten Maßnahmen zu überwachen und alle Räume zu betreten, in denen Aufnahmen oder sonstige Überwachungsergebnisse aufbewahrt werden. Darüber hinaus hat er im Rahmen seiner Aufgabenstel-

lungen die Einhaltung der Pflicht zur Richtigstellung oder Löschung nach § 13 zu überwachen.
(3) In Verfahren über Beschwerden von Betroffenen einer Aufgabe nach § 6 Abs. 1 Z 1 oder 2 vor der Datenschutzbehörde, den Verwaltungsgerichten sowie den Gerichtshöfen des öffentlichen Rechts kommt dem Rechtsschutzbeauftragten die Stellung einer mitbeteiligten Amtspartei zu.
(4) Der Rechtsschutzbeauftragte erstattet dem Bundesminister für Inneres jährlich bis spätestens 31. März des Folgejahres einen Bericht über seine Tätigkeit und Wahrnehmungen im Rahmen seiner Aufgabenerfüllung nach diesem Bundesgesetz.

Information Betroffener

§ 16. (1) Nimmt der Rechtsschutzbeauftragte wahr, dass durch Verwenden personenbezogener Daten Rechte von Betroffenen einer Aufgabe nach § 6 Abs. 1 Z 1 oder 2 verletzt worden sind, die von dieser Datenverwendung keine Kenntnis haben, so ist er zu deren Information oder, sofern eine solche aus den Gründen des § 26 Abs. 2 DSG 2000 nicht erfolgen kann, zur Erhebung einer Beschwerde an die Datenschutzbehörde nach § 90 SPG verpflichtet. In einem solchen Verfahren vor der Datenschutzbehörde ist auf § 26 Abs. 2 DSG 2000 über die Beschränkung des Auskunftsrechtes Bedacht zu nehmen.
(2) Nach Ablauf der Zeit, für die die Ermächtigung erteilt wurde, ist der Betroffene einer Aufgabe nach § 6 Abs. 1 Z 1 oder 2 von den Organisationseinheiten gemäß § 1 Abs. 3 über Grund, Art und Dauer sowie die Rechtsgrundlage der gesetzten Maßnahmen zu informieren. Über die durchgeführte Information ist der Rechtsschutzbeauftragte in Kenntnis zu setzen.
(3) Die Information kann mit Zustimmung des Rechtsschutzbeauftragten aufgeschoben werden, solange durch sie die Aufgabenerfüllung gefährdet wäre, und unterbleiben, wenn der Betroffene bereits nachweislich Kenntnis erlangt hat, die Information des Betroffenen unmöglich ist oder aus den Gründen des § 26 Abs. 2 DSG 2000 nicht erfolgen kann.

Berichte über den polizeilichen Staatsschutz

§ 17. (1) Das Bundesamt hat unter Einbeziehung der Tätigkeiten der für Verfassungsschutz zuständigen Organisationseinheiten der Landespolizeidirektionen jährlich einen Bericht zu erstellen, mit dem die Öffentlichkeit, unter Einhaltung von gesetzlichen Verschwiegenheitspflichten, über aktuelle und mögliche staatsschutzrelevante Entwicklungen informiert wird.
(2) Der Bundesminister für Inneres hat dem ständigen Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit in dessen Sitzungen über Unterrichtungen gemäß § 8 Abs. 2 erster Satz zu berichten.
(3) Über die Erfüllung der Aufgaben nach diesem Bundesgesetz sowie über die Information Betroffener nach § 16 hat der Bundesminister für Inneres dem ständigen Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit jedenfalls halbjährlich zu berichten.
(4) Den Bericht des Rechtsschutzbeauftragten gemäß § 15 Abs. 4 hat der Bundesminister für Inneres dem ständigen Unterausschuss des Ausschusses für

innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit zu übermitteln.
(5) Der Rechtsschutzbeauftragte hat dem ständigen Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit für Auskünfte über wesentliche Entwicklungen zur Verfügung zu stehen; zudem steht es dem Rechtsschutzbeauftragten frei, in solchen Angelegenheiten jederzeit von sich aus an den ständigen Unterausschuss heranzutreten. In einem solchen Fall hat er seine Absicht dem Vorsitzenden des ständigen Unterausschusses mitzuteilen, der für eine umgehende Einberufung sorgt.

## 5. Hauptstück
## Schlussbestimmungen

### Inkrafttreten

§ 18. (1) Dieses Bundesgesetz tritt mit 1. Juli 2016 in Kraft.
(2) Verordnungen auf Grund dieses Bundesgesetzes können bereits ab dem auf seine Kundmachung folgenden Tag erlassen werden; sie dürfen jedoch frühestens mit dem Inkrafttreten dieses Bundesgesetzes in Kraft gesetzt werden.

### Sprachliche Gleichbehandlung

§ 19. Soweit in diesem Bundesgesetz auf natürliche Personen bezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise. Bei der Anwendung der Bezeichnungen auf bestimmte natürliche Personen ist die geschlechtsspezifische Form zu verwenden.

### Verweisungen

§ 20. Verweisungen in diesem Bundesgesetz auf andere Bundesgesetze sind als Verweisungen auf die jeweils geltende Fassung zu verstehen.

### Übergangsbestimmungen

§ 21. (1) Vor Inkrafttreten dieses Bundesgesetzes erteilte Ermächtigungen gemäß § 91c Abs. 3 SPG in der Fassung vor Inkrafttreten dieses Bundesgesetzes gelten als Ermächtigungen gemäß § 14 Abs. 2 und bleiben bis zum festgesetzten Zeitpunkt, längstens bis zum 31. Dezember 2016, weiterhin gültig; für diese gelten die Löschungsfristen nach § 13.
(2) Personenbezogene Daten, die vor Inkrafttreten dieses Bundesgesetzes von den Organisationseinheiten gemäß § 1 Abs. 3 für die Aufgabe nach § 21 Abs. 3 SPG in der Fassung vor Inkrafttreten dieses Bundesgesetzes rechtmäßig ermittelt wurden, dürfen nach Maßgabe des § 12 Abs. 1 und 2 in der Datenanwendung gemäß § 12 verarbeitet werden.
(3) Lokale Datenanwendungen der Organisationseinheiten gemäß § 1 Abs. 3, die vor Inkrafttreten dieses Bundesgesetzes auf Grundlage des § 53 SPG geführt wurden, dürfen für die Aufgaben nach dem SPG bis zur vollständigen Inbetriebnahme der Datenanwendung nach § 12, längstens bis zum 1. Juli 2017 weitergeführt werden. Darüber hinaus dürfen diese Datenanwendungen ausschließlich für die Zwecke der Übernahme von rechtmäßig verarbeiteten Daten in die Datenanwendung nach § 12 und der Durchführung von Abfragen nach Maßgabe

anderer bundesgesetzlicher Regelungen oder unionsrechtlicher Vorschriften bis 1. Juli 2019 weitergeführt werden.
(4) Personen, die im Zeitpunkt des Inkrafttretens dieses Bundesgesetzes bereits Bedienstete der Organisationseinheiten gemäß § 1 Abs. 3 sind, haben die in § 2 Abs. 3 vorgesehene spezielle Ausbildung für Verfassungsschutz und Terrorismusbekämpfung innerhalb von drei Jahren ab dem Tag des Inkrafttretens zu absolvieren.

Vollziehung

§ 22. Mit der Vollziehung dieses Bundesgesetzes ist der Bundesminister für Inneres betraut.

Artikel 2
Änderung des Sicherheitspolizeigesetzes

Das Sicherheitspolizeigesetz (SPG), BGBl. Nr. 566/1991, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 43/2014 und die Kundmachung BGBl. I Nr. 97/2014, wird wie folgt geändert:

1. Im Inhaltsverzeichnis wird im Eintrag zu § 25 das Wort 'Kriminalpolizeiliche' durch das Wort 'Sicherheitspolizeiliche' ersetzt und es entfällt der Eintrag '§ 93a Information verfassungsmäßiger Einrichtungen'.

2. In § 6 Abs. 1 zweiter Satz werden nach dem Wort 'Bundeskriminalamtes' die Wortfolge 'und des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung' sowie nach dem Wort 'erfolgt' das Wort 'jeweils' eingefügt und es wird das Wort 'Organisationseinheit' durch das Wort 'Organisationseinheiten' ersetzt.

3. Dem § 13a wird folgender Abs. 3 angefügt:
'(3) Zum Zweck der Dokumentation von Amtshandlungen, bei denen die Organe des öffentlichen Sicherheitsdienstes Befehls- und Zwangsgewalt ausüben, ist der offene Einsatz von Bild- und Tonaufzeichnungsgeräten, sofern gesetzlich nicht anderes bestimmt ist, nach Maßgabe der Bestimmungen dieses Absatzes zulässig. Vor Beginn der Aufzeichnung ist der Einsatz auf solche Weise anzukündigen, dass er dem Betroffenen bekannt wird. Die auf diese Weise ermittelten personenbezogenen Daten dürfen nur zur Verfolgung von strafbaren Handlungen, die sich während der Amtshandlung ereignet haben, sowie zur Kontrolle der Rechtmäßigkeit der Amtshandlung ausgewertet werden. Bis zu ihrer Auswertung und Löschung sind die Aufzeichnungen gemäß den Bestimmungen des § 14 DSG 2000 vor unberechtigter Verwendung, insbesondere durch Protokollierung jedes Zugriffs und Verschlüsselung der Daten, zu sichern. Sie sind nach sechs Monaten zu löschen; kommt es innerhalb dieser Frist wegen der Amtshandlung zu einem Rechtsschutzverfahren, so sind die Aufzeichnungen erst nach Abschluss dieses Verfahrens zu löschen. Bei jeglichem Einsatz von Bild- und Tonaufzeichnungsgeräten ist besonders darauf zu achten, dass Eingriffe in die Privatsphäre der Betroffenen die Verhältnismäßigkeit (§ 29) zum Anlass wahren.'

4. In § 20 wird das Wort 'kriminalpolizeiliche' durch das Wort 'sicherheitspolizeiliche' ersetzt.

5. Nach § 21 Abs. 2 wird folgender Abs. 2a eingefügt:
'(2a) Den Sicherheitsbehörden obliegen die Abwehr und Beendigung von gefährlichen Angriffen gegen Leben, Gesundheit, Freiheit oder Eigentum auch an Bord von Zivilluftfahrzeugen, soweit sich ihre Organe auf begründetes Ersuchen des Luftfahrzeughalters oder zur Erfüllung gesetzlicher Aufgaben an Bord befinden und Völkerrecht dem nicht entgegensteht.'

6. Die §§ 21 Abs. 3, 63 Abs. 1a und 1b, 91c Abs. 3 sowie 93a samt Überschrift entfallen.

7. In der Überschrift zu § 25 wird das Wort 'Kriminalpolizeiliche' durch das Wort „Sicherheitspolizeiliche“ ersetzt.

8. In § 53 entfallen in Abs. 1 die Z 2a und 7 und es wird am Ende der Z 6 der Strichpunkt durch einen Punkt ersetzt, in Abs. 3 entfallen der Beistrich nach dem Wort 'Angriffe' und die Wortfolge 'für die erweiterte Gefahrenerforschung unter den Voraussetzungen nach Abs. 1' und in Abs. 5 entfällt die Wortfolge 'für die erweiterte Gefahrenerforschung (§ 21 Abs. 3)'.

9. In § 53 Abs. 3b wird nach der Wortfolge 'die internationale Mobilteilnehmerkennung (IMSI) der' die Wortfolge 'vom Gefährder oder' eingefügt.

10. In § 53 Abs. 4 wird die Wortfolge 'auf allgemein' durch die Wortfolge 'etwa auf im Internet öffentlich' ersetzt.

11. In § 53a entfällt in Abs. 1 die Wortfolge 'den Personen- und Objektschutz und'.

12. Nach § 53a Abs. 1 wird folgender Abs. 1a eingefügt:
'(1a) Die Sicherheitsbehörden dürfen für den Personen- und Objektschutz Erreichbarkeits- und Identifikationsdaten über die gefährdete natürliche oder juristische Person, die erforderlichen Sachdaten einschließlich KFZ-Kennzeichen zu den zu schützenden Objekten, Angaben zu Zeit, Ort, Grund und Art des Einschreitens sowie Verwaltungsdaten verarbeiten.'

13. Nach § 53a Abs. 5 wird folgender Abs. 5a eingefügt:
'(5a) Datenanwendungen nach Abs. 1a zum Schutz von verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit (§ 22 Abs. 1 Z 2), der Vertreter ausländischer Staaten, internationaler Organisationen und anderer Völkerrechtssubjekte (§ 22 Abs. 1 Z 3) sowie von kritischen Infrastrukturen (§ 22 Abs. 1 Z 6) dürfen der Bundesminister für Inneres und die Landespolizeidirektionen als datenschutzrechtliche Auftraggeber in einem vom Bundesamt für Verfassungsschutz und Terrorismusbekämpfung betriebenen Informationsverbundsystem führen. Übermittlungen der gemäß Abs. 1a verarbeiteten Daten sind an Sicherheitsbehörden für Zwecke der Sicherheitspolizei und Strafrechtspflege, an

Staatsanwaltschaften und ordentliche Gerichte für Zwecke der Strafrechtspflege, darüber hinaus an Dienststellen inländischer Behörden, soweit dies eine wesentliche Voraussetzung zur Wahrnehmung einer ihr gesetzlich übertragenen Aufgabe ist, an ausländische Sicherheitsbehörden und Sicherheitsorganisationen (§ 2 Abs. 2 und 3 PolKG) entsprechend den Bestimmungen über die internationale polizeiliche Amtshilfe und im Übrigen nur zulässig, wenn hiefür eine ausdrückliche gesetzliche Ermächtigung besteht.'

14. In § 54 entfallen in Abs. 2 die Z 1 sowie in Abs. 4 die Wortfolge 'und zur erweiterten Gefahrenerforschung (§ 21 Abs. 3)'.

15. § 54 Abs. 3 lautet:
'(3) Das Einholen von Auskünften durch die Sicherheitsbehörde ohne Hinweis gemäß Abs. 1 oder im Auftrag der Sicherheitsbehörde durch andere Personen (Vertrauenspersonen), die ihren Auftrag weder offen legen noch erkennen lassen, ist zulässig, wenn sonst die Abwehr gefährlicher Angriffe oder krimineller Verbindungen gefährdet oder erheblich erschwert wäre (verdeckte Ermittlung). Wohnungen und andere vom Hausrecht geschützte Räume dürfen im Rahmen einer verdeckten Ermittlung nur im Einverständnis mit dem Inhaber betreten werden; dieses darf nicht durch Täuschung über eine Zutrittsberechtigung herbeigeführt werden.'

16. Nach § 54 Abs. 3 wird folgender Abs. 3a eingefügt:
'(3a) Die Vertrauensperson ist von der Sicherheitsbehörde zu führen und regelmäßig zu überwachen. Ihr Einsatz und dessen nähere Umstände sowie Auskünfte und Mitteilungen, die durch sie erlangt werden, sind zu dokumentieren (§ 13a), sofern diese für die Aufgabenerfüllung von Bedeutung sein können. § 54a gilt für verdeckte Ermittlungen durch Vertrauenspersonen nicht.'

17. In § 54 Abs. 5 wird im ersten Satz vor der Wortfolge 'einer Zusammenkunft' die Wortfolge 'oder im Zusammenhang mit' eingefügt und der letzte Satz lautet:
'Die auf diese Weise ermittelten Daten dürfen auch zur Abwehr und Verfolgung gefährlicher Angriffe sowie zur Verfolgung strafbarer Handlungen in Angelegenheiten der Sicherheitsverwaltung, nach Art. III Abs. 1 Z 4 EGVG, § 3 AbzeichenG sowie § 3 Symbole-Gesetz, BGBl. I Nr. 103/2014, die sich im Zusammenhang mit oder während der Zusammenkunft ereignen, verwendet werden.'

18. In § 58b Abs. 2 erster Satz wird das Wort 'Asylverfahren' durch die Wortfolge 'Verfahren nach § 3 BFA-Verfahrensgesetz – BFA-VG, BGBl. I Nr. 87/2012,' ersetzt.

19. § 59 Abs. 2 lautet:
'(2) Jede Abfrage und Übermittlung personenbezogener Daten aus der Zentralen Informationssammlung und den übrigen Informationsverbundsystemen ist so zu protokollieren, dass eine Zuordnung der Abfrage oder Übermittlung zu einem bestimmten Organwalter möglich ist. Die Zuordnung zu einem bestimmten Organwalter ist bei automatisierten Abfragen nicht erforderlich. Von der Protokollierung gänzlich ausgenommen sind automatisierte Abfragen gemäß § 54 Abs.

4b, es sei denn, es handelt sich um einen Treffer. Die Protokollaufzeichnungen sind drei Jahre aufzubewahren und danach zu löschen.'

20. Nach § 75 Abs. 1 wird folgender Abs. 1a eingefügt:
'(1a) Die Sicherheitsbehörden sind ermächtigt, eine nach den Bestimmungen der StPO ermittelte Spur, die einer Person, die im Verdacht steht, eine mit gerichtlicher Strafe bedrohte vorsätzliche Handlung begangen zu haben, zugehört oder zugehören dürfte, und deren Ermittlung durch erkennungsdienstliche Maßnahmen erfolgen könnte (§ 64 Abs. 2), zum Zweck ihrer Zuordnung zu einer Person in der Zentralen erkennungsdienstlichen Evidenz zu verarbeiten. Zur Spur dürfen auch Verwaltungsdaten verarbeitet werden. Die Daten sind zu löschen, wenn der für die Speicherung maßgebliche Verdacht nicht mehr besteht oder der bezughabende Akt im Dienste der Strafrechtspflege zu löschen ist (§ 13a Abs. 2).'

21. In § 75 Abs. 2 wird im ersten Satz nach der Wortfolge 'zu benützen' die Wortfolge 'und zu vergleichen' eingefügt, im zweiten Satz vor dem Wort 'Übermittlungen' die Wortfolge 'Abfragen und' eingefügt sowie das Zitat 'Abs. 1' durch das Zitat 'Abs. 1 und 1a' ersetzt.

22. Nach § 80 Abs. 1 wird folgender Abs. 1a eingefügt:
'(1a) Sofern Auskunft über die gemäß § 75 Abs. 1a verarbeiteten Daten begehrt wird, sind die Sicherheitsbehörden ermächtigt, gegen Kostenersatz (Abs. 1 letzter Satz) vom Auskunftswerber Abbildungen oder Papillarlinienabdrücke herzustellen oder seine DNA zu ermitteln, und diese Daten mit den gemäß § 75 Abs. 1a verarbeiteten Daten zu vergleichen. Von der Erteilung der Auskunft ist abzusehen, wenn der Auskunftswerber an der Ermittlung dieser Daten nicht mitgewirkt oder er den Kostenersatz nicht geleistet hat. Die aus Anlass des Auskunftsverlangens ermittelten Daten über den Auskunftswerber sind gesondert zu verwahren und dürfen innerhalb eines Zeitraums von einem Jahr, im Falle der Erhebung einer Beschwerde gemäß § 31 DSG 2000 an die Datenschutzbehörde bis zum rechtskräftigen Abschluss des Verfahrens, nicht vernichtet werden.'

23. In § 91a Abs. 1 werden das Wort 'zwei' durch die Wortfolge 'der erforderlichen Anzahl von' und die Wortfolge 'nach dem Sicherheitspolizeigesetz' durch die Wortfolge 'auf dem Gebiet der Sicherheitspolizei' ersetzt.

24. § 91a Abs. 2 lautet:
'(2) Der Rechtsschutzbeauftragte und seine Stellvertreter haben gleiche Rechte und Pflichten. Im Bereich des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz – PStSG, BGBl. I Nr. 5/2016) haben sie sich regelmäßig über ihre Wahrnehmungen zu unterrichten und in grundsätzlichen Fragen der Aufgabenerfüllung eine einvernehmliche Vorgangsweise anzustreben. Sie werden vom Bundespräsidenten auf Vorschlag der Bundesregierung nach Anhörung der Präsidenten des Nationalrates sowie der Präsidenten des Verfassungsgerichtshofes und des Verwaltungsgerichtshofes auf die Dauer von fünf Jahren bestellt. Wiederbestellungen sind zulässig. Zumindest bei einem Stellvertreter muss es sich um eine Person handeln, die als Richter oder Staatsanwalt mindestens zehn Jahre tätig war und nicht gemäß § 91b Abs. 1 zweiter Satz ausgeschlossen ist. Der

Rechtsschutzbeauftragte hat gemeinsam mit seinen Stellvertretern nähere Regelungen zu ihrem Zusammenwirken, insbesondere über die Vertretung des Rechtsschutzbeauftragten im Verhinderungsfall, die Einberufung von Sitzungen, die Zusammensetzung des Rechtsschutzsenates (§ 14 Abs. 3 PStSG) sowie dessen Entscheidungsfindung in einer Geschäftsordnung zu treffen.'

25. § 91b Abs. 3 lautet:
'(3) Der Bundesminister für Inneres stellt dem Rechtsschutzbeauftragten und seinen Stellvertretern die zur Bewältigung der administrativen Tätigkeit notwendigen Personal- und Sacherfordernisse zur Verfügung, wobei diese den jeweiligen gesetzlichen Aufgaben adäquat anzupassen sind. Zur Gewährung der Unabhängigkeit sind dem Rechtsschutzbeauftragten Büroräumlichkeiten außerhalb des Raumverbundes der Generaldirektion für die öffentliche Sicherheit oder einer ihr nachgeordneten Sicherheitsbehörde zur Verfügung zu stellen. Dem Rechtsschutzbeauftragten und seinen Stellvertretern gebührt für die Erfüllung ihrer Aufgaben eine Entschädigung. Der Bundesminister für Inneres ist ermächtigt, mit Verordnung Pauschalsätze für die Bemessung dieser Entschädigung festzusetzen.'

26. In § 91c Abs. 1 wird im ersten Satz das Zitat '(§ 54 Abs. 3)' durch das Zitat '(§ 54 Abs. 3 und 3a)' ersetzt, es entfällt der zweite Satz und es wird das Wort 'Kennzeichnerkennungsgeräten' durch das Wort 'Kennzeichenerkennungsgeräten' ersetzt.

27. § 91d Abs. 1 letzter Satz lautet:
'Dies gilt jedoch nicht für Auskünfte über die Identität von Personen nach Maßgabe des § 162 StPO.'

28. In § 91d wird in Abs. 3 der Satz 'In einem solchen Verfahren vor der Datenschutzbehörde ist auf § 26 Abs. 2 DSG 2000 über die Beschränkung des Auskunftsrechtes Bedacht zu nehmen.' angefügt; in Abs. 4 wird der Strichpunkt durch einen Punkt ersetzt und es entfällt die Wortfolge 'insbesondere ist darin auf Ermächtigungen nach § 91c Abs. 3 Bezug zu nehmen.'.

29. Dem § 94 werden folgende Abs. 38 und 39 angefügt:
'(38) Die §§ 13a Abs. 3, 20, 21 Abs. 2a, die Überschrift des § 25, die §§ 54 Abs. 5, 58b Abs. 2, 59 Abs. 2, 75 Abs. 1a und 2, 80 Abs. 1a sowie der Eintrag im Inhaltsverzeichnis zu § 25 in der Fassung des Bundesgesetzes BGBl. I Nr. 5/2016 treten mit 1. März 2016 in Kraft.
(39) Die §§ 6 Abs. 1, 53 Abs. 1, 3, 3b, 4 und 5, 53a Abs. 1, 1a und 5a, 54 Abs. 2, 3, 3a und 4, 91a Abs. 1 und 2, 91b Abs. 3, 91c Abs. 1, 91d Abs. 1, 3 und 4, 96 Abs. 8 und 9 sowie das Inhaltsverzeichnis in der Fassung des Bundesgesetzes BGBl. I Nr. 5/2016 treten mit 1. Juli 2016 in Kraft. Gleichzeitig treten die §§ 21 Abs. 3, 63 Abs. 1a und 1b, 91c Abs. 3 und 93a samt Überschrift außer Kraft.'

30. Dem § 96 werden folgende Abs. 8 und 9 angefügt:
'(8) Daten, die auf Grundlage des § 53a Abs. 1 in der Fassung vor BGBl. I Nr. 5/2016 für den Personen- und Objektschutz bis zum Zeitpunkt des Inkrafttretens

des Bundesgesetzes BGBl. I Nr. 5/2016 verarbeitet wurden, dürfen auf Grundlage des § 53a Abs. 1a in der Fassung BGBl. I Nr. 5/2016 weiterverarbeitet sowie unter den Voraussetzungen des § 53a Abs. 5a in der Fassung BGBl. I Nr. 5/2016 auch im Informationsverbundsystem geführt werden.
(9) § 91a Abs. 2 fünfter Satz in der Fassung des Bundesgesetzes BGBl. I Nr. 5/2016 kommt bei Neu- oder Wiederbestellung eines Stellvertreters des Rechtsschutzbeauftragten nach Inkrafttreten des Bundesgesetzes BGBl. I Nr. 5/2016 zur Anwendung.'

31. Dem § 97 wird folgender Abs. 4 angefügt:
'(4) § 13a Abs. 3 in der Fassung des Bundesgesetzes BGBl. I Nr. 5/2016 tritt mit Ablauf des 31. Dezember 2019 außer Kraft.'"

## III. Antragsvorbringen und Verfahren

1. Zur Begründung ihres Antrags führen die Antragsteller unter dem Punkt "Darlegung der Bedenken" wörtlich zunächst Folgendes aus (Zitat ohne im Original enthaltene Hervorhebungen): 4

"Dieses Kapitel enthält in erster Linie die Argumentation jener Bedenken, die insbesondere dem primären Antrag zu 1. (siehe Kapitel 2. und 8.) sowie den eventualiter gestellten Anträgen zu 2., 3., 4. und 5. mit dem Ziel der Aufhebung des gesamten PStSG in verschiedenen Varianten zugrunde liegen. Die Reihenfolge der Anträge entspricht dabei der Präferenzhierarchie der Antragsteller/innen. Die Eventualanträge werden aus anwaltlicher Vorsicht gestellt und sind in der Reihenfolge gegenüber dem vorhergehenden (Eventual)Antrag jeweils im Umfang eingeschränkt. Damit wird antizipiert, dass der hohe Verfassungsgerichtshof den 'Sitz der Verfassungswidrigkeit' unterschiedlich beurteilen mag, je nach dem, welchen Argumenten konkret gefolgt wird. Wie sich die Anträge substanziell unterscheiden, ist oben in Kapitel 2 übersichtlich dargestellt.

Außerdem bezieht sich das Vorbringen in diesem Kapitel auch auf die Eventualanträge zu 6. und 7., mit denen nur einzelne Bestimmungen des PStSG und des SPG bekämpft werden, für den Fall, dass dem hohen Verfassungsgerichtshof die Argumente für eine Gesamtaufhebung des PStSG nicht ausreichend erscheinen sollten. Die hier dargelegten Bedenken sind für die Anfechtung einzelner Bestimmungen insbesondere dahingehend relevant, als hier bereits der Eingriff in den Schutzbereich der auch im Einzelnen geltend gemachten Grundrechte argumentiert wird.

6.1 Verletzung verfassungsgesetzlich gewährleisteter Rechte (§ 1 DSG 2000, Art 8, 10 und 13 EMRK, Art 18 und Art 7 B-VG)

Zur Vermeidung redundanter Ausführungen bei gleichzeitiger Wahrung der gebotenen Präzision werden hier einige Ausführungen zur Begründung der verfassungsrechtlichen Bedenken vorangestellt, die für die einzelnen Antragsgegenstände in

der Folge gleichermaßen gelten. Damit soll vor allem vermieden werden, dass der Text der vorliegenden Beschwerde durch sich wiederholende Ausführungen zum Eingriff in den Schutzbereich der verschiedenen Grundrechte oder durch eine ausführliche Gliederung bei der Verhältnismäßigkeitsprüfung unnötig lang und kompliziert wird.

Für die zur Prüfung vorgelegten Normen gilt grundsätzlich, dass sie entweder für sich oder im Zusammenwirken einen Eingriff

- in das Datenschutzgrundrecht gemäß § 1 DSG 2000,
- in den Schutz der Privatsphäre nach Art 8 EMRK,
- in den Schutz der Meinungs- und Informationsfreiheit nach Art 10 EMRK,
- in das (akzessorische) Recht auf einen effektiven Rechtsschutz nach Art 13 EMRK,
- in das Fernmeldegeheimnis nach Art 10a Staatsgrundgesetz 1867 (StGG)

weiters eine Verletzung

- des rechtsstaatlichen Prinzips (Art 18 B-VG) sowie
- des Gleichheitsgrundsatzes nach Art 7 B-VG

bewirken.

Das Polizeiliche Staatsschutzgesetz sowie die im Zusammenhang stehenden und ebenfalls bekämpften Normen des SPG etablieren ein System der Befugnisse zur Ermittlung, Sammlung und Weiterverarbeitung von personenbezogenen Informationen und Daten zu Verdächtigen und deren Kontakt- und Begleitpersonen. Die verschiedenen Ermittlungsmethoden (zB Observation, verdeckte Ermittlung, Einsatz von Bild- und Tonaufzeichnungsgeräten, Kennzeichenerkennungsgeräten, Auskünfte zu Anschlussinhabern und Nutzern von Internetdiensten) sind dabei nicht grundsätzlich neu sondern finden sich bereits in der Strafprozessordnung und im Sicherheitspolizeigesetz. Das PStSG stattet die für den Staatsschutz zuständigen Sicherheitsbehörden nun konzentriert mit all diesen Ermittlungsinstrumenten unter wesentlich erleichterten Voraussetzungen ohne gerichtliche Kontrolle und mit einer neuen zentralen Datenanwendung aus. Gleichzeitig wird der Bereich der Prävention — in Abgrenzung zur 'Abwehr gefährlicher Angriffe' nach § 21 SPG — noch weiter als bisher in das Vorfeld krimineller Aktivitäten verlagert, während der Kreis der Betroffenen durch flexible Gesetzesbegriffe weiter ausgedehnt wird und der Rechtsschutz unzureichend ausgestaltet ist.

'Überwachungs-Gesamtrechnung':

Für die Beurteilung der Zulässigkeit der gesetzlich normierten Grundrechtseingriffe ist dabei wesentlich, dass eine isolierte Betrachtung einzelner Befugnisse nicht ausreicht. Vielmehr sind einerseits die konkreten Ermittlungs- und Eingriffsbefugnisse in Zusammenschau mit den Tatbeständen des materiellen Strafrechts (die hier nicht angefochten werden) sowie mit komplementären und überlappenden Befugnissen derselben Organe nach anderen Gesetzen (StPO, SPG) zu sehen.

Andererseits sind auch die verfügbaren Technologien, deren mehr oder weniger präzise gesetzliche Erfassung sowie deren Eignung für Grundrechtseingriffe zu berücksichtigen.

Das deutsche Bundesverfassungsgericht hat in dessen Urteil zur Aufhebung der nationalen Umsetzung der Vorratsdatenspeicherung in Deutschland ausgeführt, dass eine staatliche Überwachungsmaßnahme bzw. deren Verhältnismäßigkeit nur beurteilt werden kann, wenn man diese in Zusammenschau mit anderen, bereits bestehenden Befugnissen betrachtet. Durch die Summe aller Eingriffe könne sich ergeben, dass der Spielraum des Gesetzgebers zur Normierung neuer Befugnisse enger wird. […] Damit beschreibt das dt. Bundesverfassungsgericht im Prinzip die Notwendigkeit einer Art 'Überwachungs-Gesamtrechnung'[…].

§ 1 DSG 2000 garantiert im ersten Satz:

'Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht.'

Das gesamte System des PStSG und der komplementären Vorschriften des SPG besteht vor allem aus Rechtsnormen zur Ermittlung personenbezogener Daten und kulminiert letztlich in einer zentralen Datenanwendung. Der Eingriff in das Datenschutzgrundrecht liegt aber nicht erst in der (automatisierten) Verarbeitung personenbezogener Daten, vielmehr erfasst § 1 DSG 2000 auch das bloße Ermitteln solcher Daten und nicht erst eine allenfalls automationsunterstützte Weiterverarbeitung in einer Datenanwendung.

Art 8 EMRK garantiert:

'Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.'

Ein System geheimer Überwachungs- und Ermittlungsbefugnisse zur Wahrung der nationalen Sicherheit ist auch nach ständiger Rechtsprechung des EGMR zweifellos an den Vorgaben des Art 8 EMRK zu messen. Zuletzt hat der EGMR in der Rechtssache Szabó und Vissy v. Ungarn […] das zentrale Risiko eines solchen Systems auf den Punkt gebracht:

'In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse.'[…]

Schon kurz zuvor hat der EGMR in der Rechtssache Roman Zakharov v. Russland[…] strikte Eingrenzungskriterien beschrieben und verlangt dabei

'(...) reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing

or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security.'[…]

Um dies sicherzustellen, verlangt der Gerichtshof die folgenden Mindestsicherungen, die ausdrücklich im kodifizierten Recht angeordnet werden müssen, um Missbrauch zu vermeiden: das Wesen der Straftaten, die Anlass zu einem Abhörbeschluss geben können; eine Definition jener Personengruppen, deren Kommunikation überwacht werden kann; eine Begrenzung der Dauer einer solchen Überwachung; das Verfahren, nach dem bei der Untersuchung, Verwendung und Speicherung der erlangten Daten vorgegangen wird; die Schutzmaßnahmen, die zur Anwendung kommen, wenn die Daten an Dritte übertragen werden; und die Umstände, unter denen die erlangten Daten gelöscht oder die Aufnahmen vernichtet werden können oder müssen.[…]

Für den Fall einer Informationssammlung und -speicherung durch einen Geheimdienst wurde ähnlich entschieden, dass nämlich 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.

Hierzu lässt sich einwenden, dass das PStSG ja grundsätzlich zu diesen Kriterien Regelungen vorsieht und daher keine Vergleichbarkeit zB mit den zitierten EGMR Entscheidungen Szabó und Vissy v. Ungarn sowie Zakharov v. Russland besteht, weil es in diesen Fällen weitgehend an entsprechenden Regeln im jeweiligen nationalen Recht überhaupt gefehlt hat. Diesem Einwand ist zu entgegnen, dass die fraglichen Regelungen des PStSG zwar vorhanden, aber — wie in der Folge zu zeigen ist — unklar, lückenhaft und nicht durch einen effektiven Rechtsschutz abgesichert sind. Damit ist die österreichische Rechtslage im Vergleich zwar auf dem Papier besser, dem vom EGMR intendierten Schutzzweck wird damit aber ebenso wenig Genüge getan.

Artikel 10 EMRK garantiert:

'Jedermann hat Anspruch auf freie Meinungsäußerung. Dieses Recht schließt die Freiheit der Meinung und die Freiheit zum Empfang und zur Mitteilung von Nachrichten oder Ideen ohne Eingriffe öffentlicher Behörden und ohne Rücksicht auf Landesgrenzen ein.'

Das PStSG normiert viele weitreichende Befugnisse zur Überwachung des Verhaltens und der Kommunikation, sowohl im Bereich der unmittelbar zwischenmenschlichen (zB § 11 Abs. 1 Z 1 bis 3) als auch der elektronischen Interaktion (zB § 11 Abs. 1 Z 5 und 7). Durch die gleichzeitig diffuse Eingrenzung des be-

troffenen Personenkreises und das schwache Kontroll- und Rechtsschutzsystem erwächst daraus die Gefahr, dass die Daten aus Kommunikationsverläufen behördlich aufgezeichnet und verwertet werden. Damit wird ein Klima geschaffen, in dem die Menschen sich bei der Äußerung der eigenen Meinung ebenso wie beim Konsum von Informationen zur Bildung einer eigenen Meinung auch bei völlig legalen Inhalten immer häufiger selbst beschränken, um mögliche nachteilige Folgen zu vermeiden. Diese Selbstbeschränkung bei der Ausübung der durch Art 10 EMRK garantierten Meinungs- und Informationsfreiheit wird auch als 'chilling-Effekt' bezeichnet.

In dieser Hinsicht hat der EGMR im Urteil Rotaru gg. Rumänien[…] erkannt, dass bereits eine einschüchternde Wirkung einen Eingriff in das Grundrecht bewirken kann. Der Eingriff in die Meinungs- und lnformationsfreiheit ist nicht direkt sondern indirekt und beruht auf einem empirischen Argument, zu dem es keine zwingenden Nachweise gibt. Es ist daher auch nicht das tragende Argument der vorliegenden Beschwerde.

Allgemeines zur Grundrechtsprüfung:

Der vorliegende Antrag folgt in seiner Logik dem klassischen Schema zur Prüfung der Verhältnismäßigkeit bei Grundrechtseingriffen. Geprüft wird, in welches verfassungsgesetzlich gewährleistete Recht durch die jeweils beleuchtete Norm eingegriffen wird.

Dem folgt die Frage, welchen (allenfalls mehreren) legitimen Zielen der Eingriff jeweils dienen soll und ob die gewählte Maßnahme geeignet ist, das jeweilige Ziel zu erreichen. Weiters wird geprüft, ob das gewählte Mittel in einer demokratischen Gesellschaft erforderlich ist oder ob gelindere Mittel zur Verfügung stehen, die angestrebten Ziele voraussichtlich im selben Maß zu erreichen.

Den Abschluss bildet die Prüfung der Adäquanz, bei der die Verhältnismäßigkeit im engeren Sinne einer eigentlichen Güterabwägung geprüft wird.

Diese Ebenen der Verhältnismäßigkeitsprüfung sind korreliert. Wenn zum Beispiel die Eignung eines Grundrechtseingriffs zur Zielerreichung abstrakt zwar durchaus fragwürdig aber nicht auszuschließen ist (Stichwort 'Vorsorgeprinzip'), bedarf es zur Adäquanz regelmäßig eines sehr hochwertigen Schutzgutes und möglichst konkreter Bedingungen. Die Ausführung der Bedenken zu den einzelnen Anträgen bauen jeweils auf Argumenten, die auf jede einzelne Ebene der Verhältnismäßigkeitsprüfung Auswirkungen zeigen. Die folgenden Ausführungen werden daher nur dann auf eine bestimmte dieser Ebenen besonders eingehen, wenn es für die Argumentation wesentlich ist.

6.2 Verletzung des rechtsstaatlichen Prinzips (Art 18 B-VG)

6.2.1 Eine zentrale Bedeutung kommt in diesem Antrag auf Normenkontrolle dem rechtsstaatlichen Prinzip zu.

Das rechtsstaatliche Prinzip kommt nach herrschender Auffassung insbesondere in der Gesetzesbindung der Vollziehung nach Artikel 18 B-VG zum Ausdruck. Für den Gesetzgeber ergibt sich daraus vor allem die Verantwortung, Normen hinreichend bestimmt und klar zu formulieren.

Pflichten und vor allem auch Rechte des/der Einzelnen müssen gesetzlich (möglichst) präzise geregelt sein und deren Durchsetzung durch entsprechende Institutionen garantiert sein. Durch die Bestimmtheit — genauer: Vorherbestimmtheit — der Rechte und Pflichten durch Gesetz unterscheidet sich der Rechtsstaat von seinem Gegenteil, dem Polizeistaat.

Der EGMR verlangt bei geheimen Überwachungsmaßnahmen, dass das Gesetz in seinen Bestimmungen hinreichend klar sein muss, um dem Bürger adäquate Hinweise über die Bedingungen und Umstände zu geben, unter denen die Behörden befugt sind, in das Recht auf Achtung des Privatlebens und des Briefverkehrs einzugreifen.' […] Im Hinblick auf das Missbrauchsrisiko, das jedem geheimen Überwachungssystem innewohnt, müssen solche Maßnahmen auf einem besonders präzisen Gesetz beruhen. Es ist notwendig, klare, detaillierte Bestimmungen in dieser Sache zu haben, insbesondere da die zur Verfügung stehende Technologie immer komplexer wird.[…]

6.2.2 Das der österreichischen Rechtsordnung immanente Konzept des 'Fehlerkalküls' (Adolf Julius Merkl) antizipiert, dass in der Praxis des Rechts Fehler unvermeidbar sind und daher entsprechende Rechtsschutzsysteme geschaffen werden müssen, um einen Rechtsstaat zu etablieren. In diesem Sinne ist auch das in Artikel 13 EMRK ausdrücklich verfassungsgesetzlich verankerte Gebot eines effektiven Rechtsschutzes eine wesentliche Säule des rechtsstaatlichen Prinzips.

Der Begriff 'rechtsstaatliches Prinzip' fand 1949 erstmals Eingang in die Begründung eines Erkenntnisses des VfGH. […] Schon drei Jahre später qualifizierte der VfGH das rechtsstaatliche Prinzip als leitenden Grundsatz der Bundesverfassung, dessen Abänderung als Gesamtänderung der Bundesverfassung zu qualifizieren ist:

'Dem rechtsstaatlichen Prinzip entspricht es, dass alle Akte staatlicher Organe im Gesetz und mittelbar letzten Endes in der Verfassung begründet sein müssen, und dass für die Sicherung dieses Postulates wirksame Rechtsschutzeinrichtungen bestehen'.[…]

Das Gebot des effektiven Rechtsschutzes blieb die zentrale Konstante in der Rechtsstaatsjudikatur des VfGH[…].

6.2.3 Das Polizeiliche Staatsschutzgesetz weist an neuralgischen Punkten auf beiden Ebenen — jener der hinreichenden Normenbestimmtheit und jener des effektiven Rechtsschutzes — schwere Mängel auf.

Einerseits sind zentrale Begriffe wie 'Gruppierung' (§ 6 Abs.1 Z 1), 'ideologisch motivierte Kriminalität' (§ 1 Abs.2; vgl. auch (§ 6 Abs. 2 Z 2) oder 'ideologisch motivierte Gewalt' (§ 6 Abs.1 Z 1) nicht hinreichend bestimmt, obwohl diese Normenbestandteile wesentliche Voraussetzungen für Grundrechtseingriffe beschreiben. Andererseits bestehen im Rechtsschutzsystem massive Lücken, sodass gleichzeitig eine geringe Chance besteht, dass das Problem der unbestimmten Begriffe im Rahmen effektiver Rechtsschutz- und Kontrollmechanismen kompensiert wird. Die umfangreichen Befugnisse der Staatsschutzorgane sind schon bei abstrakten Gefährdungslagen — unterhalb der Schwelle eines 'gefährlichen Angriffs' (§ 16 SPG) — anwendbar und werden vom Rechtsschutzbeauftragten (RSB) beim Bundesministerium für Inneres für bis zu sechs Monaten im Voraus bewilligt.

Diese Bewilligung wird entweder in Bezug auf eine bestimmte Person oder auf eine Gruppierung erteilt. Es liegt im Ermessen der 'Staatschutzorgane' (Organisationseinheiten nach § 1 Abs.3 PStSG), welche Personen in der Folge einer solchen Gruppierung zugerechnet werden oder als Kontakt- und Begleitpersonen nicht nur zufällig mit der Gruppierung in Verbindung stehen und daher Subjekt der Überwachung werden. Ermächtigungen können jeweils um weitere sechs Monate auch mehrfach verlängert werden, solange dies 'zur Erfüllung der Aufgabe voraussichtlich erforderlich ist' (§ 14 Abs. 1 PStSG). Die (grundsätzlich gebotene) 'Information' bestimmter Betroffener kann mit Zustimmung des Rechtsschutzbeauftragten aufgeschoben werden, solange durch sie die Aufgabenerfüllung gefährdet wäre' (§ 16 Abs. 3 PStSG).

Die von der Rechtsprechung des VfGH geforderte faktische Effektivität des Rechtsschutzes wird sohin unterlaufen. In seinem Erkenntnis VfSlg 11.196/1986 führte der VfGH Grundsätzliches zu dieser Problemstellung aus, weshalb bezogen auf die gegenständlichen Prüfungsanträge ein ausführliches Zitat notwendig erscheint:

'Der VfGH kann von seiner im Prüfungsbeschluss bezogenen ständigen Judikatur zum rechtsstaatlichen Prinzip ausgehen (...). Ihr zufolge gipfelt der Sinn des rechtsstaatlichen Prinzips darin, dass alle Akte staatlicher Organe im Gesetz und mittelbar letzten Endes in der Verfassung begründet sein müssen und ein System von Rechtsschutzeinrichtungen die Gewähr dafür bietet, dass nur solche Akte in ihrer rechtlichen Existenz als dauernd gesichert erscheinen, die in Übereinstimmung mit den sie bedingenden Akten höherer Stufe erlassen wurden. Der Gerichtshof bleibt auch bei der im Einleitungsbeschluss an diese Annahme geknüpften Annahme, dass die hier unabdingbar geforderten Rechtsschutzeinrichtungen ihrer Zweckbestimmung nach ein bestimmtes Mindestmaß an faktischer Effizienz für den Rechtsschutzwerber aufweisen müssen. Zunächst ist hierzu die Klarstellung geboten, dass von faktischer Effizienz deshalb die Rede ist, weil unter Effizienz allein unter Umständen bloß das letzten Endes bewirkte Erreichen einer Entscheidung rechtsrichtigen Inhalts durch das Ergreifen von Rechtsbehelfen verstanden werden könnte, nicht aber auch die mitgemeinte Übersetzung einer solchen Entscheidung in den Tatsachenbereich. 'Schutz' als Teilaspekt des Ausdrucks 'Rechtsschutz' ist auf den Rechtsunterworfenen bezogen und meint nicht

zuletzt die — rechtzeitige — Wahrung und Gewährleistung einer faktischen Position, weshalb Rechtsschutzeinrichtungen diesen Zweck notwendig in sich schließen. Der VfGH hält im Hinblick auf diesen Inhalt des Begriffes Rechtsschutzeinrichtung, mithin insbesondere des Begriffs Rechtsbehelf, auch an der Ansicht fest, dass es nicht angeht, den Rechtsschutzsuchenden generell einseitig mit allen Folgen einer potenziell rechtswidrigen behördlichen Entscheidung solange zu belasten, bis sein Rechtsschutzgesuch endgültig erledigt ist. Zu berücksichtigen ist in diesem Zusammenhang allerdings nicht nur seine Position, sondern auch – Zweck und Inhalt der Regelung, ferner die Interessen Dritter sowie schließlich das öffentliche Interesse. Der Gesetzgeber hat unter diesen Gegebenheiten einen Ausgleich zu schaffen, wobei aber dem Grundsatz der faktischen Effektivität eines Rechtsbehelfs der Vorrang zukommt und dessen Einschränkung nur aus sachlich gebotenen, triftigen Gründen zulässig ist.'

Diesen Grundgedanken bekräftigte der VfGH in seiner Entscheidung VfSlg 13.182/1992, in der er ausführte, dass

'... gesetzliche Regelungen, die sachlicherweise dazu führen, dass ein behördliches Fehlverhalten vorläufig hingenommen werden muss, (...) – wenn es irgendwie vermeidbar ist –, nicht so ausgestaltet werden (dürfen), dass daraus endgültige Belastungen entstehen'.

6.2.4 Die Kombination aus der mangelnden Bestimmtheit wichtiger Eingriffsvoraussetzungen und dem schwachen Rechtsschutz erzeugt ein hohes Risiko, dass das dichte Netz der Überwachungsbefugnisse (siehe den Übelblick sogleich) über immer weitere Teile der Bevölkerung ausgeworfen wird. Die in der Vergangenheit öffentlich bekannt gewordenen Beispiele, bei denen die Kriminalpolizei nach der StPO gegen Tierschützer des VGT […] oder das BVT gegen Mitglieder der studentischen Protestbewegung 'Uni Brennt' wegen Mitgliedschaft zu einer kriminellen Organisation bzw. einer terroristischen Vereinigung (§§ 278a und 278b StGB) ermittelt haben, zeigen, dass dieses Risiko sehr real und naheliegend ist.

Die Organisationseinheiten nach § 1 Abs. 3 PStSG, im Folgenden als 'Staatsschutzorgane' bezeichnet, dürfen dabei fast alles, was der Kriminalpolizei nach der StPO an Befugnissen zur Verfügung steht, allerdings ohne die Anordnung der Staatsanwaltschaft oder eine Bewilligung des Gerichts zu benötigen. Die Befugnisse des SPG stehen den Staatsschutzorganen gemäß § 5 PStSG ausdrücklich zur Verfügung und werden vor allem in den §§ 10 und 11 PStSG teilweise für die Staatsschutzorgane redundant normiert und teilweise erweitert. Die Auskunftspflichten sämtlicher Körperschaften des öffentlichen Rechts und deren Anstalten gegenüber den Staatsschutzorganen (§ 10 Abs. 3) kumulieren gemeinsam mit den Ergebnissen aus allen Ermittlungsbefugnissen nach dem PStSG und einem praktisch uneingeschränkten Zugang zu Daten, die nach dem SPG oder der StPO ermittelt wurden (§ 12 Abs. 1 vorletzter Satz), schließlich in einer neuen Datenanwendung nach § 12 Abs. 1.

Diese Datenanwendung darf vom BVT als Informationsverbundsystem zwischen dem Bundesminister für Inneres und den Landespolizeidirektionen zum Zweck der Bewertung von wahrscheinlichen Gefährdungen sowie zum Erkennen von Zusammenhängen und Strukturen mittels operativer oder strategischer Analyse betrieben werden.

Bei einigen Anfechtungsgegenständen wird geltend gemacht, dass die zu prüfenden Normen das in Artikel 18 B-VG garantierte Rechtsstaatsprinzip und/oder das Gebot des effektiven Rechtsschutzes nach Artikel 13 EMRK in Verbindung mit Artikel 8 EMRK verletzen. Die behauptete Verletzung des Artikel 18 B-VG entsteht aus zwei verschiedenen mit einander verzahnten Problemen im Hinblick auf die Gesetzesbindung der Vollziehung: Einerseits enthalten die relevierten Normen vor allem zu den Eingriffsvoraussetzungen viele unbestimmte Gesetzesbegriffe ('Gruppierung', 'ideologisch motivierte Kriminalität' bzw. 'ideologisch motivierte Gewalt'). Andererseits besteht kein zuverlässiges und effektives System zur Kontrolle und zum Rechtsschutz, welches geeignet wäre, die – bis zu einem gewissen Grad schwer zu vermeidende – Unschärfe wichtiger Begriffe zu kompensieren und in der Praxis zur notwendigen Konkretisierung bzw. Eingrenzung zu führen.

6.3 Verletzung des Rechtsstaatsgebots durch das PStSG als (schleichende) Gesamtänderung der Bundesverfassung im Sinne von Art 44 Abs. 3 B-VG

6.3.1 In der österreichischen Verfassungsordnung findet sich der Begriff des 'Rechtsstaates' nicht, er lässt sich sohin anhand des positiven Verfassungsrechts nicht definieren. Außer Frage steht, dass das rechtsstaatliche Prinzip als Grundprinzip der Bundesverfassung in der Judikatur des VfGH und in der Lehre (letztlich) unbestritten ist.

Ungeklärt ist hingegen die Frage der Reichweite des normativen Gehalts der verfassungsrechtlichen Grundordnung - dh die Definition jener 'Rechtsschicht', deren Abänderung oder Verletzung als Gesamtänderung der Bundesverfassung gemäß Art 44 Abs.3 B-VG der Zustimmung (auch) durch das Bundesvolk bedarf.

Unstrittig ist jedenfalls, dass das rechtsstaatliche Grundprinzip unter dem erhöhten Bestandsschutz des Art 44 Abs.3 B-VG steht – es ist sohin der Disposition sowohl des einfachen als auch des Verfassungsgesetzgebers entzogen.

6.3.2 Wie oben in Punkt 6.2 ausgeführt, verletzen zahlreiche der angefochtenen Normen des PStSG sowie des SPG bzw die darauf basierenden potenziellen Vollziehungsakte das Rechtsstaatsprinzip. Sie sind deshalb – wie beantragt – wegen Verfassungswidrigkeit aufzuheben.

Tatsächlich erweisen sich aber sämtliche tragenden Bestimmungen des PStSG wegen Verletzung des Rechtsstaatsprinzips als verfassungswidrig, sodass durch die Aufhebung einzelner Bestimmung des PStSG alleine ein verfassungskonformer Zustand gar nicht hergestellt werden kann. Das gilt logisch vor allem dort, wo die Verfassungswidrigkeit nicht durch eine positive Bestimmung oder Wort-

folge sondern durch eine Unterlassung des Gesetzgebers bewirkt wird, weil der hohe Verfassungsgerichtshof hier als 'negativer Gesetzgeber' an Gestaltungsgrenzen stößt.

Der verfassungsmäßige Zustand kann letztlich nur durch Aufhebung des gesamten PStSG wegen Verfassungswidrigkeit schon seines Konzeptes wiederhergestellt werden, da nach Aufhebung der zentralen Bestimmungen des PStSG, welche die Verfassungswidrigkeit begründen, ein der Vollziehung zugängliches Gesetz nicht mehr vorliegen würde.

6.3.3 Durch die Summe der schwerwiegenden Verletzungen des Rechtsstaatsprinzips durch die angefochtenen Normen des PStSG sowie des SPG bzw. die darauf basierenden potenziellen Vollziehungsakte erweist sich das Bundesgesetz vom 26.02.2016, BGBl. I Nr. 5/2016 aber auch als Gesamtänderung der österreichischen Bundesverfassung im Sinne von Art 44 Abs.3 B-VG.

Die nachstehend in den Punkten 6.4 und 7. dargestellten rechtsstaatlichen Defizite können dazu führen, dass der Kreis der Betroffenen immer weiter ausgedehnt wird (und theoretisch binnen weniger Jahre einen relevanten Teil der österreichischen Bevölkerung ausmachen kann) und gleichzeitig keine wirksamen Kontroll- und Rechtsschutzmechanismen bestehen, mit denen solche Tendenzen effektiv zurückgedrängt werden (können).

Um dies zu veranschaulichen: Der Rechtsschutzbeauftragte kann zwar überprüfen, welche Daten konkret in den Datenanwendungen gespeichert sind. Er hat aber keine Befugnis zu prüfen, was die Datenanwendungen rund um das Informationsverbundsystem gemäß §§ 12 PStSG und § 53a Abs. 5a SPG an Verknüpfungsarbeit leisten können und welche Informationen dabei abgeleitet werden können (durch sog. 'Data-Mining'), ohne dabei neue Datenbankeinträge zu schaffen, die dann wieder der Kontrolle des RSB unterliegen. Es ist keine Art der Kontrolle vorgesehen, durch welche effektiv überprüft würde, ob die von § 10 Abs. 2 PStSG geforderte Abgrenzung zur Rasterfahndung nach § 141 StPO bei der technischen Umsetzung auch erfüllt wird.

6.3.4 Der VfGH hat sich bereits 1988 — abstrakt — mit dem Problem einer 'schleichenden' Gesamtänderung der Bundesverfassung beschäftigt:

'Der Verfassungsgerichtshof bleibt bei seinem in der bisherigen _Judikatur (zuletzt VfGH 23.06.88, V 29/88 u.a.) eingenommenen Standpunkt, dass — angesichts der Verpflichtung zur baugesetzkonformen Interpretation (vgl. etwa VfGH 01.07.87, G 78/87) — einer Verfassungsbestimmung im Zweifel kein Inhalt beizumessen ist, der sie in Widerspruch zu den leitenden Grundsätzen des Bundesverfassungsrechts (Art 44 Abs. 3 B-VG) stellen würde. Zu einem solchen Widerspruch könnten Eingriffe in die Grundprinzipien *der* Bundesverfassung, wie etwa eine Einschränkung der Gesetzesprüfungskompetenz des Verfassungsgerichtshofes oder eine Durchbrechung der Grundrechtsordnung, nicht nur führen, wenn schwerwiegende und umfassende Eingriffe in die Grundprinzipien vorgenommen werden; vielmehr können auch bloß partiell wirkende Maßnahmen —

gehäuft vorgenommen — im Effekt zu einer Gesamtänderung der Bundesverfassung führen (vgl. VfGH 23.06.88, V 29/88 u.a.)'[…]

Insbesondere unter dem Aspekt einer 'Überwachungs-Gesamtrechnung' erweist sich das durch das Bundesgesetz vom 26.02.2016, BGBl. I Nr. 5/2016 Erlassene als partiell wirkende Maßnahmen im Sinne von VfSlg 11.829, die im Ergebnis bzw. in Summe mit den zahlreichen seit dem 11.09.2001 erlassenen Überwachungsnormen zu einer 'schleichenden Gesamtänderung' der österreichischen Bundesverfassung im Sinne von Art 44 Abs. 3 B-VG geführt haben (könnten).

6.4 Ineffektivität des Rechtsschutzsystems

Die in diesem Antrag vorgebrachten verfassungsrechtlichen Bedenken gegen das Polizeiliche Staatsschutzgesetz basieren vielfach auf dem Argument eines mangelhaften Rechtsschutzes, in dessen Zentrum die Institution des Rechtsschutzbeauftragten (RSB) beim Bundesministerium für Inneres (BM.I) steht. Zur Vermeidung von Missverständnissen sei vorausgeschickt, dass sich diese Kritik nicht auf den aktuellen Organwalter bezieht, der im Hinblick auf seine Integrität und seine rechtsstaatlichen Intentionen über jeden Zweifel erhaben ist, sondern vielmehr auf die Ausgestaltung seiner Befugnisse, seiner Organisation und seiner Ausstattung.

Die Geltendmachung von Rechtsschutzmängeln ist im abstrakten Normenkontrollverfahren vor dem Verfassungsgerichtshof, wenn es darum geht, den Sitz der Verfassungswidrigkeit zu bestimmen, eine besondere Herausforderung. Im Zusammenhang mit Rechtsschutz- und Kontrollaufgaben ist bekanntlich eine mangelhafte Norm für den Grundrechtsschutz besser als gar keine. Eine Aufhebung einer Norm, die zwar Rechtsschutz bietet, aber eben zu wenig, würde die argumentierte Verletzung verfassungsgesetzlich gewährleisteter Rechte nicht beseitigen. Nur wenn der Eingriff durch eine (abgrenzbare) positive Vorschrift im Rahmen der Rechtsschutzregelung bewirkt wird, kann deren Aufhebung den verfassungsmäßigen Zustand herstellen (siehe zB unten § 15 Abs. 1 letzter Satz PStSG). In allen anderen Fällen gibt es zwei Optionen:

1. Die mangelhaften rechtsstaatlichen Absicherungen in den Bereichen Rechtsschutz und Kontrolle sind ein systematisches Problem, sodass selbst bei Aufhebung einzelner, bestimmter Befugnisse die Verfassungswidrigkeit weiters besteht und nur die Aufhebung des gesamten Gesetzes den rechtmäßigen Zustand herstellt.

2. Die Rechtsschutzdefizite führen dazu, dass die Ausübung einzelner, bestimmter Befugnisse keiner hinreichenden Kontrolle unterliegen und daher die Befugnis selbst als unverhältnismäßig zu sehen ist, weil es keine (hinreichende) Absicherung gibt, dass die Befugnis auch in der Vollzugspraxis im Rahmen der (normativ allenfalls gegebenen) Verhältnismäßigkeit bleibt.

Im vorliegenden Antrag werden beide Varianten argumentiert, wobei Option 1. das primäre Antragsbegehren wesentlich stützt. Bei der — eventualiter bean-

tragten — Anfechtung einzelner Befugnisse wird regelmäßig auf die hier bereits argumentierten Rechtsschutzdefizite im Sinne der Option 2. verwiesen. Besonderheiten in dieser Hinsicht aus der konkreten Befugnis werden jeweils ausdrücklich argumentiert, insbesondere bei Vergleichen zum jeweiligen Rechtsschutz bei einer verwandten oder gleichen Bestimmung nach der StPO.

6.4.1. Kritik an den Befugnissen des RSB – Rechtsschutzdefizite

6.4.1.1 Akteneinsicht

Das in der Rechtsordnung zum Ausdruck kommende Vertrauen in den RSB ist angesichts der Zwillingsbestimmungen des § 91d Abs 1 letzter Satz SPG sowie des § 15 Abs. 1 letzter Satz PStSG begrenzt. Der erste Satz gewährt in beiden Bestimmungen dem Kontrollorgan zunächst volle Einsicht in alle Akten ohne Beschränkung durch das Amtsgeheimnis. Dem folgt jeweils im letzten Satz eine ebenso diffuse wie massive Einschränkung. Erwähnenswert ist dabei zunächst die Variante des § 91d Abs. 1 letzter Satz SPG in der Fassung vor der Novelle BGBl. I Nr. 5/2016 — also der zum Zeitpunkt der Einbringung dieses Antrags geltenden Rechtslage:

[…]

Diese Ausnahme von der Akteneinsicht kann logisch nur so verstanden werden, dass eine Gefahr für die nationale Sicherheit oder für Menschenleben gerade dadurch ausgelöst wird, dass der Rechtsschutzbeauftragte Kenntnis von bestimmten Informationen erhält. Nimmt man nicht an, dass die Gefahr vom RSB selbst ausgeht, kann damit logisch gesehen nur das Risiko adressiert sein, dass solche Informationen durch den RSB an Dritte weitergegeben werden, unter Begehung eines gerichtlich strafbaren Amtsmissbrauchs und wahrscheinlich in Idealkonkurrenz zu einem der Delikte im 14., 15. oder 16. Abschnitt des Strafgesetzbuches.

Die alte Bestimmung des § 91d Abs. 1 letzter Satz SPG befand sich praktisch wortgleich im ersten Begutachtungsentwurf zum PStSG, dort im ursprünglich vorgeschlagenen § 16 Abs. 1 letzter Satz. Mit der Regierungsvorlage wurde die schließlich in § 15 Abs. 1 letzter Satz PStSG normierte Bestimmung auf die nun geltende Fassung 'reduziert'.

[…]

Demnach darf die Akteneinsicht des RSB dann ausgenommen werden, wenn ansonsten (also bei voller Akteneinsicht des RSB) eine Gefahr für Zeugen oder Dritte nach Maßgabe des § 162 StPO besteht.

Der Verweis auf § 162 StPO erweckt den Eindruck, der RSB unterliege denselben Einschränkungen wie ein Strafgericht. Diese Norm gibt dem Gericht ein Ermessen, einen Zeugen anonym aussagen zu lassen, wenn bestimmte Tatsachen

vorgebracht werden, dass ansonsten Leben, Gesundheit, körperliche Unversehrtheit oder Freiheit des Zeugen oder eines Dritten gefährdet sein könnte.

Bei dieser Aufzählung des § 162 StPO fällt gegenüber der alten Fassung von § 91d SPG (bzw. dem ersten Entwurf zu § 16 PStSG) auf, dass eine Gefährdung der 'nationalen Sicherheit' kein ausdrücklich genanntes Kriterium ist. Eine effektive Einschränkung ist dies aber nicht, weil kaum ein Szenario vorstellbar ist, bei der im Zusammenhang mit 'verfassungsgefährdenden Angriffen' die nationale Sicherheit bedroht wäre, ohne dass gleichzeitig 'eine Gefahr für Leben, Gesundheit, körperliche Unversehrtheit oder Freiheit des Zeugen oder eines Dritten' bestünde.

Nach der StPO handelt es sich aber gerade nicht um eine Beschränkung gegenüber dem Gericht oder der Person des Richters, vielmehr begegnet es dem Umstand, dass die Hauptverhandlung im Strafverfahren grundsätzlich öffentlich und jedenfalls Parteien-öffentlich ist.

§ 51 StPO regelt dementsprechend die Akteneinsicht und verweist ebenfalls auf § 162 StPO, wobei unzweifelhaft ist, dass dem Gericht alle Informationen vorliegen und das Gericht entscheidet, welche Informationen den Parteien (oder einer Partei) ausnahmsweise vorenthalten werden dürfen.

Die Beschränkung betrifft im Strafverfahren also vielmehr den Beschuldigten bzw. Angeklagten, dem Art 6 EMRK grundsätzlich das Recht gewährt, über die Identität von Zeugen in Kenntnis zu sein und volle Akteneinsicht zu haben. Die Rechtfertigung dieser Beschränkung liegt in einer Güterabwägung auf Basis bestimmter Tatsachen, aus denen sich die Gefährdungslage ergibt. Auch hier zeigt § 162 StPO, dass keinesfalls eine Schutzrichtung gegenüber dem Gericht besteht. 'Bestimmte Tatsachen', die eine Gefährdung behaupten, müssen nämlich 'vorgebracht werden', das heißt, dass regelmäßig die Anklage gegenüber dem Gericht konkret argumentieren muss, warum die Beschuldigtenrechte im Einzelfall beschränkt werden sollen. Wenn das Gericht die Tatsachen als stichhaltig beurteilt, lässt es nach eigenem Ermessen die anonyme Aussage zu. Demgegenüber haben die Organisationseinheiten nach § 1 Abs. 3 PStSG keine Pflicht, die Einschränkung der Akteneinsicht gegenüber dem RSB oder einer anderen Stelle zu begründen, und der RSB hat gegenüber den Behörden keine Diskretionsbefugnis wie ein Gericht nach § 162 StPO.

Die hinter der Regelung des § 162 StPO stehende Annahme, dass vom Beschuldigten eines Strafverfahrens eine Gefahr für Zeugen ausgehen könnte, entspricht der allgemeinen Lebenserfahrung. Es ist aber nicht nachvollziehbar, weshalb vom RSB eine Gefahr für Zeugen, Dritte oder gar die öffentliche Sicherheit ausgehen soll. Im selben Maße müsste jeder Beamte der Staatsschutzbehörden bzw. jeder Polizeibeamte, dessen Aufgabe und Sicherheitsklasse den Zugang zu solchen Akten erlaubt, eine ebensolche Gefahr darstellen. Es ist nicht nachvollziehbar, warum der RSB weniger vertrauenswürdig sein soll als die den Fall bearbeitenden Sicherheitsbeamten.

Der RSB ist nach § 91d SPG und § 15 Abs. 1 PStSG eben nicht in derselben Position wie ein Richter nach § 162 StPO.

Der Wortlaut des § 15 Abs. 1 letzter Satz PStSG legt nahe, dass die der Kontrolle unterliegenden Staatsschutzorgane selbst entscheiden, ob die Einsicht des (als einzig) zur Kontrolle berufenen RSB zu beschränken ist. Eine weitere Entscheidungsinstanz dazu ist nicht vorgesehen, der RSB kann gegen eine solche Beschränkung nichts unternehmen. Die österreichische Rechtsordnung kennt weder im Bereich der Justiz noch im Bereich der Verwaltung eine Einschränkung, wonach ein zum Rechtsschutz oder zur Genehmigung einer Maßnahme berufenes Gericht nicht alle entscheidungserheblichen Aktenstücke kennen darf.

Aus dem Umstand, dass die Akteneinsicht des RSB potentiell in jedem einzelnen Fall eingeschränkt sein könnte, entsteht das Problem, dass damit unangekündigte, stichprobenartige Kontrollen durch den RSB praktisch ins Leere laufen. Denn in jedem Fall erhalten die kontrollierten Organisationseinheiten so die Gelegenheit, unter Berufung auf § 15 Abs. 1 letzter Satz PStSG die Akten vor der Kontrolle zu sichten und Aktenstücke auszunehmen, die der RSB — möglicherweise auch aus gesetzlich nicht anerkannten Gründen — nicht sehen soll.

Würde der VfGH hinnehmen, dass im Verfahren nach Art 144 B-VG einzelne entscheidungserhebliche Aktenstücke von der Einsicht durch die Verfassungsrichterinnen und Richter ausgenommen wären, weil deren Kenntnis das Leben von Menschen oder die öffentliche Sicherheit gefährdet? Und ist der Rechtsschutzbeauftragte beim Bundesministerium für Inneres weniger vertrauenswürdig als die Richterinnen und Richter des VfGH?

Nun ist der RSB das einzige Kontroll- und Genehmigungsorgan im System des SPG ebenso wie nach dem PStSG. Allenfalls mögliche Beschwerden an die Datenschutzbehörde mit einem weiteren Rechtszug zum Bundesverwaltungsgericht sind demgegenüber nur nachträgliche Rechtsschutzinstrumente, die jedoch bedingen, dass entweder der Betroffene von der Maßnahme erfährt oder der Rechtsschutzbeauftragte kommissarisch Beschwerde führt — die hier argumentierten Probleme werden damit jedenfalls nicht verringert. Die Einschränkung der Akteneinsicht ist dabei nur ein Beispiel, dass die Konstruktion des RSB eben keinen adäquaten Ersatz zu einer richterlichen Kontrolle etwa nach dem Vorbild der StPO darstellt. Wesentlich ist, dass die Institution des Rechtsschutzbeauftragten in allen Bereichen, wo sie vorgesehen ist (StPO, SPG, MBG, FinStrG), nicht die Funktion hat, gerichtliche Kontroll-und Rechtsschutzaufgaben zu ersetzen, sondern vielmehr sie durch begleitende Kontrolle und kommissarisch für Betroffene wahrgenommene Rechtsschutzhandlungen zu ergänzen. Besonders deutlich wird dies beim Rechtsschutzbeauftragten der Justiz, dem nach § 147 StPO unter anderem die Prüfung und Kontrolle gerichtlicher Genehmigungen und Bewilligungen obliegt, der also bloß einen zusätzlichen Sicherungsmechanismus darstellt und nicht den primären ersetzt. Auch nach dem erst kürzlich novellierten § 74b Finanzstrafgesetz besteht der Rechtsschutz durch den (kürzlich geschaffenen) RSB beim Finanzministerium als Begleitung, wenn eine Kon-

teneinschau nach § 9 Kontenregister- und Konteneinschaugesetz durch den Einzelrichter am Bundesfinanzgericht entschieden wird.

Damit soll zum Ausdruck gebracht werden, dass ein effektiver Rechtsschutz eben beides erfordert: eine richterliche Kontrolle und einen begleitenden bzw. kommissarischen Rechtsschutz durch den RSB. Der Vergleich mit anderen Rechtsmaterien, die bestimmte Aufgaben einem Rechtsschutzbeauftragten zuweisen, zeigt dabei auch, dass die anfechtungsgegenständliche Konstruktion des Rechtsschutzes auch unsachlich ist und daher Art 7 B-VG verletzt.

Zusammenfassung zur Akteneinsicht:

§ 91d Abs. 1 letzter Satz SPG sowie § 15 Abs. 1 letzter Satz PStSG bewirken eine massive Beschränkung der Kontrolltätigkeit des Rechtsschutzbeauftragten, weil dieser niemals freien Zugang zu Akten hat. Potentiell ist in jedem Akt, in den er Einsicht nehmen will, zuerst zu kontrollieren, ob darin Aktenstücke von der Einsicht des RSB auszunehmen sind. Nachdem der Zweck der Norm offenbar der Schutz von Menschenleben ist, darf ein Beamter einer Organisationseinheit nach § 1 Abs. 3 PStSG auch nicht (fahrlässig) dem RSB Akten ungeprüft aushändigen. Angesichts des höchstwertigen Schutzzwecks ist die 'Kann-Bestimmung' als zwingend zu verstehen. Daher darf es routinemäßig keine freie Akteneinsicht des RSB ohne Vorabkontrolle der Akten durch die zuständigen Sicherheitsorgane geben. Das Konzept einer stichprobenartigen und überraschenden Kontrolle steht dem RSB damit jedenfalls nicht mehr zur Verfügung.

Anzumerken ist, dass die 'Einschränkung' dieser Ausnahme von der Akteneinsicht per Verweis auf § 162 StPO gegenüber der Regierungsvorlage zum PStSG, mit der auf Kritik in der rechtspolitischen Debatte reagiert wurde, geradezu eine Irreführung der Rechtsadressaten darstellt. Die ursprünglich vorgeschlagene Norm hat zumindest sofort verständlich gemacht, was die Einschränkung bedeutet. Bei der nun geltenden Fassung bedarf es spezieller juristischer Kenntnisse und umfassender Überlegungen, um zu erschließen, dass der Bedeutungsgehalt im Wesentlichen derselbe geblieben ist. Die Unterminierung von unangekündigten Kontrollen der Staatsschutzbehörden durch den RSB stellt einen Verstoß gegen den Gleichheitsgrundsatz des Art 7 B-VG (verstanden als Sachlichkeitsgebot), das nicht nur die Vollziehung sondern auch den Gesetzgeber bindet, dar.

6.4.1.2 Beschränkung der Befugnisse des RSB als formale Verfassungswidrigkeit wegen Verletzung der verfassungsgesetzlichen Absicherung gemäß § 91a SPG

Die Aufgabe nach § 6 Abs. 1 Z 3 PStSG (Schutz vor verfassungsgefährdenden Angriffen im Ausland) war nach Auffassung der Antragsteller schon bisher von der Aufgabe der erweiterten Gefahrenerforschung umfasst, weil es nach § 21 Abs.3 SPG alt keine Rolle spielte, ob die Verdachtslage auf einer Meldung aus dem Ausland basiert oder nicht. Mit der ausdrücklichen Normierung dieser Aufgabe nimmt der Gesetzgeber eine Auslagerung dieser Aufgabe und der damit verbundenen Befugnisse ins PStSG vor. Gleichzeitig erfahren die Befugnisse des RSB gegenüber dem alten § 21 Abs.3 eine massive Einschränkung, weil Handlun-

gen im Rahmen der Aufgabenerfüllung nach § 6 Abs.1 Z 3 PStSG vom Rechtsschutz gemäß § 14 PStSG überhaupt nicht erfasst sind (vgl. auch unten Punkt 7.7).

Eine Einschränkung der Befugnisse des RSB darf aber nach der Verfassungsbestimmung des § 91a Abs. 3 SPG nur mit einer Zweidrittel-Mehrheit im Nationalrat beschlossen werden. Das PStSG ist daher auch formal […] fehlerhaft, weil die 'Auslagerung' von Befugnissen aus dem SPG ins PStSG bei gleichzeitiger Beschränkung der Befugnisse des RSB jedenfalls als Beschränkung im Sinne des § 91a Abs. 1 SPG zu sehen ist. Ansonsten wäre es dem Gesetzgeber freigestellt, die verfassungsgesetzlich abgesicherte Bestandsgarantie der Befugnisse des RSB durch geschickte Rechtsgestaltung zu umgehen.

6.4.1.3 Gesamtbeurteilung: Die Institution Rechtsschutzbeauftragter (RSB) ist kein Richterersatz

Neben den konkreten Einschränkungen des PStSG und des SPG; besteht die Grundsatzkritik an der Konzeption des Rechtsschutzes durch die konkrete Ausgestaltung des RSB. Von zentraler Bedeutung für einen effektiven Rechtsschutz ist die Frage, ob die für den gesamten Bereich der Sicherheitspolizei und des Staatsschutzes zentrale Kontrollinstanz des RSB auch mit hinreichenden Mitteln und Unabhängigkeitsgarantien ausgestattet ist.

Der RSB im BM.I gehört organisatorisch jener ministeriellen Behörde an, die für die Überwachungsmaßnahmen in letzter Instanz verantwortlich ist — dem BM.I. Er ist zwar sachlich weisungsfrei gestellt, aber schon allein wegen seiner organisatorischen Eingliederung in das Innenministerium nicht unabhängig. Daran ändert auch nichts, dass dem RSB nun gemäß § 91b Abs. 3 SPG Büroräumlichkeiten außerhalb des Raumverbundes der Generaldirektion für die öffentliche Sicherheit zur Verfügung zu stellen sind. Weiters wird er von der Exekutive bestellt, nämlich vorn Bundespräsidenten auf Vorschlag der Bundesregierung (§ 91a Abs. 2 SPG), die Präsidenten des Nationalrates sowie der Höchstgerichte haben im Zuge der Bestellung lediglich Anhörungsrechte. Falls diese nach der Anhörung (schwere) Bedenken haben, gibt es weder ein Einspruchsrecht noch sonstige normierte Konsequenzen — es bleibt allein das Vertrauen auf eine konsensorientierte Bundesregierung und einen umsichtigen Bundespräsidenten.

Die persönlichen Qualifikationsvoraussetzungen entsprechen auch nicht jenen eines unabhängigen Richters (vgl. § 91b Abs. 1 SPG).

Der Umstand, dass sich der Rechtsschutzbeauftragte und seine Stellvertreter im Bereich des polizeilichen Staatsschutzes regelmäßig austauschen und in Fragen von grundsätzlicher Bedeutung für die Aufgabenerfüllung eine einheitliche Vorgehensweise anstreben sollen, haben mit echter richterlicher Kontrolle (und den verfassungsmäßigen richterlichen Garantien) oder zumindest einer Entscheidung über eine Genehmigung von Ermittlungsmaßnahmen im Kollegium (was die Qualität der Entscheidungsfindung erhöht) nichts zu tun.

Daran ändert auch weder der Umstand, dass — in Zukunft — zumindest ein Stellvertreter mindestens zehn Jahre lang als Richter oder Staatsanwalt tätig gewesen sein muss, noch dass es zu einer räumlichen Trennung zwischen dem Büro des Rechtsschutzbeauftragten und den Arbeitsräumlichkeiten der Generaldirektion für öffentliche Sicherheit oder einer ihr nachgeordneten Behörde kommt, etwas. Dass eine verdeckte Ermittlung (§ 11 Abs. 1 Z 2 iVm § 54 Abs. 3 und 3a SPG) und eine Auskunft über Daten einer Nachrichtenübermittlung (§ 11 Abs. 1 Z 7) der Rechtsschutzbeauftragte und zwei seiner Stellvertreter mit Stimmenmehrheit als 'Rechtschutzsenat' (§ 14 Abs. 3) genehmigen müssen, ist zwar für diese Fälle eine kleine Verbesserung, ändert aber an den wesentlichen Schwächen im Rechtsschutz- und Kontrollsystem nicht viel.

Die Schwächen des Rechtsschutzes bei der Genehmigung von Maßnahmen durch den RSB wird zudem perpetuiert durch die in § 14 Abs. 2 lapidar normierte Anordnung 'Verlängerungen sind zulässig', ohne zu bestimmen, unter welchen Voraussetzungen, wie oft und wie lange solche Verlängerungen zulässig sein sollen. Dies kommt einer Generalermächtigung gleich, die auf den Grundsatz der Verhältnismäßigkeit keine Rücksicht nimmt.

Schließlich besteht ein praktisch schwerwiegendes Problem darin, dass die Einrichtung des Rechtsschutzbeauftragten nicht einmal annähernd ausreichend ausgestattet ist, um einen effektiven kommissarischen Rechtsschutz zu bieten. Um sicherzustellen, dass eine hohe Meldedisziplin unter den Beamten herrscht, müsste der RSB daher regelmäßige und signifikante Stichproben-Kontrollen im gesamten Bundesgebiet durchführen, was vor allein einen entsprechenden Personalaufwand bedeuten würde.

Tatsächlich besteht die Institution des RSB nach den Angaben auf der Website des BM.I aus dem Rechtsschutzbeauftragten selbst, zwei Stellvertreterinnen (beide nur nebenberuflich), zwei Referenten und einer Sekretariatsstelle. Für die mit dem PStSG entstehenden neuen Aufgaben ist nach der 'Wirkungsorientierten Folgenabschätzung' zur Regierungsvorlage eine zusätzliche neue Referentenstelle sowie (bei Bedarf) eine zusätzliche halbe Sekretariatsstelle vorgesehen. Es macht nicht den Anschein, dass der RSB mit diesen Kapazitäten mehr tun kann, als den Angaben der zu kontrollierenden Beamten grundsätzlich Glauben zu schenken und die tatsächlich vorgelegten Meldungen fast ausschließlich rechtlich zu prüfen.

Ein Rechtsschutzbeauftragter mit Sitz in Wien, zwei Stellvertreterinnen, einer (allenfalls eineinhalb) Sekretariatsstelle und drei Mitarbeitern, zugeordnet dem Bundesministerium für Inneres, können nicht 270 Mitarbeiter/innen des BVT und einen Polizeiapparat von etwa 30.000 über die ganze Republik verstreuten Beamtinnen und Beamten kontrollieren, insbesondere wenn selbst seine stichprobenartigen Kontrollen letztlich vom Wohlwollen der zu Kontrollierenden abhängen.

Der RSB entspricht daher nach Ansicht der Antragsteller/innen nicht den vom EGMR geforderten Kriterien einer unabhängigen Kontrollinstanz. Es sei angemerkt, dass zu dieser Frage seit 2010 eine (in formeller Hinsicht bereits als

zulässig erkannte) Beschwerde aus Österreich beim Europäischen Gerichtshof für Menschenrechte (EGMR) mit der Beschwerde-Nummer 3599/10 (Tretter u.a. v. Österreich) anhängig ist.

6.4.2. Transparenz und parlamentarische Kontrolle (§ 17 PStSG)

Die Berichtspflichten des Bundesministers für Inneres und des Rechtsschutzbeauftragten an den 'ständigen Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit' schaffen nur eine oberflächliche Transparenz. Die Anforderungen des § 17 sind im besten Fall ein absolut notwendiges Mindestmaß an parlamentarischer Kontrolle und sorgen dafür, dass die Tätigkeitsberichte zumindest schlüssig sein müssen. Bei einem stark ausgestalteten operativen Rechtsschutz- und Kontrollsystem könnte damit — zumindest im Hinblick auf die verfassungsrechtliche Zulässigkeit — durchaus das Auslangen gefunden werden. Eine Kompensation für den mangelhaften Rechtsschutz ist darin aber nicht zu sehen.

6.5 Verletzung des Gleichheitssatzes nach Art 7 B-VG

Auch der in Art 7 B-VG enthaltene Gleichheitsgrundsatz wird durch den ineffizienten Rechtsschutz gemäß PStSG und SPG verletzt. Soweit in den Anfechtungen einzelner Normen (auch) eine Verletzung von Art 7 B-VG geltend gemacht wird, zielt diese Geltendmachung auf die Verletzung des Sachlichkeitsgebots, das auch den Gesetzgeber bindet.[…]

Diese Bindung des Gesetzgebers an das Sachlichkeitsgebot gilt auch für die Bestimmungen zu den Befugnissen des Rechtsschutzbeauftragten gemäß PStSG und die komplementären Vorschriften des SPG. Das Sachlichkeitsgebot erweist sich hinsichtlich des Rechtsschutzes gemäß PStSG und der komplementären Vorschriften des SPG als verletzt, insbesondere im Vergleich zum Rechtsschutzsystem der Strafprozessordnung (StPO).

Den Antragsteller/innen ist bewusst, dass im Bereich des Polizeirechts andere Sachverhalte als in der Strafprozessordnung geregelt werden, sohin (oberflächlich betrachtet) unterschiedliche Sachverhalte ungleich geregelt werden; allerdings wird sowohl im Bereich des Polizeirechts als auch im Bereich der Strafprozessordnung allein durch die Qualität des Rechtsschutzes die Grundrechts- und Verfassungskonformität sichergestellt — oder eben nicht. Durch die thematische und praktische Nähe der beiden Bereiche erscheint ein wertender Vergleich der jeweiligen Regelungen gerechtfertigt.

Der Gesetzgeber ist für die faktisch ineffiziente Ausgestaltung des Rechtsschutzes […] im Bereich des PStSG und der komplementären Vorschriften des SPG im Vergleich zur thematisch verwandten StPO jede Begründung schuldig geblieben, wodurch (auch) der Gleichheitsgrundsatz gemäß Art 7 B-VG verletzt wird.

6.6. Zusammenfassende Darstellung der geltend gemachten Verfassungswidrigkeiten

6.6.1 Einzelne Bestimmungen des PStSG greifen in materielle Grundrechte ein, manche Grundrechte bzw. Verfassungsbestimmungen werden durch das gesamte System des PStSG und der komplementären Vorschriften des SPG verletzt.

6.6.2 Das Polizeiliche Staatsschutzgesetz weist im Hinblick auf die verfassungsrechtlich gebotene hinreichende Normenbestimmtheit und den effektiven Rechtsschutz schwere Mängel auf. Zentrale Begriffe wie 'Gruppierung', 'ideologisch motivierte Kriminalität' oder 'ideologisch motivierte Gewalt' sind nicht hinreichend bestimmt, obwohl diese Normenbestandteile wesentliche Voraussetzungen für Grundrechtseingriffe beschreiben. Die umfangreichen Befugnisse der Staatsschutzorgane kommen schon bei abstrakten Gefährdungslagen, auch unterhalb der Schwelle eines 'gefährlichen Angriffs' zum Tragen. Im Rechtsschutzsystem hingegen bestehen massive Lücken, sodass nur eine geringe Chance besteht, dass das Problem der unbestimmten Begriffe im Rahmen effektiver Rechtsschutz- und Kontrollmechanismen kompensiert wird. Das aus Art 18 B-VG abgeleitete Rechtsstaatsprinzips wird daher durch die angefochtenen Normen verletzt.

6.6.3 Da das gesamte System des PStSG und der komplementären Vorschriften des SPG vor allem aus Rechtsnormen zur Ermittlung personenbezogener Daten besteht und letztlich in einer zentralen Datenanwendung kulminiert, wird das PStSG dazu führen, dass der Kreis der Betroffenen immer weiter ausgedehnt wird (der wahrscheinlich binnen weniger Jahre einen relevanten Teil der österreichischen Bevölkerung ausmachen wird) und gleichzeitig keine wirksamen Kontroll- und Rechtsschutzmechanismen bestehen, mit der solche Tendenzen effektiv zurückgedrängt werden (können). Ohne (effektiven) Rechtsschutz stellt dies einen unverhältnismäßigen Grundrechtseingriff dar, wodurch § 1 DSG 2000 verletzt wird, aber auch Art 10 EMRK, da aufgrund der weitreichenden Befugnisse zur Überwachung des Verhaltens und der Kommunikation, sowohl im Bereich der unmittelbar zwischenmenschlichen als auch der elektronischen Interaktion, ein Klima geschaffen wird, in dem die Menschen sich bei der Äußerung der eigenen Meinung ebenso wie beim Konsum von Informationen zur Bildung einer eigenen Meinung selbst bei völlig legalen Inhalten immer häufiger selbst beschränken werden, um mögliche nachteilige Folgen zu vermeiden.

Art 8 EMRK (und das akzessorische Recht auf einen effektiven Rechtsschutz nach Art 13 EMRK) werden verletzt, da das PStSG zwar festlegt, welche Arten von Informationen gespeichert, gegenüber welchen Personengruppen Überwachungsmaßnahmen ergriffen und 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, wie die Art und Weise der Speicherung und das Verfahren des Informationsabrufs zu erfolgen haben sowie welche Verwendungszwecke für die abgerufenen Informationen zulässig sind. Aber all diese Regelungen sind unklar, lückenhaft und nicht durch einen effektiven Rechts-

schutz abgesichert. Damit genügt das PStSG nicht dem von der EMRK (und dem EGMR) intendierten Schutzzweck.

6.6.4 Das Polizeirecht und die Strafprozessordnung sind — wie oben ausgeführt — thematisch eng verbundene Bereiche mit jeweils tiefgreifenden Eingriffen in verfassungsmäßig gewährleistete Rechte. Ein wertender Vergleich der jeweiligen Regelungen ist daher gerechtfertigt. Da der Gesetzgeber für die faktisch ineffiziente Ausgestaltung des Rechtsschutzes im Bereich des PStSG und der komplementären Vorschriften des SPG im Vergleich zur StPO jede sachliche Begründung schuldig geblieben ist, wird das vom VfGH aus dem Gleichheitsgrundsatz gemäß Art 7 B-VG abgeleitete Sachlichkeitsgebot verletzt.

6.6.5 Die Summe der schwerwiegenden Verletzungen des aus Art 18 B-VG abgeleiteten Rechtsstaatsprinzips durch die angefochtenen Normen des PStSG sowie des SPG bzw. die darauf basierenden potenziellen Vollziehungsakte erweist sich als massive Verletzung eines 'Baugesetzes' und dadurch als Gesamtänderung der österreichischen Bundesverfassung im Sinne von Art 44 Abs.3 B-VG, sodass das gesamte PStSG sowie die angefochtenen Normen des SPG als verfassungswidrig aufzuheben sind.

Unter dem Aspekt einer 'Überwachungs-Gesamtrechnung' wiederum kann das PStSG sowie die komplementären Bestimmungen des SPG als eine jener partiell wirkenden Maßnahmen im Sinne der Judikatur des VfGH gelten, die in Summe bzw. im Ergebnis mit den zahlreichen, seit dem 11.09.2001 erlassenen Überwachungsnormen zu einer 'schleichenden Gesamtänderung' der österreichischen Bundesverfassung im Sinne von Art 44 Abs. 3 B-VG geführt haben (könnten). Auch aus diesem Grund sind das gesamte PStSG sowie die angefochtenen Normen des SPG als verfassungswidrig aufzuheben.

6.6.6 Angemerkt sei, dass nach Meinung der Antragsteller/innen das PStSG durch eine bloße Aufhebung der zentralen angefochtenen Bestimmungen allein gar nicht repariert werden kann, da es diesfalls als sinnentleerte Hülle zurückbliebe, die einer Vollziehung in der vom Gesetzgeber intendierten Form gar nicht mehr zugänglich wäre. Dies muss die Aufhebung des gesamten PStSG wegen Verfassungswidrigkeit nach sich ziehen."

Unter dem Punkt "Zur Anfechtung einzelner Normen ('Besonderer Teil')" führen die Antragsteller dann Folgendes aus (Zitat ohne im Original enthaltene Hervorhebungen): 5

"7.1 Mangelnde Bestimmtheit im Einzelnen

[…]

Im Folgenden wird gezeigt, warum die zentrale Bestimmung des § 6 PStSG in mehrfacher Hinsicht große Bedenken im Hinblick auf die Verständlichkeit und Transparenz des gesamten Entwurfs mit sich bringt.

7.1.1. § 6 Abs. 1 Z 1 (Erweiterte Gefahrenerforschung)

[…]

Die Erläuterungen zu § 6 PStSG führen aus, dass sich die erweiterte Gefahrenerforschung im Hinblick auf Gruppierungen — die nun vollständig aus dem SPG in das PStSG überführt werden soll – in der Praxis bewährt habe. Gleichzeitig enthalten die Materialien keinen Hinweis auf Nachweise, Berichte oder Statistiken, auf welche die Annahme der Bewährung des Instruments in der Praxis gestützt wird. Außerdem drängt sich die Frage auf, warum zur Erfüllung des Aufgabenbereichs 'erweiterte Gefahrenerforschung von Gruppierungen' die Notwendigkeit für erweiterte Befugnisse nach dem PStSG erforderlich sind, wenn sich das Instrument angeblich in der Praxis bewährt hat. Für eine — mit Grundrechtseingriffen verbundene — Erweiterung von Befugnissen im Hinblick auf ein 'bewährtes' Instrument trifft den Staat zumindest die Rechtfertigungslast, warum die Erweiterung erforderlich sein soll.

Statt 'weltanschaulich motivierter Kriminalität', so der Wortlaut nach dem ersten Begutachtungsentwurf, wurde nunmehr der Begriff 'ideologisch motivierte Kriminalität' normiert. Offenbar wurde im Gesetzgebungsprozess damit auf Kritik in der rechtspolitischen Debatte, dass der Begriff der 'weltanschaulich motivierten Kriminalität' problematisch, weil zu unbestimmt und zu missbrauchsanfällig ist, reagiert. Damit ändert sich am Tatbestand und somit an der vorgebrachten Kritik jedoch nichts, weil 'ideologisch' und 'weltanschaulich' synonyme Begriffe sind.

Versteht man den Begriff der Ideologie wertneutral, handelt es sich um 'erstarrte Leitbilder' sozialer Gruppen oder Organisationen, die zur Begründung und Rechtfertigung ihres Handelns dienen, also um ihre Ideen, Kategorien und Wertvorstellungen, somit um ihre 'Weltanschauung'. Im allgemeinen Sprachgebrauch wird der Begriff 'Ideologie' zumeist abwertend nur für manipulative, unzulängliche oder nicht wissenschaftlich begründete Ideen-Systeme und Theorien verwendet, die im Interesse weltanschaulicher, wirtschaftlicher oder politischer Zielsetzungen der Verschleierung und Rechtfertigung von Interessen dienen. Der Gesetzgeber sollte unklare und emotional aufgeladene Begriffe in einem eingriffsintensiven Gesetz bestmöglich vermeiden. Auf die berechtigte Kritik an diesem im Entwurf verwendeten Gesetzesbegriff zu reagieren, indem er durch den synonymen griechischen Begriff mir der gleichen Bedeutung ersetzt wird, ist ein reiner Etikettenschwindel, der die Kritik nicht ernst zu nehmen bereit ist.

Laut den Erläuterungen ist es erklärtes Ziel des Polizeilichen Staatsschutzgesetzes, den Bedrohungen des insbesondere islamistischen Terrorismus mit den entsprechenden Mitteln zu begegnen. Terrorismus (insbesondere islamistischer Prägung) ist nach einhelliger Meinung darauf gerichtet, die rechtsstaatliche Ordnung und demokratische Systeme westlicher Prägung anzugreifen und letztendlich zu zerstören. Statt den Begriffen 'weltanschaulich' bzw 'ideologisch' oder 'religiös motivierter Kriminalität' sollte der Gesetzgeber präzisere Formulie-

rungen wählen, um den Anwendungsbereich des Gesetzes auf die Aktivitäten von Personen einzuschränken, die eigentlich das Ziel der neuen Bestimmungen sind (Aktivitäten, die die demokratische bzw rechtsstaatliche Ordnung gefährden).

Das Kernproblem der Unbestimmtheit in § 6 Abs. 1 Z 1 ist für das PStSG geradezu paradigmatisch. Die äußerst unscharfen Begriffe als wesentliche Voraussetzung für den Einsatz weitgehender Eingriffsbefugnisse sind unter dem Deckmantel der nationalen Sicherheit und Terrorbekämpfung extrem anfällig für Missbrauch.

Wenn einzelne Mitglieder einer Gruppe oder Organisation ein gerichtlich strafbares Verhalten setzen, sollen diese einer entsprechenden strafrechtlichen Haftung zugeführt werden. Dadurch wird aber die Organisation selbst nicht automatisch zur 'kriminellen' oder gar 'terroristischen Vereinigung'. Auf diese Weise führt nämlich ein strafbares Verhalten Einzelner dazu, dass eine mit den rechtlich geschützten Werten verbundene Mehrheit Eingriffe in ihre Freiheit hinnehmen muss, ohne einen Anlass dazu gegeben zu haben. Die zentrale Installation des undefinierten Begriffes der 'Gruppierung' im PStSG leistet jedoch einer solchen Entwicklung enormen Vorschub. In Kombination mit dem mangelhaften Rechtsschutz besteht so die Gefahr einer unkontrollierten Ausweitung der Instrumente des vorbeugenden Schutzes vor Sicherheitsgefährdungen auf immer weitere Kreise der Bevölkerung.

7.1.2. § 6 Abs. 1 Z 2 (Vorbeugender Schutz vor verfassungsgefährdenden Angriffen durch eine Person)

[…]

Eine Definition des Begriffs 'vorbeugender Schutz' findet sich im Gesetzestext nicht.

Der Wortlaut lässt auf Prävention schließen, also der Vermeidung einer in der Zukunft liegenden Gefährdung. Die Norm verweist auch auf § 22 SPG, dessen Überschrift 'Vorbeugender Schutz von Rechtsgütern' lautet und der auf § 21 SPG folgt, in dem die Abwehr allgemeiner Gefahren und die Beendigung gefährlicher Angriffe normiert ist. Bei dieser Gefahrenabwehr ist die Bedrohung eines Rechtsgutes von entscheidender Bedeutung. Im Umkehrschluss darf es beim vorbeugenden Schutz somit noch nicht zu einer Bedrohung gekommen sein, denn diese würde ja unter die Gefahrenabwehr fallen. Der Einsatzbereich des vorbeugenden Schutzes endet demnach mit dem Eintritt einer konkret strafbaren Vorbereitungshandlung.[…]

Nach dem Gesetzeswortlaut beginnt der Einsatzbereich, wenn ein begründeter Gefahrenverdacht für einen verfassungsgefährdenten Angriff vorliegt, wohingegen im Begutachtungsentwurf noch auf 'wahrscheinliche Angriffe' abgestellt wurde. Zwar findet sich dieser Bezug nicht mehr im PStSG, jedoch verweist die Klammer am Ende der Ziffer 2 auf § 22 Abs. 2 SPG. wo sich wiederum ein Bezug zur Wahrscheinlichkeit von Angriffen findet.

Nach den Materialien ist unter 'begründetem Gefahrenverdacht' mehr als die bloße Möglichkeit oder Nichtausschließbarkeit (eines Angriffs), aber weniger als 'mit Gewissheit zu erwarten' zu verstehen. Dieser Verdacht muss darauf gerichtet sein, dass der Betroffene einen verfassungsgefährdenden Angriff in absehbarer Zeit begehen werde.

Somit beginnt der Anwendungsbereich des vorbeugenden Schutzes mit der Wahrscheinlichkeit der Begehung eines konkreten Angriffs in absehbarer Zeit. Um die Begründungspflicht prozessual abzusichern, wären klare Regelungen erforderlich, wo und wie die Begründungen für das Vorliegen eines konkreten Gefahrenverdachts schriftlich zu dokumentieren und vorzulegen sind. Problematisch ist jedenfalls, dass die Befugnisse nach diesem Bundesgesetz bereits weit im Vorfeld einer strafbaren Handlung ausgelöst werden, wobei einige Delikte im Deliktskatalog selbst schon die Strafbarkeit weit in den Vorbereitungsbereich verlagern (z.B. § 278b Abs. 2 StGB).

Ein überbordendes Sicherheitsdenken ist ein weiterer Schritt hin zum Überwachungsstaat, in dem sich die rechtsstaatliche Demokratie selbst preisgeben würde. Die Unklarheit, ab welcher Schwelle der Konkretisierung einer Verdachtslage die Aufgabe vorliegt, die weitgehende Eingriffe in die Grundrechte nach § 1 DSG 2000, Art 8 und 10 EMRK erlaubt, bewirkt die Unverhältnismäßigkeit und damit die Verfassungswidrigkeit dieser Bestimmung.

7.2 § 6 Abs. 1 Z 3 PStSG (Schutz vor verfassungsgefährdenden Angriffen im Ausland)

[…]

Bei dieser Bestimmung fehlt die Einschränkung eines begründeten Gefahrenverdachts, es bedarf also offensichtlich keiner konkreten Bedrohungssituation mehr (ganz abgesehen von einer konkreten Rechtsgutbeeinträchtigung).[…] Das Hauptproblem dieser Bestimmung sitzt eigentlich nicht direkt in der Norm selbst sondern in den Unterlassungen im Rahmen der Rechtsschutzgestaltung, über die allgemein schon beschriebenen Defizite hinaus.

Es bedarf im Rahmen dieser Aufgabe nämlich keiner Genehmigung von Ermittlungen durch den Rechtsschutzbeauftragten und die besonderen Löschfristen sind (ohne juristische Auslegungskunststücke) nicht anwendbar.

Die Regelung der Aufgabe ist daher im Hinblick auf die damit verbundenen Befugnisse ohne effektiven Rechtsschutz unverhältnismäßig.

7.3 § 6 Abs. 2 PStSG (Definition verfassungsgefährdender Angriff)

[…]

Auch nach Lektüre der Materialien zum PStSG ist nicht erkennbar, auf Basis welcher Annahmen der Katalog an Straftaten zustande gekommen ist, der in Summe den zentralen Begriff des 'verfassungsgefährdenden Angriffs' definiert. Außerdem ist — nicht nur für juristische Laien — schwer erschließbar, welche strafrechtlichen Tatbestände in welcher Ausprägung verfassungsgefährdende Angriffe darstellen und damit in die Zuständigkeit der Staatsschutzorgane fallen. Demgegenüber ist die im Entwurf vorliegende Ausbildungsverordnung Verfassungsschutz und Terrorismusbekämpfung (AusbV-VT) auf Basis des § 2 Abs. 3 PStSG) bemerkenswert. Dort wird festgelegt, wie viele Unterrichtseinheiten die Beamten der Organisationseinheiten gemäß § 1 Abs. 3 PStSG für verschiedene Bereiche zu absolvieren haben. Demnach sind für 'Juristische Module' insgesamt 16 Einheiten vorgesehen, davon 8 Einheiten zu den Aufgaben und Befugnissen im Rahmen des Polizeilichen Staatsschutzes sowie zum Rechtsschutz, 4 Einheiten zu Sicherheitspolizeigesetz und Strafprozessrecht sowie weitere 4 Einheiten zum Datenschutz.

Besonders problematisch bleiben die Abgrenzungsschwierigkeiten bei der 'verschachtelten' Venweisungstechnik in § 6 Abs. 2 Z 2 PStSG, der die 'in § 278c StGB genannten strafbaren Handlung[en], in den Katalog aufnimmt. Damit sind unter anderem Delikte wie Körperverletzung, (qualifizierte) gefährliche Drohung oder Datenbeschädigung als 'verfassungsgefährdender Angriff' zu subsumieren, sofern sie religiös oder ideologisch motiviert sind.

Diese Regelung setzt voraus, dass die Polizei erkennen kann, wann etwa eine gefährliche Drohung weltanschaulich motiviert ist, weil in diesem Falle der Staatsschutz zuständig wäre. Durch die Formulierung der 'in § 278e StGB genannten strafbaren Handlungen' werden nämlich die dort aufgezählten Straftatbestände unabhängig davon erfasst, ob die Straftat in einem terroristischen Zusammenhang begangen wird, wie es § 278c StGB für sich genommen ansonsten voraussetzt. Welchen Unterschied diese Formulierung macht, ist sogar für Menschen mit spezieller juristischer Expertise nicht einfach zu erkennen.

Die Adressaten der Norm sind aber nicht nur die Beamten, die zu deren Vollzug berufen sind, sondern auch alle Personen, in deren Grundrechte durch die Norm potentiell eingegriffen wird. Im Erkenntnis zur Aufhebung der Vorratsdatenspeicherung ist der Verfassungsgerichtshof eben diesem Argument gefolgt, weil der Individualantrag ansonsten unzulässig gewesen wäre. Daher muss die Norm nicht nur für speziell geschulte Beamte sondern auch für juristisch durchschnittlich verständige Menschen im Wesentlichen verständlich sein. Die Gestaltung des 'verfassungsgefährdenden Angriffs' nach § 6 PStSG erfüllt den Anspruch an eine faktenbasierte Sicherheitspolitik jedenfalls nicht, solange der Gesetzgeber nicht zu erklären vermag, aufgrund welcher Entwicklung welche der neu vorgeschlagenen Befugnisse notwendig geworden sind.

Routinemäßig enthalten die Materialien zum PStSG auch eine 'wirkungsorientierte Folgenabschätzung' (WFA). Bei Betrachtung des Inhalts der WFA zeigt sich, dass sich diese darauf beschränkt, die Folgen für den Bundeshaushalt zu beschreiben. Eine Folgenabschätzung im Hinblick auf die erwarteten Auswirkungen

auf die Sicherheitslage und die Aufklärungsarbeit im Rahmen gerichtlicher Strafverfahren nach der Strafprozessordnung, auf die Kriminalitätsentwicklung und die Aufklärungs- sowie die Präventionsstatistik fehlt ebenso wie eine Einschätzung der Auswirkungen auf die Grundrechte der in Österreich lebenden Menschen und auf die Gesellschaft insgesamt. Die Bezeichnung als 'wirkungsorientierte Folgenabschätzung' ist mit Hinsicht auf das vorliegende Dokument geradezu irreführend. Die Problemanalyse verzichtet auf jegliche Art von Statistik, Fallzahlen, konkreter Fallbeispiele oder dokumentierter konkreter Erfahrungen, welche die Notwendigkeit von Änderungen und die Einführung neuer und erweiterter Befugnisse objektiv nachvollziehbar werden ließen.

Die Notwendigkeit der Änderungen bzw. Neuerungen wird postuliert aber nicht begründet. In den Grundrechten, insbesondere der Europäischen Menschenrechtskonvention, zieht sich ein Prinzip klar durch: Die Rechtfertigungslast für Grundrechtseingriffe liegt beim Staat und nicht auf Seiten der Menschen, die den Eingriff in ihre Grundrechte für ungerechtfertigt halten.

Die 'Wer nichts zu verbergen hat, hat auch nichts zu befürchten'-Doktrin verkehrt diesen liberalen Abwehrcharakter unserer Grundrechte ins Gegenteil und verdächtigt alle, die für sich eine Sphäre ohne staatlichen Einblick als verfassungsrechtlich geschützten Grundzustand reklamieren. Wenn der Gesetzgeber Grundrechtseingriffe normiert, hat er auch ein Mindestmaß an sachlicher Begründung mitzuliefern, ansonsten ist von der Unverhältnismäßigkeit der fraglichen Maßnahme auszugehen.

Damit ein verfassungsgefährdender Angriff nach § 6 Abs. 2 Z 2 vorliegt, muss die Tat ideologisch oder religiös motiviert sein. Diese Hervorhebung religiös oder ideologisch motivierter Straftaten (die es auch schon in der bis zum 30.06.2016 bestehenden Regelung der erweiterten Gefahrenerforschung des § 21 Abs.3 Z 1 und 2 SPG gibt) ist im PStSG ebenso unsachlich. Eine solche unsachliche Differenzierung verstößt gegen Artikel 7 B-VG, da es nicht ersichtlich ist, warum 'ideologisch oder religiös motivierte Gewalt' eine größere Gefahr darstellen sollte als andere Kriminalität. Warum eine religiöse oder weltanschauliche Motivation schon grundsätzlich als gefährlich eingestuft wird, ist nur verständlich, wenn man die Religion oder Weltanschauung als 'abweichende Religion oder Weltanschauung' versteht.

Die Hervorhebung religiös oder weltanschaulich motivierter Kriminalität als Hervorhebung bestimmter, als fremd empfundenen Religionen oder Weltanschauungen birgt ua die Gefahr in sich, dass politischer Aktivismus, der mit solchen abweichenden Weltanschauungen verknüpft wird, schnell ins Visier der Ermittlungsbehörden gerät. Im Übrigen ist auch die Bewertung bestimmter Gefahren als verfassungsgefährdend durch den Gesetzgeber nichts anderes als der Ausdruck einer Weltanschauung.

Die Feststellung, ob eine bereits begangene Straftat ideologisch oder religiös motiviert war, stellt den Rechtsanwender typischerweise schon vor eine echte Herausforderung. Zur Beurteilung, ob ein 'verfassungsgefährdender Angriff' nach

§ 6 Abs. 2 Z 2 vorliegt, müssen diese Elemente der inneren Tatseite für Sachverhalte beurteilt werden, die noch nicht einmal die Schwelle einer konkreten Rechtsgutbedrohung im Sinne eines 'gefährlichen Angriffs' (§ 16 SPG) erreicht haben. Obwohl im Rahmen der Aufgabenerfüllung nach § 6 Abs. 1 in der Regel erst zu beurteilen ist, mit welcher Wahrscheinlichkeit (vgl. dazu oben 7.1.2.) ein 'verfassungsgefährdender Angriff' droht, ist die innere Motivation der potentiellen Täter die wichtigste Abgrenzung zur Aktivierung der Befugnisse nach dem PStSG. Eine derart unbestimmte Norm, die als Grundlage für schwere Grundrechtseingriffe dienen soll, verletzt das verfassungsrechtlich gebotene Determinierungsgebot.

Nachfolgend werden unter 7.3.1. einzelne Bestimmungen innerhalb des § 6 Abs. 2 als verfassungswidrig kritisiert und im Eventualbegehren — für den Fall, dass der VfGH den Argumenten zur Gesamtaufhebung des PStSG nicht folgt — einzeln bekämpft. Zusammengefasst besteht das Problem darin, dass die Definition des 'verfassungsgefährdenden Angriffs' in § 6 Abs. 2 einen weit überschießenden Anwendungsbereich der präventiven Überwachung normiert, damit in unverhältnismäßiger Weise Grundrechtseingriffe gestattet und daher verfassungswidrig ist.

Hingegen gibt es keinen Antrag, mit dem nur § 6 Abs. 2 oder der gesamte § 6 isoliert bekämpft würde. Der Grund dafür ist, dass im Falle der Aufhebung dieser zentralen Bestimmung kein vollziehungstauglicher Rest des Gesetzes verbleiben würde, weil damit dem PStSG quasi der Boden entzogen wäre. Die mangelnde Transparenz und Bestimmtheit des § 6 ist daher ein weiteres Argument für die Aufhebung des gesamten PStSG als verfassungswidrig.

Ebenfalls als Argument für die Gesamtaufhebung, nicht jedoch im Wege einer gesonderten Anfechtung im Rahmen der Eventualanträge, wird hier außerdem Kritik im Hinblick auf die Verweise in § 6 Abs. 2 PStSG auf weitere Tatbestände des materiellen Strafrechts vorgebracht.

Dies betrifft § 283, §§ 79 bis 82 Außenwirtschaftsgesetz 2011 sowie die 'Computer-Delikte', auf die § 6 Abs. 2 Z 5 PStSG verweist.

Es bleibt hier unbestritten, dass eine 'Verhetzung' nach § 283 StGB ein Ausmaß erreichen kann, dass dadurch tatsächlich die öffentliche Sicherheit in einer verfassungsgefährdenden Weise gefährdet sein kann, weshalb auch keine eigenständige (eventualiter beantragte) Anfechtung des Verweises im Rahmen der Definition des 'verfassungsgefährdenden Angriffs' erfolgt. Das Problem im Zusammenhang mit dem PStSG entsteht aber durch die bereits kritisierte enorme Unschärfe der Kriterien, bei deren Vorliegen eine Gefahrenlage zur Aktivierung der Kompetenzen des PStSG angenommen werden darf. Die Beurteilung, ob ein bestimmtes Verhalten als 'Verhetzung' zu qualifizieren ist, wirft häufig schon dann schwierige Rechtsfragen auf, wenn ein bestimmter Sachverhalt ex post subsumiert werden soll. Noch viel schwerer ist die Beurteilung, wann ein Verhalten, das noch nicht einmal die Schwelle eines ‚gefährlichen Angriffs' (§ 16 SPG) erreicht hat, so zu deuten ist, dass eine ernsthafte Wahrscheinlichkeit besteht,

dass dieses Verhalten später zu einer Bedrohung der nach § 283 Abs. 3 StGB geschützten Rechtsgüter werden könnte. Bei einem weiten Verständnis der Aufgabe könnte man eine sachliche aber scharfe Kritik an einer der in § 283 Abs. 1 Z 1 StGB genannten Gruppen[…] auch als Vorstufe zu einer späteren Verbreitung von Gewaltaufrufen deuten. Das rechtsstaatliche Risiko besteht darin, dass die weite Vorverlagerung der Präventionsaufgaben bei diesem Tatbestand geradezu eine Einladung zu Willkür darstellt, während kein effektives Kontroll- und Rechtsschutzsystem existiert, mit dem dieses Risiko zuverlässig beherrscht werden könnte.

Ganz ähnlich ist das Problem bei einer erweiterten Gefahrenerforschung zu den Delikten nach §§ 79 bis 82 Außenwirtschaftsgesetz 2011 gelagert. Seitens der materiellen Strafnorm liegt der Schwerpunkt der Kritik hier bei der Bestimmtheit aus der Sicht ex ante, welches Verhalten nach diesen Strafbestimmungen sanktioniert ist. Diese Tatbestände haben weitgehend sehr komplexe Voraussetzungen in einer Gemengelage aus zusammenhängenden sachlichen (wirtschaftlichen und technischen) und rechtlichen Fragen. Es müssen bestimmte Handelsnormen und Bescheide (teilweise der Europäischen Union) beachtet werden und die damit verbundenen Sachfragen können sehr komplex sein. Beispielsweise ist gerade bei technologischen Produkten auch im Softwarebereich manchmal schwierig festzustellen, ob eine bestimmte Technologie auch für militärische Zwecke verwendet werden könnte (sog. 'Dual Use'-Frage), weil dann das Anbieten in bestimmten Ländern verboten und nach dem AußWG sanktioniert wäre. Diese Komplexität in der Gefahrenerforschung zu erfassen, bevor sich ein Sachverhalt noch zum konkreten Angriff entwickelt hat, bietet für einen Rechtsstaat zu viel Interpretationsspielraum, um für Grundrechtseingriffe hinreichend bestimmt zu sein.

Auch bei den 'Cybercrime'-Straftatbeständen nach den §§ 118a, 119, 119a, 126a, 126b oder 126c StGB ergibt sich die Unbestimmtheit und die Unverhältnismäßigkeit erst in Kombination mit der systematischen weiten Vorverlagerung der Präventionsaufgaben durch Sicherheitsbehörden. Die Sachverhalte, mit welchen die genannten Delikte typischerweise verwirklicht werden, sind in den meisten Fällen von einer gewissen Komplexität im Rahmen verschiedener Handlungsabschnitte geprägt. Die Phänomene beginnen oft harmlos mit 'Spam'-E-Mails oder den ersten Schritten eines 'Social-Engineering', die für sich genommen noch relativ harmlos und nicht strafrechtlich sanktioniert sind. Diese Handlungen sind oft von rechtmäßiger sozialer oder wirtschaftlicher Interaktion nicht unterscheidbar. Schritt für Schritt verdichten sich diese Sachverhalte dann zur Bedrohung eines bestimmten Rechtsguts. Regelmäßig ergibt erst eine forensische Aufarbeitung (wenn überhaupt) ein vollständiges Bild, wie der Angriff durch die einzelnen Schritte zustande gekommen ist. Wenn sich nun in der Prävention der Sachverhalt bereits so verdichtet hat, dass bereits ein Angriff erkennbar ist, dann liegt auch ein 'gefährlicher Angriff' iSd § 16 SPG vor.

Vor dieser Schwelle aber ist die Ausdehnung der Ermittlungsbefugnisse nach dem PStSG zu solchen Sachverhalten für den Bereich der erweiterten Gefahrenerforschung eine Einladung, eine Bedrohungslage willkürlich anzunehmen.

Präventives Handeln ist hier oft kaum denkmöglich und dennoch steht in diesen Fällen auch die volle Breite der Maßnahmen undifferenziert zur Verfügung. Eine sachliche Einschränkung, etwa im Hinblick auf eine Beurteilung der Bedrohungslage durch CERT.at oder Vergleichbares, existiere zu § 6 Abs. 2 Z 5 PStSG nicht. Demgegenüber besteht kein effektives Kontroll- und Rechtsschutzsystem, das einer willkürlichen Rechtsanwendung systematisch entgegenstehen könnte.

Anschaulich ausgedrückt eröffnet die viel zu weite und in transparente Definition des 'verfassungsgefährdenden Angriffs' den zum 'Staatsschutz' berufenen Organen die Möglichkeit, Ermittlungen mit schweren Grundrechtseingriffen einzuleiten, um die 'Gefahr einer Gefahr' zu beurteilen, dass jemand möglicherweise zum ersten Mal ein 'Hass-Posting' irgendwo im Internet verfassen könnte. Dabei dürfen nach § 12 Abs. 1 Z 4 PStSG auch unmittelbare Kontakt- und Begleitpersonen in die Ermittlungen gezogen werden. Wie weit der Kreis der Ermittlungen dadurch potentiell gezogen wird, zeigen verschiedene Studien, wonach ein typischer Nutzer schon im Jahr 2009 zB in Facebook im Durchschnitt ca. 120 Freunde[…] hatte und diese Zahl im Jahr 2014 bei etwa 300 Freunden pro Nutzer liegt.[…]

Ein Bericht des 'Guardian' vom 28. Oktober 2013 zu den von Edward Snowden veröffentlichten Dokumenten belegt wiederum, dass die typische Überwachung sozialer Medien durch den US Amerikanischen Nachrichtendienst NSA Freundschaftsverknüpfungen bis zum dritten Grad reicht, also die Freunde der Freunde der Freunde eines Verdächtigen erfasst.[…] Bei der im Jahr 2013 angenommenen durchschnittlichen Zahl von 190 Freunden pro Nutzer in Facebook umfasst der Kreis nach der dritten Ableitung dann 1.334.978 Nutzer.

Diese Zahlen zeigen, dass in Kombination mit dem völlig unzureichenden Kontroll- und Rechtsschutzsystem so die große Gefahr einer uferlosen Ausweitung nachrichtendienstlicher Ermittlungen besteht.

In Sinne der eben vorgebrachten Argumente verletzt § 6 Abs. 2 PStSG, § 1 DSG 2000, Art. 8 und Art. 10 EMRK, das rechtsstaatliche Gebot des Art. 18 B-VG sowie Art. 7 B-VG im Sinne des allgemeinen Sachlichkeitsgebots.

7.3.1. Anfechtung einzelner Verweise in § 6 Abs. 2 PStSG

7.3.1.1. Landfriedensbruch in führender Teilnahme (§ 274 Abs.2 erster Fall StGB)

Der Landfriedensbruch in führender Teilnahme (§ 274 Abs.2 erster Fall StGB, 'Rädelsführerschaft') ist im PStSG als verfassungsgefährdender Angriff definiert (§ 6 Abs.2 Z 2), der die Zuständigkeit der Staatsschutzbehörden und damit weitreichende Überwachungsbefugnisse begründet, sofern die Tat ideologisch oder religiös motiviert ist.

Auch wenn die Bestimmung des § 274 StGB (in Kraft seit 01.01.2016) neugefasst wurde, bleibt sie insgesamt problematisch. Die Norm hat ihre Wurzeln in der Aufstandsbekämpfung des 19. Jahrhunderts und wurde in den letzten Jahren

vermehrt gegen Fußballfans und gegen politischen Protest herangezogen. Die generalpräventive Wirkung des Einsatzes von Strafrecht gegen Einzelne macht das jeweilige Milieu unattraktiv. Die bloße Teilnahme an einer Versammlung kann damit nämlich in unmittelbare Nähe zu einem strafrechtlichen Delikt gerückt werden. Wer also an einer Demonstration aufgrund zivilgesellschaftlichen Engagements teilnimmt, muss damit rechnen, sich selbst der Gefahr strafrechtlicher Verfolgung auszusetzen, wenn im Zuge dieser Demonstration auch nur einzelne Teilnehmer ein strafrechtlich sanktioniertes Verhalten setzen.

Damit wird von der Ausübung dieses verfassungsrechtlich gewährleisteten Rechts abgeschreckt und es kommt zu einem sogenannten 'Chilling-effect'. In der jüngeren Vergangenheit kam es zu einem verstärkten Einsatz gerichtlichen Strafrechts gegen Versammlungsteilnehmer. Polizei und Justiz wendeten neben dem Landfriedensbruch noch weitere Straftatbestände, wie z.B. §§ 284 und 285 StGB, wieder häufiger an. Zahlreiche Demonstrationsteilnehmer wurden auf diesen Grundlagen festgenommen und es kam zu entsprechenden Anzeigen. Wegen der großen Anzahl an potentiellen Tätern werden dabei Ermittlungen großen Ausmaßes und damit weit reichende Überwachung erlaubt.

Im Begutachtungsentwurf (110/ME XXV. GP) fanden sich noch der gesamte § 274 StGB sowie die §§ 284 und 285 StGB in der Definition des verfassungsgefährdenden Angriffs (allerdings ohne das Tatbestandsmerkmal der [damals] weltanschaulichen oder religiösen Motivation). Diese Delikte haben idR keinen terroristischen oder schwerkriminellen Hintergrund, der die Staatsschutzbehörden auf den Plan rufen müsste. Der Gesetzgeber hat teilweise auf die Kritik der Zivilgesellschaft reagiert und die noch im Begutachtungsentwurf enthaltenen §§ 284 und 285 StGB letztlich nicht im PStSG übernommen. Inwiefern der (in Bezug auf die Anwendungspraxis) ganz ähnlich gelagerte Landfriedensbruch (in führender Teilnahme) die verfassungsmäßige Ordnung insgesamt gefährden sollte, ist nicht ersichtlich.

Die genannten Risiken ließen sich möglicherweise mit einem starken Kontroll- und Rechtsschutzsystem angemessen eindämmen. Wie aber bereits die Ausführungen unter Punkt 6. des vorliegenden Antrags begründen, sind die im PStSG normierten Kontroll- und Rechtsschutzinstrumente nicht effektiv und genügen den Anforderungen des Artikel 13 EMRK nicht. Gleichzeitig knüpfen die weitreichenden Befugnisse nach dem PStSG (unter anderem) an die mögliche Drohung der Verwirklichung des Delikts nach § 274 Abs.2 erster Fall StGB, 'sofern diese ideologisch oder religiös motiviert ist'.

Durch das Zusammenwirken von mangelnder Normenklarheit, der weiten Vorverlagerung der Ermittlungen in den Bereich straffreier (möglicher) Vorbereitungshandlungen, den tiefgreifenden Eingriffsbefugnissen und dem mangelhaften Rechtsschutz verletzt die Norm die unter Punkt 6. genannten verfassungsgesetzlich gewährleisteten Rechte.

7.3.1.2. Terroristische Straftaten (§ 278c StGB)

Im Eventualantrag konkret bekämpft wird in § 6 Abs.2 Z 2 die Wortfolge 'oder in § 278c StGB genannten'. Die Definition ist einerseits unverhältnismäßig weit, weil sie zu viele Delikte in den Aufgabenbereich des Staatschutzes zieht. Wie bereits ausgeführt sind damit unter anderem Delikte wie Körperverletzung, (qualifizierte) gefährliche Drohung oder Datenbeschädigung als 'verfassungsgefährdender Angriff' zu qualifizieren, sofern sie religiös oder ideologisch motiviert sind. Außerdem ist die Regelung völlig intransparent und schon aus diesem Grund aufzuheben.

Die Verletzung der unter Punkt 6. genannten Grundrechte liegt einerseits in der mangelnden Qualität der gesetzlichen Grundlage. Andererseits knüpft das PStSG schon an den Verdacht einer möglichen Begehung in der Zukunft Befugnisse mit weitgehenden Grundrechtseingriffen, die aufgrund des mangelhaften Kontroll- und Rechtsschutzsystems für Missbrauch enorm anfällig sind. Aus diesen Gründen ist die Aufzählung des § 278c StGB in § 6 Abs.2 Z 2 verfassungswidrig.

7.3.1.3. Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses zugunsten des Auslands (§ 124 StGB)

Im Eventualantrag konkret bekämpft wird in § 6 Abs.2 Z 4 die Verweisung auf § 124 StGB. Es ist nicht erkennbar, warum jede 'Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses zugunsten des Auslands' automatisch einen verfassungsgefährdenden Angriff darstellt und in die ausschließliche Zuständigkeit der Staatsschutzorgane fallt.

Eine Eingrenzung auf Fälle betreffend kritische Infrastruktur wie bei den 'Computerdelikten' in der Aufzählung des § 6 Abs.2 Z 5 existiert dazu nicht. Die schlichte Aufzählung erscheint insofern jedenfalls überschießend. Die Einbeziehung dieses Straftatbestands in die Definition des 'verfassungsgefährdenden Angriffs' führt dazu, dass die 'Staatsschutzorgane' von Amts wegen potentiell bei jedem Unternehmen Ermittlungen führen und insbesondere Zugang zum IT-System eines betroffenen Unternehmens erlangen können.

Der Kreis der potentiell Betroffenen ist deshalb so weit, weil praktisch jeder Angriff auf das IT-System eines Unternehmens, wenn auch nur als Vorstufe, geeignet ist, sich Zugang zu Unternehmensdaten zu verschaffen und damit Geschäftsgeheimnisse zugunsten des Auslands auszuspionieren. Die Aufgabenstellungen nach § 6 Abs.1 PStSG sind so weit in den Präventivbereich vorverlagert, dass schon erste, für sich genommen noch relativ harmlose Attacken auf ein IT-System zumindest soweit einen Gefahrenverdacht begründen, dass Ermittlungen eingeleitet werden dürften, um die Wahrscheinlichkeit eines weiterführenden Angriffs mit dem Ziel der Wirtschaftsspionage zugunsten des Auslands zu erforschen.

An dieser Stelle sei daran erinnert, dass die von Edward Snowden im Frühjahr 2013 veröffentlichten Dokumente zur Überwachungspraxis des US-amerikanischen Geheimdienstes NSA an vielen Stellen belegen, dass die Überwachung auf strategisch wichtige Ziele im Bereich der Privatwirtschaft und deren

Geschäftsgeheimnisse gerichtet war. Da es zugleich bislang keine Belege gibt, dass sich diese Praxis geändert hätte, würden nach der hier bekämpften Rechtslage schon die 'Snowden-Leaks' einen hinreichenden Gefahrenverdacht begründen, um viele Unternehmen mit entsprechenden Ermittlungen vor solcher Wirtschaftsspionage zugunsten des Auslands 'zu schützen', ob die betroffenen Unternehmen dies wollen oder nicht.

In Verbindung mit dem mangelhaften Kontroll- und Rechtsschutzsystem bewirkt diese Norm unverhältnismäßige Grundrechtseingriffe und ist daher verfassungswidrig.

7.4 § 9 Abs. 1 PStSG (Datenverwendung, sensible Daten)

[…]

Angemessene Vorkehrungen zur Wahrung der Geheimhaltungsinteressen sind grundsätzlich schon immanenter Bestandteil des Datenschutzgrundrechts nach § 1 DSG 2000, was in § 14 DSG 2000 eine Ausgestaltung erfährt, und keine Besonderheit der 'sensiblen' oder der 'strafrechtsrelevanten' Daten. Die Formulierung könnte den Eindruck erwecken, bei allen anderen personenbezogenen Daten seien keine angemessenen Vorkehrungen notwendig, um die Geheimhaltungsinteressen zu wahren. Das eigentliche Problem liegt aber darin, dass diese Norm — als Teil der besonderen gesetzlichen Ermächtigung zur Verarbeitung sensibler Daten iSd § 9 Z 3 DSG 2000 — selbst eine nähere Beschreibung vornehmen sollte, welche angemessenen Vorkehrungen zu treffen sind, anstatt nur den Kern des ohnehin anwendbaren § 14 DSG 2000 zu wiederholen. Die Antragsteller/innen sind sich bewusst, dass hier möglicherweise entgegen zu halten ist, dass dieses Problem mit der Beseitigung der bekämpften Wortfolge auch nicht behoben wird. In diesem Sinne ist das Argument auch als weiterer Beitrag zur Begründung der notwendigen Gesamtaufhebung des PStSG zu sehen.

Dies trifft jedenfalls auch auf den letzten Satz des § 9 Abs.1 zu, welcher nicht gesondert bekämpft wird, weil das Problem in einer Unterlassung liegt. Das Umgehungsverbot von gesetzlichen Verschwiegenheitspflichten sollte nämlich angesichts der Reichweite und der niederschwelligen Verfügbarkeit aller Befugnisse nach § 11 weiter gefasst sein. Dass im Strafverfahren die Berechtigung zur Entschlagung nach § 157 StPO eher eng gehalten ist, lässt sich durch das engmaschige Rechtsschutznetz der Strafprozessordnung rechtfertigen. Im PStSG sollten aber auch gesetzliche Verschwiegenheitspflichten, die nicht von § 157 erfasst sind (zB das allgemeine Arzt-Patienten-Geheimnis) ebenfalls berücksichtigt und deren Durchbrechung als ultima ratio an strengere Anforderungen geknüpft werden.

Ein besonderes Gefährdungspotential für die Demokratie besteht vor allein darin, dass auf Basis der Befugnisse des PStSG zumindest im Hinblick auf das Ermittlungsverfahren die Immunität von Nationalratsabgeordneten unterwandert werden darf. Der Ermittlungsschutz des § 157 StPO greift hier nicht. Außerdem setzt die Definition des 'verfassungsgefährdenden Angriffs' nur die 'rechts-

widrige Verwirklichung des Tatbestandes' einer in der Folge aufgezählten strafbaren Handlung voraus.

Weil die durch Artikel 57 B-VG garantierte Immunität nicht per se die Strafbarkeit der Handlungen der Abgeordneten ausschließt, sind Ermittlungen auch trotz der 'politischen Immunität' zulässig. Ein Vernehmungsverbot ähnlich dem § 155 Abs.1 Z 3 StPO im Hinblick auf 'Personen, denen Zugang zu klassifizierten Informationen des Nationalrates oder des Bundesrates gewährt wurde, soweit sie gemäß § 18 Abs.1 des Bundesgesetzes über die Informationsordnung des Nationalrates und des Bundesrates, BGBl. I Nr. 101/2014, zur Verschwiegenheit verpflichtet sind', findet sich im PStSG nicht.

7.5 § 10 (Ermittlungsdienst für Zwecke des polizeilichen Staatsschutzes)

[…]

7.5.1 Zu Absatz 1 (Zwecke der Datenverarbeitung):

Die Definition der Zwecke für eine rechtmäßige Datenverarbeitung der verschiedensten Kategorien personenbezogener Daten, darunter gemäß § 10 Abs. 1 PStSG ausdrücklich auch sensible Daten im Sinne des § 4 Z 2 DSG 2000, ist praktisch mit der Definition der Aufgaben der 'Staatsschutzorgane' gleichgesetzt. Diese Bestimmung ist gemeinsam mit der in § 12 Abs. 1 PStSG folgenden Zweckbindung zu lesen. Demzufolge ist die Verarbeitung der dort aufgelisteten personenbezogenen Daten zu Betroffenen sowie zu Kontakt- und Begleitpersonen sowie zu Informanten und schließlich von tat- und fallbezogenen Informationen zum Zweck der 'Bewertung von wahrscheinlichen Gefährdungen sowie zum Erkennen von Zusammenhängen und Strukturen mittels operativer oder strategischer Analyse'[…] erlaubt. Das heißt in Umkehrschluss, dass die Organwalter der 'Staatsschutzorgane', solange sie nur dienstlich handeln, niemals reflektieren müssen, ob und welche personenbezogenen Daten sie für welche bestimmten Zwecke verarbeiten dürfen — weil sie schlichtweg alle im PStSG aufgezählten sowie 'aus allen anderen verfügbaren Quellen' (§ 10 Abs. 5 PStSG, '...insbesondere durch Zugriff etwa auf im Internet öffentlich zugängliche Daten') ermittelten personenbezogenen Daten verarbeiten dürfen, soweit dies (nach Einschätzung der Organwalter) zur Erfüllung ihrer Aufgaben erforderlich ist. Diese letztlich pauschale Ermächtigung ist unverhältnismäßig.

Die Anfechtung des § 10 Abs. 1 Z 1, 2 und 3 erfolgt schon im Zusammenhang mit der Anfechtung der Aufgabendefinition des § 6 Abs. 1 und ist damit nach Ansicht der Antragsteller/innen logisch untrennbar verbunden. Denn die Definition der Aufgaben und die zugehörigen Ermittlungsbefugnisse wären nicht viel wert, wenn am Ende keine Aufzeichnung der Ergebnisse erfolgen dürfte.

Besonders bekämpft wird jedoch § 10 Abs. 1 letzter Satz: 'wobei sensible Daten gemäß § 4 Z 2 Datenschutzgesetz 2000 — DSG 2000, BGBl. I Nr. 165/1999, nur insoweit ermittelt und weiterverarbeitet werden dürfen, als diese für die Erfüllung der Aufgabe unbedingt erforderlich sind.'

Komplementär mit § 9 Abs. 1 soll diese Norm die besondere gesetzliche Ermächtigung zur Verarbeitung sensibler Daten iSd § 9 Z 3 DSG 2000 sein. Die Bedeutung ist mit anderen Worten: wenn das BVT zuständig ist, darf es auch sensible Daten verarbeiten. Wenn eine Datenverarbeitung für die Aufgabenerfüllung nur bedingt oder gar nicht erforderlich ist, ist ihre Durchführung auch dann rechtswidrig, wenn es keine sensiblen Daten sind. Das Gesetz ordnet also eine Selbstverständlichkeit an und erweckt zugleich den falschen Eindruck, diese gelte nicht für nicht sensible Daten. Vielmehr sollte es konkretisieren, wann eine solche unbedingte Erforderlichkeit besteht.

7.5.2 Absatz 2 und 5 (Weiterverarbeitung ermittelter Daten, automationsunterstützter Datenabgleich)

Zunächst wird in Absatz 2 die Befugnis zur Datenverarbeitung ausdrücklich von der 'Rasterfahndung' abgegrenzt (automationsunterstützter Datenabgleich im Sinne des § 141 StPO. Gemäß Absatz 5 sind die 'Staatschutzbehörden' dem gegenüber ausdrücklich berechtigt,

'personenbezogene Daten aus allen anderen verfügbaren Quellen durch Einsatz geeigneter Mittel, insbesondere durch Zugriff etwa auf im Internet öffentlich zugängliche Daten, zu ermitteln und weiterzuverarbeiten'.

Die Ermittlung und Weiterverarbeitung 'durch Zugriff etwa auf im Internet öffentlich zugängliche Daten' kann nun durch Menschen erfolgen, die systematisch 'das Internet' nach bestimmten Schlagworten durchsuchen. Vorstellbar ist etwa, dass Beamte mit frei verfügbaren Diensten wie Google und Facebook ihre online-Recherchen ausführen. An dieser Stelle sei angemerkt, dass die öffentliche Debatte in den 1990er-Jahren zur Einführung der 'Rasterfahndung' schon große Kritik seitens der Zivilgesellschaft hervorbrachte — weshalb die Maßnahme zunächst auch nur befristet eingeführt wurde — obwohl die Möglichkeiten einer heutigen einfachen 'Google-Suche' damals kaum vorstellbar waren. Die ersten Suchmaschinen damals[…] waren außerdem nicht nur viel weniger komplex, auch die Größenordnung der verfügbaren Datenmenge war um Dimensionen kleiner.

Aus damaliger Sicht wurden die — vereinzelt schon damals antizipierten — heutigen Möglichkeiten für eine 'elektronische Rasterfahndung' gewissermaßen als 'science fiction'-Argumente gar nicht ernsthaft in die Debatte einbezogen. Eingedenk der Tatsache, dass man heute ohne technische Kenntnisse auch zB über Facebook Gesichtserkennungsdienste zur Verfügung hat, um mit einem Referenzbild zu einer Person diese im Netz wiederzufinden, käme das aus damaliger Sicht für sich bereits der Eingriffsintensität einer 'Rasterfahndung' gleich.

Nun ist aber anzunehmen, dass moderne Ermittlungstechnologien auch den österreichischen Verfassungsschützern zur Verfügung stehen. Hierzu gibt es einen großen Markt privater Anbieter für Software zum Zweck der sogenannten 'Open Source Intelligence' (OSINT). Im Prinzip handelt es sich um hochspeziali-

sierte Suchmaschinen-tools, die speziell für nachrichtendienstliche und/oder polizeiliche Ermittlungsbedürfnisse maßgeschneidert sind und systematisch auf der Basis bestimmter Algorithmen alle im Internet zugänglichen Daten durchsuchen, um daraus Informationen zu gewinnen. Die Funktionen der öffentlich verfügbaren Suchmaschinen und sozialen Netzwerke werden dabei regelmäßig automatisiert mitgenutzt.

Nach § 10 PStSG dürfen einerseits mit weitgehenden Befugnissen alle möglichen (auch sensiblen) Daten aus nicht öffentlichen Quellen ermittelt werden, auch wenn sie dem Kommunikationsgeheimnis oder einem sonstigen Berufsgeheimnis unterliegen (vgl. § 12 PStSG, außer der Geheimnisschutz liegt innerhalb jener Grenzen, wo § 157 StPO ein Recht zur Zeugnisverweigerung garantiert. All diese Daten dürfen dann — wohl auch in Verbindung mit den 'im Internet' ermittelten Daten — gemeinsam weiterverarbeitet werden.

Es stellt sich daher die Frage, worin eigentlich die Abgrenzung zur 'kleinen Rasterfahndung' gemäß 141 Abs. 2 StPO besteht. Dort heißt es:
'(2) Datenabgleich ist zulässig, wenn die Aufklärung eines Verbrechens (§ 17 Abs. 1 StGB) ansonsten wesentlich erschwert wäre und nur solche Daten einbezogen werden, die Gerichte, Staatsanwaltschaften und Sicherheitsbehörden für Zwecke eines bereits anhängigen Strafverfahrens oder sonst auf Grund bestehender Bundes- oder Landesgesetze ermittelt oder verarbeitet haben.'

Das Problem besteht schon dem Grunde nach darin, dass nicht exakt definiert ist, was unter einem 'Datenabgleich' zu verstehen ist. Nach der Legaldefinition des § 141 Abs. 1 StPO ist 'Datenabgleich'

'der automationsunterstützte Vergleich von Daten (§ 4 Z 1 DSG 2000) einer Datenanwendung, die bestimmte, den mutmaßlichen Täter kennzeichnende oder ausschließende Merkmale enthalten, mit Daten einer anderen Datenanwendung, die solche Merkmale enthalten, um Personen festzustellen, die auf Grund dieser Merkmale als Verdächtige in Betracht kommen'.

Nach Auffassung der Antragsteller/innen ist auch eine systematische Sammlung von Daten, welche die Behörde aus allen im Internet (und sonst) verfügbaren Quellen anlegt, eine Datenanwendung im Sinne dieser Bestimmung. Es handelt sich dann zumindest um interne Datenanwendungen der Sicherheits- und/oder Strafverfolgungsbehörden, auf die sich § 141 Abs. 2 StPO bezieht.

Festzuhalten ist, dass dieses Problem nicht durch das vorgeschlagene PStSG neu entsteht, sondern schon bisher aufgrund der unpräzisen Formulierungen — sowohl in § 141 StPO als auch im bestehenden § 53 Abs. 2 SPG — latent ist. Durch die ausdrückliche Erweiterung der gesetzlichen Grundlagen auf die Verarbeitung von insbesondere durch Zugriff etwa auf im Internet öffentlich zugängliche Daten, die großzügige Erweiterung sonstiger Ermittlungsbefugnisse der 'Staatsschutzorgane' sowie den reduzierten Rechtsschutz werden die Abgrenzungsschwierigkeiten zur 'Rasterfahndung' nun aber potenziert.

Logisch definieren lässt sich die Rasterfahndung als Schnittmengenbildung nach Merkmalen von Daten aus verschiedenen Quellen. Typischerweise besteht dabei Vollzugriff auf die jeweiligen Datenbanken[.] Daraus wird dann — vereinfacht gesagt — die Schnittmenge gebildet. Technisch gesehen wäre es möglich, diese 'Schnittmengenbildung' über mehrere Datenbanken hinweg mit einer eigenen Software zu bewerkstelligen, die selbst gar kein Teil der jeweiligen Datenanwendung ist, sondern nur über Schnittstellen auf diese zugreift. Die Ermittler könnten die daraus gewonnenen Informationen sehen, ohne dass dafür ein neuer Eintrag in den jeweils verglichenen Datenbanken entsteht.

Auch die Zugriffsprotokollierung würde in diesem Fall nur einen Zugriff auf die einzelnen Werte, die aus der jeweiligen Datenbank verwendet wurden, offenlegen; der Umstand der Informationsgewinnung durch 'Data-Mining' wäre jedoch nicht erkennbar.

Festzuhalten ist, dass auch die Sammlung und Aufbewahrung allgemein zugänglicher Quellen wie Artikel in Zeitschriften einen Eingriff in das Privatleben darstellt, sofern sie systematisch durch Behörden (Geheimdienste, Verfassungsschutz) erfolgt.[…] In § 10 Abs. 5 PStSG besteht die Einschränkung nur in Bezug auf die demonstrativ genannten 'öffentlich zugängliche Daten' im Internet, während ansonsten als Auffangtatbestand 'personenbezogene Daten aus allen anderen verfügbaren Quellen' ermittelt werden dürfen.

Die bekämpften Bestimmungen in § 10 PStSG sind verfassungswidrig, weil sie eine aus den genannten Gründen unverhältnismäßige Ermittlung und Weiterverarbeitung personenbezogener Daten erlauben. Zur Ermittlung von im Internet öffentlich zugänglicher Daten und Informationen gibt es überhaupt keine Grenzen im Hinblick auf die daraus entstehende systematische Informationssammlung sowie die technischen Möglichkeiten zur Ermittlung selbst. Die Unzulässigkeit der 'Rasterfahndung' (§ 141 StPO) ist zwar normiert, wird aber durch die weiteren Befugnisse zur Datensammlung und Zusammenführung in einem Informationsverbundsystem praktisch ad absurdum geführt.

Die mangelhaften Kontroll- und Rechtsschutzinstrumente sorgen dafür, dass allfällige Grenzüberschreitungen in der Praxis nicht bemerkt werden. Daraus folgt eine Verletzung von § 1 DSG 2000, Art 8 EMRK für sich sowie in Verbindung mit Art 13 EMRK.

7.6 § 11 PStSG (Besondere Bestimmungen für die Ermittlungen)

[…]

7.6.1 Zu Absatz 1 (Besondere Ermittlungsbefugnisse):
Observation nach § 54 Abs. 2 SPG und technische Hilfsmittel nach § 54 Abs. 2a SPG sind aus dem Bestand des SPG auch im PStSG vorgesehen. Durch die legistische Technik der Verweisung wird aber schwerer lesbar, was damit eigentlich normiert wird. § 54 Abs. 2a SPG lautet:

'(2a) Zur Unterstützung der Observation gemäß § 54 Abs. 2 ist der Einsatz technischer Mittel, die im Wege der Übertragung von Signalen die Feststellung des räumlichen Bereichs ermöglichen, in dem sich die beobachtete Person oder der beobachtete Gegenstand befindet, zulässig, wenn die Observation sonst aussichtslos oder erheblich erschwert wäre.'

Damit sind sowohl Peilsender, vor allem aber auch sog 'IMSI-Catcher[…] adressiert, die ebenso zur Unterstützung von Observationen eingesetzt werden.

Die in § 11 Abs. 1 Z 2 PStSG vorgesehene verdeckte Ermittlung besteht sowohl nach 54 Abs. 3 SPG als auch nach § 131 StPO. Auffällig ist, dass die Strafprozessordnung deutlich strenger ist, was die Zulässigkeitsvoraussetzungen betrifft. Nach der StPO darf die Maßnahme von der Staatsanwaltschaft höchstens für einen Zeitraum von drei Monaten angeordnet werden. Demgegenüber kann die Ermächtigung des Rechtsschutzbeauftragten für eine verdeckte Ermittlung nach dem PStSG jeweils für einen Zeitraum von sechs Monaten erteilt werden.

Der im Vergleich zur StPO erleichterte Zugang zu diesem Ermittlungsinstrument in Verbindung mit einem gleichzeitig sehr schwachen Rechtsschutzsystem bewirken die Unverhältnismäßigkeit und damit eine Verletzung der unter Punkt 6. genannten materiellen Grundrechte. Außerdem verletzt die unsachliche Regelung Artikel 7 B-VG. Zwar behandelt die StPO, die sich auf bereits begangene oder zumindest versuchte Straftaten bezieht, nicht exakt dieselben Sachverhalte wie das PStSG, das sich auf die präventive Gefahrenerforschung bezieht. Insofern darf der Gesetzgeber die ungleichen Sachverhalte auch ungleich regeln.

Aber ein wertender Vergleich mit den strengeren Bestimmungen der StPO zeigt, dass es gerade bei Ermittlungen im Vorfeld der Strafbarkeit und unter der Schwelle eines 'gefährlichen Angriffs' (§ 16 SPG) sachlich geboten wäre, die Voraussetzungen strenger zu normieren. § 11 Abs. 1 Z 2 PStSG erlaubt aber im Gegenteil eine verdeckte Ermittlung unter deutlich weniger strengen Voraussetzungen. Eine Begründung in den Gesetzesmaterialien fehlt dazu. Die Bestimmung ist daher unsachlich und verletzt Art 7 B-VG im Sinne des allgemeinen Sachlichkeitsgebots.

Zu Z 3 (Einsatz von Bild- und Tonaufzeichnungsgeräten):

§ 11 Abs. 1 Z 3 PStSG erlaubt den Einsatz von Bild- und Tonaufzeichnungsgeräten und verweist in Klammer auf die parallel weiterhin bestehende Bestimmung des § 54 Abs. 4 SPG. Eine Gegenüberstellung der beiden Normen zeigt einen auffälligen Unterschied:

| § 11 PStSG — Besondere Bestimmungen für die Ermittlungen | § 54 SPG — Besondere Bestimmungen für die Ermittlung |
|---|---|
| § 11 (1) Zur erweiterten | § 54 (4) Die Ermittlung |

| | |
|---|---|
| Gefahrenerforschung (§ 6 Abs. 1 Z 1) und zum vorbeugenden Schutz vor verfassungsgefährdenden Angriffen (§ 6 Abs. 1 Z 2) ist die Ermittlung personenbezogener Daten nach Maßgabe des § 9 und unter den Voraussetzungen des § 14 zulässig durch (…)<br>3. Einsatz von Bild- und Tonaufzeichnungsgeräten (§ 54 Abs. 4 SPG); dieser darf verdeckt erfolgen, wenn die Erfüllung der Aufgabe ansonsten aussichtslos wäre | personenbezogener Daten mit Bild- und Tonaufzeichnungsgeräten ist nur für die Abwehr gefährlicher Angriffe oder krimineller Verbindungen und zur erweiterten Gefahrenerforschung (§ 21 Abs. 3) zulässig; sie darf unter den Voraussetzungen des Abs. 3 auch verdeckt erfolgen. Das Fernmeldegeheimnis bleibt unberührt. Unzulässig ist die Ermittlung personenbezogener Daten jedoch<br><br>1. mit Tonaufzeichnungsgeräten, um nichtöffentliche und nicht in Anwesenheit eines Ermittelnden erfolgende Äußerungen aufzuzeichnen;<br>2. mit Bildaufzeichnungsgeräten, um nichtöffentliches und nicht im Wahrnehmungsbereich eines Ermittelnden erfolgendes Verhalten aufzuzeichnen. |

Das SPG enthält also die wesentlichen Ausnahmen, dass nichtöffentliche und nicht in Anwesenheit eines Ermittelnden erfolgende Äußerungen weder in Bild noch in Ton aufgezeichnet werden dürfen. Das PStSG enthält diese Einschränkung hingegen nicht. Nun liegt das Wesen dieser in § 54 Abs. 4 SPG ausdrücklich normierten Einschränkung aber in der Abgrenzung von der Befugnis nach § 136 StPO, also die 'optische und akustische Überwachung von Personen' (vulgo 'Späh- und Lauschangriff'). Dieser Begriff wird zunächst in § 134 Z 4 StPO definiert als

'die Überwachung des Verhaltens von Personen unter Durchbrechung ihrer Privatsphäre und der Äußerungen von Personen, die nicht zur unmittelbaren Kenntnisnahme Dritter bestimmt sind, unter Verwendung technischer Mittel zur Bild- oder Tonübertragung und zur Bild- oder Tonaufnahme ohne Kenntnis der Betroffenen'.

Im Vergleich zu den Regelungen in SPG und PStSG fallt auf, dass die StPO ausdrücklich auch die technischen Mittel zur Bild- und Tonübertragung nennt, während für die Gefahrenabwehr und Erforschung nur die technischen Mittel zur Aufzeichnung genannt sind. Das Wesen des Lausch- und Spähangriffs nach § 136 StPO liegt eben darin, dass Bild und Ton aus der Ferne aufgezeichnet werden und eben kein Ermittler unmittelbar anwesend sein muss. Genau dieses Szenario schließen die Ausnahmen in § 54 Abs. 4 SPG ausdrücklich aus und bewirken damit eine eindeutige Abgrenzung zum 'Lausch- und Spähangriff' nach der StPO.

Wenn nun diese Ausnahmen in § 11 Abs. 1 Z 3 PStSG nicht aufgenommen wurden, obwohl ansonsten auf die Parallelbestimmung des § 54 Abs. 4 SPG verwiesen wird, muss daraus abgeleitet werden, dass der Gesetzgeber damit auch beabsichtigt, diese Einschränkung im PStSG gerade nicht zu normieren.

Es handelt sich also nicht um eine planwidrige Lücke, die durch Analogie zu schließen wäre, sondern um eine bewusste Ausweitung der Befugnisse gegenüber der 'normalen' Sicherheitspolizei nach SPG. Nach diesem Verständnis kommen jedoch große Zweifel auf, welche Unterschiede praktisch zwischen dem 'Lausch- und Spähangriff' nach § 136 StPO und der 'Bild- und Tonaufzeichnung' nach § 11 Abs. 1 Z 3 PStSG besteht — zumal die StPO diese Befugnis an deutlich strengere Voraussetzungen und auch Rechtschutzvorkehrungen knüpft.

Die erweiterte (oder bestenfalls missverständliche) Regelung des § 11 Abs. 1 Z 3 PStSG normiert einen schweren Eingriff in die Privatsphäre und verletzt § 1 DSG 2000 sowie Art 8 EMRK, weil sie keine Differenzierung innerhalb des Aufgabenbereichs in Bezug auf die Schwere der Bedrohung vornimmt und ihr Wortlaut die wichtige Abgrenzung zum 'Lausch- und Spähangriff' nach der StPO in Frage stellt. Durch den mangelhaften Rechtsschutz bewirkt die Regelung eine hohe Missbrauchsgefahr. Schließlich ist die unterschiedliche Regelung im Wortlaut im Vergleich zu § 54 Abs. 4 SPG sachlich nicht gerechtfertigt und verletzt daher Art 7 B-VG.

Zu Z 5 (Auskunft über Standortdaten)

Die Befugnis nach § 11 Abs. 1 Z 5 für die Auskunft über IP-Adressen und die zugehörigen Anschlussinhaber sowie die aktuelle und historische Standortdatenerfassung erfährt in der neuen Fassung der Regierungsvorlage eine wichtige ausdrückliche Ausdehnung. Die IP-Adressen-Auskünfte, das heißt die Zugangsdaten zu einem Internetanschluss, dürfen von den Staatsschutzorganen nicht nur für Ermittlungen gegen bestimmte Personen sondern auch gegen Gruppierungen gefordert werden. Gleichzeitig muss auch der Rechtsschutzbeauftragte die Maßnahme nur abstrakt für sechs Monate im Voraus für die Beobachtung einer gefährlichen 'Gruppierung' genehmigen. Hier können die Behörden also die Reichweite der Ermittlungsmaßnahmen sehr flexibel steuern, in dem der Kreis der Verdächtigen enger oder weiter definiert wird. Ob ein Eingriff in die verfassungsrechtlich geschützte Privatsphäre eines Betroffenen (Verdächtigen) auch im Einzelfall verhältnismäßig ist, wird nicht mehr überprüft, wenn die Genehmigung

insgesamt bezüglich der Gruppierung vorliegt, welcher das Individuum zugeordnet wird.

Daran anschließend dehnt Ziffer 5 die Überwachungsbefugnis ausdrücklich auf 'Kontakt- und Begleitpersonen' aus, womit der Kreis der Betroffenen gerade im Falle der Beobachtung einer gefährlichen 'Gruppierung' in der Praxis stark anwachsen wird. Das ist relevant, weil damit die Gefahr droht, dass immer weitere Kreise der Bevölkerung von Ermittlungsmaßnahmen betroffen sein werden und damit deren personenbezogene Daten auch in den Datenbanken der 'Staatsschutzorgane' verarbeitet werden.

In Bezug auf Standortdaten zu einem mobilen Endgerät wird der Kreis der potentiell Betroffenen sowohl im SPG als auch — durch die Änderung mit der Regierungsvorlage ausdrücklich — im PStSG ausgedehnt. Nach der derzeit geltenden Rechtslage dürfen die Sicherheitsbehörden gemäß § 53 Abs. 3b SPG 'Auskunft über Standortdaten und die internationale Mobilteilnehmererkennung (IMSI) der von dem gefährdeten oder diesen begleitenden Menschen mitgeführten Endeinrichtung [z]u verlangen sowie technische Mittel zur Lokalisierung der Endeinrichtung zum Einsatz [zu] bringen.'

Der letzte Halbsatz ist die abstrakte Ermächtigung zum Einsatz von sog. 'IMSI-Catchern' (siehe dazu schon oben Punkt 7.6.1.).

Nun erfolgt im SPG (siehe unten zu den SPG Änderungen Z 9) die Erweiterung, dass diese Befugnis auch auf den 'Gefährder' ausgedehnt wird. Das PStSG geht noch einen deutlichen Schritt weiter, weil nach dem Wortlaut des § 11 Abs. 1 Z 5 die Auskünfte zu Standortdaten und IMSI zulässig zur Überwachung einer 'Gruppierung', von Betroffenen im Sinne des § 6 Abs. 1 Z 2 PStSG (= Gefährder) sowie deren Kontakt oder Begleitpersonen sind. Diese Ausdehnung ist schon deshalb bemerkenswert, weil seit der Schaffung der ursprünglichen Befugnis in § 53 Abs.3b SPG durch die SPG-Novelle 2007 in der öffentlichen Debatte seitens des Bundesministeriums für Inneres stets prominent argumentiert wurde, dass diese Befugnis eigentlich nur geschaffen wurde, um vermisste Wanderer oder Schifahrer zu finden oder suizidgefährdete Menschen rechtzeitig aufzufinden.

Für die Prävention oder Aufklärung von Straftaten wurde stets darauf verwiesen, dass Standortdatenauskünfte nach der Strafprozessordnung (StPO) nur aufgrund eines Gerichtsbeschlusses zulässig sind.

Offenbar wird also die bisherige Rechtfertigung ohne weitere Erklärung dazu aufgegeben und der Polizei sowie den Staatsschutzorganen damit selbst das Instrument in die Hand gelegt, Menschen aktuell und historisch zu lokalisieren und allenfalls Bewegungsprofile daraus zu erstellen. Dies ist ein besonders anschauliches Beispiel für die schleichende Ausdehnung von Befugnissen und der damit verbundenen Grundrechtseingriffe.

Schließlich zeigt § 14 Abs. 2 PStSG, dass die Maßnahme der Standortdatenermittlung auch pro futuro immer wieder fortgesetzt und damit 'laufend' genehmigt

werden kann, so dass über jeweils 6 Monate hinweg vollständige Bewegungsprofile erstellt werden können — also eine Art 'quick freeze'-Vorratsdatenspeicherung ohne richterliche Genehmigung.

Die Regelung greift in unverhältnismäßiger Weise in Art 8 EMRK ein, der den Menschen auch den Anspruch gewährt, sich auch im öffentlichen Raum grundsätzlich unbeobachtet von staatlichen Organen zu bewegen. Die bekämpfte Bestimmung eröffnet die Möglichkeit, die systematische Beobachtung von Bürgern unangemessen auszudehnen. Durch die Erfassung der Ergebnisse in einer Datenbank liegt auch ein Eingriff in das Datenschutzgrundrecht des § 1 DSG 2000 vor, der insbesondere auch aufgrund des mangelhaften Rechtschutzes ungerechtfertigt ist. Die Bestimmung ist daher verfassungswidrig.

Zu Z 6 (PNR für ALLE Verkehrsmittel, Boden, Wasser, Luft):

Z 6 erlaubt den Zugriff auf den 'Passenger Name Record' jeder Art von Verkehrsmittel. Ähnlich wie beim Zugriff auf Telekommunikationsdaten (zumindest nach der StPO) sollten die Zugriffsbefugnisse auch hier beschränkt werden, sodass der Gesetzgeber schon in der gesetzlichen Eingriffsgrundlage eine Abwägung vorzeichnet, die durch eine Verhältnismäßigkeitsprüfung im Einzelfall ergänzt werden soll. Derzeit ist zur Vorratsspeicherung von Fluggastdaten im Zusammenhang mit einem Abkommen zwischen der EU und Kanada ein Verfahren vor dem EuGH anhängig, wobei mit einer baldigen Entscheidung zu rechnen ist.

Falls der EuGH ähnlich wie im Urteil zur 'Vorratsdatenspeicherung' von Telekommunikationsdaten auch Vorgaben zur Verwendung der Daten aussprechen sollte, sind diese dringend zu berücksichtigen. Im Übrigen besteht auch im Zusammenhang mit Reisebewegungen das Problem, dass damit gesetzlich anerkannte Verschwiegenheitspflichten (oder Berechtigungen) unterwandert werden können.

Zu Z 7 (Auskünfte Verkehrs- und Zugangsdaten TKG und ECG).

Diese Ermächtigung ist der wohl schwerwiegendste Eingriff ins Telekommunikationsgeheimnis seit der Vorratsdatenspeicherung. Der Gesetzgeber der Strafprozessordnung ging geradezu selbstverständlich davon aus, dass bei diesen Eingriffen in das Kommunikationsgeheimnis (§ 93 TKG) jedenfalls ein Richtervorbehalt als Rechtsschutzgarantie zu installieren ist. Daher sind die vergleichbaren Ermittlungsbefugnisse nach der Strafprozessordnung — also wenn es um die Aufklärung konkreter, bereits begangener Straftaten geht — gemäß [§]§ 134 ff. StPO nur aufgrund einer Anordnung der Staatsanwaltschaft, die ein Gericht zu bewilligen hat, zulässig. Diese Grenze respektiert aktuell sogar das SPG, weil auch der geltende § 53 Abs.3a SPG keine umfassenden Verkehrs- und Standortdatenauskünfte zulässt. § 11 Abs.1 Z 7 PStSG gewährt demgegenüber umfassende Eingriffe in das Kommunikationsgeheimnis ohne Richtervorbehalt.

In der Rechtsprechung und Literatur ist die Meinung zunehmend verbreitet, dass auch Verkehrsdaten vom Schutz des Fernmeldegeheimnisses gemäß Art 10a

StGG erfasst sind[…], demzufolge darf eine Auskunft über Verkehrsdaten ausschließlich aufgrund einer richterlichen Genehmigung erfolgen. Dieser (gegenüber dem in Art 10 StGG normierten Briefgeheimnis) erweiterte Umfang des Art 10a StGG wurde in der Vergangenheit mehrfach bezweifelt, ergibt sich jedoch — trotz der Ähnlichkeit zwischen Brief- und Fernmeldegeheimnis und der Vorbildwirkung des Art 10 StGG für den erst 1975 eingeführten Art 10a StGG — klar aus den zwischen den beiden Grundrechten bestehenden Unterschieden.

Dass der Gesetzgeber für den Fernmeldeverkehr gegenüber dem Briefgeheimnis höheren Schutz normiert hat, indem er als Eingriffsvoraussetzung in allen Fällen zwingend einen richterlichen Befehl verlangt, zeigt bereits, dass die Überlegungen zum Schutzbereich des Art 10 StGG nicht undifferenziert auf Art 10a StGG übertragen werden können. Zudem sind die jeweils betroffenen Daten unterschiedlich schutzbedürftig. Im Kern schützt das Fernmeldegeheimnis — in Anlehnung an Art 10 StGG — den Inhalt der übertragenen Kommunikation. Anders als das Briefgeheimnis geht der Schutz des Art 10a StGG jedoch weiter und umfasst auch die sogenannten 'äußeren Kommunikationsdaten', also Verkehrsdaten zu Kommunikationsvorgängen.

Dieses Verständnis des Schutzbereiches war in der Vergangenheit nicht unumstritten, ist jedoch unter Berücksichtigung des Schutzzwecks des Grundrechts die einzige im Ergebnis zufriedenstellende Interpretation: Verkehrsdaten erlauben regelmäßig Rückschlüsse auf den Inhalt von Nachrichten (z.B. hilfe@anonyme-alkoholiker.at als Adressat einer E-Mail, Anruf bei einem psychosozialen Beratungsdienst) und können — bis zu einem gewissen Grad, insbesondere vom Durchschnittsanwender — nicht 'vermieden' oder verschleiert werden.

Im Gegensatz dazu besteht beim 'klassischen' Brief immer die Möglichkeit, Nachrichten nach außen hin anonym zu übermitteln, indem z.B. auf dem Briefumschlag kein Absender angegeben wird. Aus diesem Grund war eine völlige Gleichstellung der Verkehrsdaten mit den 'äußeren Kommunikationsdaten' eines Briefes schon zum Zeitpunkt der Entstehung des Art 10a StGG nicht möglich: Das Fernmeldegeheimnis kann für Nachrichteninhalte nur dann effektiven Schutz bieten, wenn auch die äußeren Gesprächs- oder anderen Kommunikationsdaten in den Schutzbereich einbezogen werden.

Zudem unterscheidet sich die im Rahmen des Fernmeldegeheimnisses geschützte Kommunikation auch quantitativ vom klassischen Briefverkehr: Das Kommunikationsvolumen ist mit der Entwicklung neuer Technologien — insbesondere E-Mail und Mobiltelefonie — rasant gestiegen, wobei die Anzahl der dabei entstehenden Verkehrsdaten linear mit wächst.

Aus einer entsprechend großen Ansammlung von Verkehrsdaten können daher nicht nur einzelne Kommunikationsparameter abgeleitet werden, sondern gleichsam Profile der Betroffenen erstellt werden, aus denen wiederum auf Kommunikationsinhalte geschlossen werden kann: So weist zum Beispiel regelmäßiger Kontakt zu Fachärzten für Onkologie auf eine Krebserkrankung hin,

häufiger Kontakt zu bestimmten Uhrzeiten auf Freundschaften bzw. Arbeitskollegen usw.

Würden Verkehrsdaten aus dem Schutzbereich des Art 10a StGG ausgeklammert, so könnte durch die Ansammlung einer entsprechend großen Menge solcher Daten der Schutzzweck des Fernmeldegeheimnisses faktisch ausgehöhlt werden.

Die angeführten Daten können ein umfassendes Persönlichkeitsbild eines Menschen liefern und geben sogar oft mehr Information preis als bloße Inhaltsdaten. Wenn die Ermittlung dieser Daten, insbesondere gemeinsam mit der Erfassung von Standortdaten (Z 5), die ein Bewegungsprofil nachzeichnen, über einen Zeitraum von einigen Monaten erfolgt, kommt es zu einer kompletten Durchleuchtung eines Menschen. Schon in seinem Erkenntnis zur Vorratsdatenspeicherung hat der hohe Verfassungsgerichtshof ausgesprochen[…], dass es angesichts der 'Streubreite' des Eingriffs, des Kreises und der Art der betroffenen Daten und der daraus folgenden Schwere des Eingriffs in das Recht auf informationelle Selbstbestimmung (Zugriff auf Daten, die im Fall ihrer Verknüpfung nicht nur die Erstellung von Bewegungsprofilen ermöglichen, sondern auch Rückschluss auf private Vorlieben und den Bekanntenkreis einer Person zulassen), erforderlich ist, 'dass der Gesetzgeber durch geeignete Regelungen sicherstellt, dass diese Daten nur bei Vorliegen eines vergleichbar gewichtigen Interesses im Einzelfall für Strafverfolgungsbehörden zugänglich gemacht werden und dies einer richterlichen Kontrolle unterliegt'.

Wie schon in der Kritik zu Z 5 vorgebracht besteht auch hier das Problem, dass die Ermittlungsmaßnahmen nach § 14 PStSG für 6 Monate in die Zukunft genehmigt werden kann und diese Genehmigung auch immer wieder verlängert werden darf. Damit wird praktisch eine Art 'Quick-Freeze'-Vorratsdatenspeicherung normiert — aber ohne richterliche Kontrolle.

Nicht außer Acht gelassen werden darf auch die Frage der organisatorischen und technischen Abwicklung von Auskünften über Kommunikationsdaten gemäß § 11 Abs.1 Z 7 PStSG. Konkret geht es um die Anwendbarkeit der 'Datensicherheitsverordnung' zum TKG (DSVO) und die Anbindung an die sog. 'Durchlaufstelle', die nach §§ 8 ff DSVO den exklusiven Weg[…] für solche Datenauskünfte darstellt. Dadurch soll einerseits die Datensicherheit gewährleistet werden, außerdem enthält die Durchlaufstelle auch eine Funktion zur automatisierten Erfassung der statistischen Daten über sämtliche Auskunftsfälle. Die letztgenannte Funktion hat eine wichtige grundrechtspolitische Bedeutung, weil damit die Grundlage für spätere Evaluierungen geschaffen wird.

Aber auch für den Rechtsschutz ist die Bedeutung gerade dort wichtig, wo die Polizei alleine der Kontrolle durch den Rechtsschutzbeauftragten unterliegt — weil auf diese Weise der RSB die Zahl der ihm gemeldeten Fälle mit dem objektiven Wert zur Zahl der Auskunftsfälle aus der DLS-Statistik vergleichen kann.

Die in § 11 Abs. 1 Z 7 PStSG normierte Befugnis ist aus den dargelegten Gründen verfassungswidrig. Sie lässt einen Eingriff in das Fernmeldegeheimnis des Art 10a

StGG ohne Richtervorbehalt zu. Die Auskunft über Verkehrsdaten für den Präventionsbereich der erweiterten Gefahrenerforschung steht in unangemessener Weise für jede Aufgabenerfüllung nach § 6 Abs. 1 Z 1 und 2 zur Verfügung. Das mangelhafte Kontroll- und Rechtsschutzsystem ist gleichzeitig zu schwach, um einem extensiven Gebrauch dieser Befugnis entgegen zu wirken. Damit verletzt die Bestimmung auch § 1 DSG 2000 sowie Art 8 EMRK für sich und in Verbindung mit Art 13 EMRK. Die Regelung ist schließlich insbesondere im Vergleich mit der StPO sachlich nicht gerechtfertigt und verletzt daher Art 7 B-VG.

7.7 § 12 Abs. 1 (Datenanwendung, Informationsverbundsystem)

Durch § 12 iVm §§ 10 und 11 wird eine äußerst mächtige Datenbank geschaffen, deren Eingriffsintensität sehr hoch ist, während ihre Kontrolle und der diesbezügliche Rechtsschutz unzureichend ausgestaltet sind. Die Aufzählung der Kategorien der Betroffenen und der Daten in § 12 Abs. 1 ist sehr umfassend und greift tief in die Persönlichkeitssphäre der Betroffenen ein. Aufgrund der Formulierung 'tat- und fallbezogene Informationen und Verwaltungsdaten verarbeiten, die gemäß §§ 10 oder 11 oder auf Grundlage des SPG oder der StPO ermittelt wurden' wird die — zunächst sehr detaillierte — Festlegung der zu verarbeitenden Daten auch unbestimmt und unüberblickbar weit.

Die (nachfolgend konkret ausgeführten) Mängel im Rechtsschutzsystem bewirken letztlich die Unverhältnismäßigkeit der Datenanwendung.

Gemäß § 12 Abs.4 ist es zulässig, die Daten 'an ausländische Sicherheitsbehörden und Sicherheitsorganisationen (§ 2 Abs. 2 und 3 PolKG) sowie Organe der Europäischen Union oder Vereinten Nationen' zu übermitteln. Nähere Kriterien für diese Übermittlungsbefugnis ergeben sich weder aus dem PStSG noch aus anderen Bestimmungen wie etwa dem (einschlägigen) Polizeikooperationsgesetz.

Für den Betroffenen ist nicht erkennbar, nach welchen Kriterien Daten über ihn potenziell in das Ausland übermittelt werden. Die Regelung des § 12 Abs.4 ist daher unbestimmt und sowohl an sich, als auch im Hinblick auf den Umfang der gemäß § 12 Abs.1 zu verarbeitenden — uns somit potenziell zu übermittelnden — Daten äußerst weitgehend. Darüber hinaus besteht hinsichtlich dieser Befugnis zur Übermittlung von Daten in das Ausland kein spezifischer Rechtsschutz. Der Rechtsschutzbeauftragte ist in die Übermittlung nicht eingebunden. Ob der RSB nach § 15 Abs. 1 überhaupt Einsicht in die gemäß § 12 Abs. 5 protokollierten Übermittlungen nehmen darf, ist auch im Zusammenhang mit der Exklusion des Aufgabenbereichs nach § 6 Abs. 1 Z 3 PStSG (siehe sogleich) völlig unklar. Aufgrund der Einschränkung der Akteneinsicht im Einzelfall ist jedenfalls nicht gewährleistet, dass der RSB hier seine Kontrolltätigkeit wirksam entfalten kann.

Auch die einschlägigen Normen zur Rechtshilfe, etwa das Polizeikooperationsgesetz, das EU-Polizeikooperationsgesetz oder bilaterale Abkommen, enthalten keine Bestimmungen zum Rechtsschutz. In Zukunft sollen aber sogar die Daten der Analysedatenbank, in der zB bloße Kontaktpersonen und andere zur Beurtei-

lung der Wahrscheinlichkeit verfassungsgefährdender Angriffe gespeichert werden, an ausländische Behörden weitergegeben werden dürfen. Die Weitergabe von Daten in diesem frühen Stadium führt dazu, dass Fußballfans, Demonstranten, Internetforenuser usw. ohne ihr Wissen an ausländische Geheimdienste gemeldet werden, und aufgrund dieser Meldungen dann zB kein Visum erhalten oder Ziel der Angriffe von NSA, CIA, BND und GCHQ werden können.

Nach einer Übermittlung personenbezogener Daten ins Ausland wären Betroffene im Hinblick auf die weitere Verarbeitung im Ausland darauf angewiesen, dass Ihnen die Rechtsordnung des 'Empfängerstaates' der Daten einen Rechtsschutz gewährt. Für den praktisch wichtigsten Partnerstaat in diesem Zusammenhang, nämlich die USA, hat bereits der EuGH in der 'Safe Harbor' Entscheidung[…] festgestellt, 'dass es für die Betroffenen keine administrativen oder gerichtlichen Rechtsbehelfe gab, die es ihnen erlaubten, Zugang zu den sie betreffenden Daten zu erhalten und gegebenenfalls deren Berichtigung oder Löschung zu erwirken'.

Gar kein Rechtsschutz besteht nach dem eindeutigen Wortlaut des § 14 Abs.1 sowie Abs.2 erster Satz PStSG auch im Hinblick auf alle Daten, die im Rahmen der Aufgabe nach § 6 Abs.1 Z 3 PStSG (verfassungsgefährdender Angriff im Ausland) ermittelt werden, weil dort ausdrücklich nur die Aufgaben nach § 6 Abs.1 Z 1 und 2 PStSG genannt sind. Ein Grund für diese Lücke ist weder aus dem Gesetz noch den Materialien erkennbar.

Gemäß § 12 Abs. 6 obliegt die Kontrolle der Datenanwendung nach Abs. 1 dem Rechtsschutzbeauftragten nach Maßgabe des § 91c Abs. 2 SPG sowie § 15 Abs. 1. § 91c Abs. 2 SPG normiert eine einmalige Befassung des Rechtsschutzbeauftragten und § 15 Abs. 1 sieht eine Pflicht vor, dem Rechtsschutzbeauftragten bei der Wahrnehmung seiner Aufgaben jederzeit Einblick in die Datenanwendung zu gewähren.

§ 15 Abs. 1 bezieht sich somit auf die Inhalte der Datenanwendung, also die gespeicherten Daten, nicht aber die Datenanwendung selbst und deren Architektur. Die Kontrolle der Datenanwendung nach § 12 Abs. 1 weist somit ein zweifaches Defizit auf: Der Rechtsschutzbeauftragte ist im Hinblick auf die in § 91c Abs. 2 SPG normierte Frist von nur drei Tagen sowie auf seine personelle Ausstattung nicht in der Lage, die Datenanwendung selbst und deren Architektur initial effektiv zu kontrollieren und danach ist eine laufende Kontrolle der Datenanwendung selbst und deren Architektur überhaupt nicht mehr vorgesehen.

Dass sich der Kontrollauftrag des Rechtsschutzbeauftragten in § 12 Abs. 6 nur auf die Datenanwendung nach Absatz 1 bezieht ist missverständlich und führt möglicherweise ebenfalls zu bedenklichen Rechtsschutzlücken. Das Problem besteht hier vor allem darin, dass § 12 Abs. 2 die Anmerkung der Richtigstellung sowie der Einstellung oder Verfahrensbeendigung vorschreibt und dabei offen lässt, ob diese Anmerkungen unmittelbarer Bestandteil der Datenbank nach Absatz 1 ist. Weil zugleich § 12 Abs. 1 keinen Hinweis enthält, dass auch die Anmerkungen nach Absatz 2 unmittelbarer Bestandteil der Datenanwendung nach Absatz 1 sind, ist normativ in Frage zu stellen, ob sich die Kontrollaufgabe

des RSB nach § 12 Abs. 6 auch auf solche Anmerkungen bezieht. Damit besteht eine weitere Unklarheit, durch welche die Anfälligkeit des PStSG für Missbrauch verstärkt wird.

Hinzu kommt, dass die in § 12 Abs. 6 normierte Kontrolle auch komplexe Auswertungen der Datenanwendung nicht erfasst, seien es komplexe Datenbankabfragen, die durch Kombination der Daten ad-hoc ganz neue Informationen zutage fördern können, oder Auswertungen durch externe, nicht zur Datenanwendung gehörende Software, die über eine Schnittstelle auf die Datenanwendung zugreift. In beiden Fällen können ad-hoc neue, eingriffsintensive Informationen entstehen, die nicht gespeichert werden und deren Abfrage auch nicht gemäß § 12 Abs. 5 protokolliert wird, da nach dieser Bestimmung nur einzelne Abfragen protokolliert werden. Es werden sohin im Fall einer komplexen Abfrage nur die Abfragen der einzelnen Daten protokolliert, deren Kombination für die komplexe Abfrage erforderlich ist. Wie diese Daten kombiniert werden, und was das Ergebnis davon war, wird somit jedoch nicht protokolliert.

Es besteht daher eine deutliche Lücke in der Kontrolle der Datenanwendung durch den Rechtsschutzbeauftragten, da dieser weder komplexe oder externe Abfragen noch die Architektur und Funktionsweise der Datenanwendung kontrollieren kann. Beides wäre jedoch unbedingt erforderlich, um die tatsächlichen Instrumente und Vorgehensweisen der 'Staatsschutzorgane' sowie die tatsächliche Nutzung der Daten verstehen und effektiv kontrollieren zu können. Wie dargestellt wurde, reicht dazu die normierte Kontrollmöglichkeit der gespeicherten Daten an sich nicht aus.

Insbesondere ist aufgrund der dargelegten Mängel der Kontrolle und der mangelnden Determinierung der für die Durchführung des PStSG zu schaffenden Datenanwendungen auch nicht sichergestellt, dass die durch das PStSG geschaffenen Befugnisse zur Datenverarbeitung nicht faktisch wie das Instrument der 'Rasterfahndung' (automationsunterstützter Datenabgleich im Sinne des § 141 Strafprozessordnung) eingesetzt werden. Diese Befugnisse sind so weitgehend, dass dies möglich erscheint, wenngleich dies nach dem Wortlaut des § 10 Abs. 2 nicht zulässig sein soll. Die Grenze ist jedoch fließend, unter anderem weil nicht exakt definiert ist, was unter einem 'Datenabgleich' zu verstehen ist.

Gemäß §10 PStSG sind die Organisationseinheiten gemäß § 1 Abs. 3 ausdrücklich berechtigt, 'Daten, die sie in Vollziehung von Bundes- oder Landesgesetzen rechtmäßig verarbeitet haben' (Abs. 2), Daten 'von den Dienststellen der Gebietskörperschaften, den anderen Körperschaften des öffentlichen Rechts und den von diesen betriebenen Anstalten' (Abs. 3) und nach Maßgabe des Abs. 4 Bilddaten von Rechtsträgern des öffentlichen oder privaten Bereichs zu verwenden sowie 'personenbezogene Daten aus allen anderen verfügbaren Quellen durch Einsatz geeigneter Mittel insbesondere durch Zugriff etwa auf im Internet öffentlich zugängliche Daten, zu ermitteln und weiterzuverarbeiten'.

Nach Auffassung der Antragsteller/innen ist auch eine systematische Sammlung von Daten, welche die Behörde aus allen im Internet (und sonst) verfügbaren

Quellen anlegt, eine Datenanwendung im Sinne des § 141 Abs. 1 StPO. Es handelt sich dann zumindest um interne Datenanwendungen der Sicherheitsbehörden iSd § 141 Abs.2 StPO. Nach dem Regime des § 10 PStSG können somit Daten aus verschiedenen Datenanwendungen abgefragt und miteinander in Beziehung gesetzt werden. Eine Beschränkung auf Daten zu bereits namentlich bekannten Personen, die eine Abfrage der einzelnen in § 10 PStSG genannten Daten nach Merkmalen (§ 141 Abs. 1 StPO) ausschließen würde, ist dabei nicht vorgesehen. Da, wie oben erläutert, nur die einzelnen Abfragen, nicht aber die Ad-hoc-Kombination der verschiedenen Daten protokolliert werden und der Kontrolle unterliegen, kann nicht überprüft werden, ob die in § 10 PStSG geschaffenen Möglichkeiten zur Datenverwendung so eingesetzt werden, dass dies einem Datenabgleich iSd § 141 Abs. 2 StPO oder sogar iSd § 141 Abs. 3 StPO gleichkommt.

Anzumerken ist, dass die Einführung der 'Rasterfahndung' in den 1990er Jahren massive Kritik seitens der Zivilgesellschaft hervorbrachte. Die heute verfügbaren Datenmengen und die heutigen Mittel — z.B. bereits eine einfache Google-Suche — übersteigen jedoch das damals Vorstellbare bei Weitem.

Es handelt sich daher bei der Befugnis, personenbezogene Daten aus allen anderen verfügbaren Quellen durch Einsatz geeigneter Mittel insbesondere durch Zugriff etwa auf im Internet öffentlich zugängliche Daten, zu ermitteln und weiterzuverarbeiten' (§ 10 Abs. 5 PStSG) um eine sehr weitgehende Befugnis. Wenngleich das Grundrecht des § 1 Abs. 1 DSG auf allgemein verfügbare Daten nicht anzuwenden ist, fallen auch öffentlich verfügbare Informationen unter den Begriff der Privatsphäre iSd Art 8 EMRK wenn sie von Behörden systematisch gesammelt und gespeichert werden.[…]

Somit ist auch das Ermitteln und Verarbeiten von im Internet öffentlich zugänglichen personenbezogenen Daten ein Eingriff in das Grundrecht des Art 8 Abs. 1 EMRK. Zu betonen ist daher, dass solch ein Eingriff in jedem Fall gemäß Art 8 Abs. 2 EMRK ausreichend gesetzlich determiniert sein muss.

Die im Internet öffentlich zugänglichen Daten können nicht nur von einem Menschen ermittelt werden, sondern auch — ressourcenschonend, systematisch sowie ungleich rascher und umfassender — von einer darauf spezialisierten Software. § 10 Abs. 5 PStSG nennt dazu nur den 'Einsatz geeigneter Mittel' ohne weitere Präzisierung oder Schranken.

Die technische Entwicklung der letzten Jahre hat eine große Zahl sogenannter 'Open Source Intelligence'- (kurz OSINT) Instrumente hervorgebracht. Dabei handelt es sich um speziell für Ermittlungen im Sicherheitsbereich angefertigte Software, im Wesentlichen spezialisierte Suchmaschinen, die automatisiert nach bestimmten Filtern, die vom Anwender konkretisiert werden, alle im Internet verfügbaren Quellen analysieren. Auf diese Weise wird die Ermittlungsarbeit, die sonst durch menschliche Intelligenz gesteuert wird, durch komplexe Algorithmen an die Maschine ausgelagert. So kann die Maschine selbständig eine beachtliche Datensammlung erzeugen, die in einem weiteren Schritt von menschlichen

Ermittlern genutzt wird. Diese ursprünglich vor allem für Geheimdienste entwickelten Instrumente drängen international zunehmend in den Bereich der polizeilichen Gefahrenabwehr. Es besteht bereits ein großer und ständig wachsender Markt an Anbietern und Produkten für OSINT Tools, darunter befinden sich auch österreichische Unternehmen. […]

Ob eine solche Software durch das BVT genutzt wird, ist durch das Gesetz nicht determiniert, die §§ 10 ff PStSG stehen dem jedoch nicht entgegen.

Aus all den genannten Gründen wäre es erforderlich, die Datenanwendungen deutlich umfassender zu determinieren, als dies im PStSG der Fall ist. Eine solche nähere Determinierung könnte zum Teil im Gesetz erfolgen und mittels einer Durchführungsverordnung zu den §§ 10 ff weiter detailliert werden, wie dies zB auch im Rahmen der Einführung der Vorratsdatenspeicherung mit der 'Datensicherheitsverordnung TKG-DSVO' (BGBl. II Nr. 402/2011) erfolgt ist. In einer solchen Verordnung zu den §§ 10 ff PStSG sollten technische Spezifikationen der durch die §§ 10 ff PStSG geschaffenen Datenanwendungen festgelegt werden sowie Kontrollmaßnahmen, wie insbesondere die Auditierung der Datenanwendungen zum Zweck der Prüfung, ob diese den festgelegten Spezifikationen entsprechen.

Zusammenfassung:

Eine gesonderte Anfechtung des § 12 erfolgt im Rahmen der Eventualbegehren, wobei § 12 aufgrund der zahlreichen strukturellen Mängel zunächst zur Gänze angefochten wird. Eventualiter zu diesem Antragsbegehren werden getrennt § 12 Abs. 1 Z 1 und 4 angefochten, weil die Datensammlung zu 'Gruppierungen' nach Z 1 schon aufgrund der Unbestimmtheit des Begriffs unverhältnismäßig ist, während die Datensammlung zu Kontakt- und Begleitpersonen nach Z 4 durch die Akzessorietät im Prinzip durch das selbe Problem Gefahr läuft, uferlos zu werden. Die gesonderte Anfechtung der Ermächtigung zur Verarbeitung sensibler Daten nach Abs.1 letzter Satz wurde bereits oben begründet.

Die hier ausgeführten Gründe, weshalb die Datenanwendung nach § 12 PStSG als Informationsverbundsystem in der normierten Form unverhältnismäßig ist, gilt sinngemäß auch für die gesonderte Anfechtung des novellierten § 53a Abs. 5a SPG. Es handelt sich gleichsam um die korrespondierende Bestimmung im SPG zur Datenanwendung nach dem PStSG und wird mit derselben Begründung bekämpft.

7.7.1. Datenverarbeitung und Löschungsfristen

[…]

Geregelt werden in § 13 Abs. 1 PStSG besondere Löschungsverpflichtungen, wobei die Löschung unter bestimmten Voraussetzungen unterbleiben kann. § 13 Abs. 1 letzter Satz normiert, dass nach Ablauf von sechs Jahren 'die Daten' jedenfalls zu löschen sind. Auch wenn der Wortlaut nicht ganz eindeutig ist,

ergibt sich aus einer systematischen Interpretation, dass sich diese Höchstfrist nur auf die Speicherung personenbezogener Daten bezieht, die aufgrund einer Aufgabe gemäß § 6 Abs. 1 Z 1 oder 2 PStSG ermittelt wurden. Für Daten, die zur Erfüllung einer Aufgabe gemäß § 6 Abs. 1 Z 3 PStSG gespeichert wurden, gilt die Höchstfrist von sechs Jahren somit nicht. Ansonsten enthält das PStSG keine ausdrückliche Regelung für Daten, die aufgrund der Aufgabe gemäß § 6 Abs. 1 Z 3 gespeichert wurden.

Nach den Materialien[…] sind Verdächtige gemäß § 6 Abs. 1 Z 3 zwar nicht ausdrücklich in § 12 Abs. 1 (Analysedatenbank, die als Informationsverbundsystem betrieben werden darf) genannt, sie sind aber unter § 12 Abs. 1 Z 3 zu subsumieren. Demnach können diesbezügliche Daten also in der Analysedatenbank gespeichert werden. Der Gesetzestext (§ 12 .Abs. 1 Z 3) lässt jedoch verschiedene Interpretationen des Begriffes 'Verdächtige' in diesem Zusammenhang zu.

Durch die verschachtelte Verweisungstechnik des § 12 ist unklar, ob die zur Aufgabenerfüllung nach § 6 Abs. 1 Z 3 ermittelten Daten unter § 12 Abs. 1 Z 3 in der Analysedatenbank überhaupt verarbeitet werden dürfen. Dies ist nämlich nur 'zu Verdächtigen eines verfassungsgefährdenden Angriffs' erlaubt, während § 6 Abs. 1 Z 3 Personen erfasst, 'die im Verdacht stehen, im Ausland einen Sachverhalt verwirklicht zu haben, der einem verfassungsgefährdenden Angriff entspricht'.

Die Höchstfrist für gespeicherte Daten von fünf Jahren in § 12 Abs. 3 bezieht sich also unter anderem auf 'Verdächtige' gemäß § 12 Abs. 1 Z 3 und erfasst damit jedenfalls Personen, gegen die aufgrund der StPO wegen eines verfassungsgefährdenden Angriffs ermittelt wird oder werden könnte. Die Erläuterungen zur Regierungsvorlage führen zu § 6 Abs. 1 Z 3 aus:

'Die an diese Aufgabe anknüpfenden Datenverarbeitungsermächtigungen beschränken sich auf § 10; besondere Ermittlungsmaßnahmen nach § 11 kommen dafür nicht in Betracht, wenn nicht zusätzliche Umstände hinzutreten, die eine Aufgabe nach § 6 Abs. 1 Z 1 oder 2 begründen.'

Diese Höchstspeicherfrist gilt nach dem Wortlaut und der Systematik des Gesetzes eindeutig nur für Daten, die in der Analysedatenbank gemäß § 12 Abs. 1 gespeichert wurden, nicht aber für Daten, die gemäß § 10 Abs. 1 Z 3 zu Betroffenen zur Aufgabenerfüllung nach § 6 Abs. 1 Z 3 in anderen Datenanwendungen gespeichert wurden. Eine allgemeine Höchstdauer für die Speicherung von Daten, die aufgrund § 10 Abs. 1 Z 3 und 4 ermittelt wurden, ist im PStSG nicht normiert.

Gemäß § 12 Abs. 1 vorletzter Satz dürfen in der Analysedatenbank auch tat- und fallbezogene Informationen und Verwaltungsdaten verarbeitet werden, die gemäß §§ 10 oder 11 PStSG oder auf Grundlage des SPG oder der StPO ermittelt wurden. Wenn solche (personenbezogenen) Daten nun nicht mit einer Aufgabe gemäß § 6 Abs. 1 Z 1 oder 2 in Zusammenhang stehen, bezieht sich die besonde-

re Löschungsverpflichtung des § 13 nicht auf diese Daten. Diese Daten werden nämlich in den Fällen der Ermittlung auf Grundlage des SPG oder der StPO nicht nach dem PStSG ermittelt (arg §13 Abs. 1 erster Satz 'nach diesem Bundesgesetz ermittelte personenbezogene[n] Daten). Die Überführung solcher Daten in die Analysedatenbank stellt kein 'Verarbeiten' iSd § 4 Z 9 DSG 2000 (worunter ua das 'Ermitteln von Daten' fällt) dar, sondern ein 'Übermitteln' iSd Z 12 leg cit (Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers).

Selbst wenn aber ein Zusammenhang solcher Daten mit einer Aufgabe gemäß § 6 Abs. 1 Z 1 oder 2 PStSG besteht, sind solcherart übermittelte Daten strenggenommen auch dann nicht nach dem PStSG ermittelt — sondern höchstens übermittelt, womit die besondere Löschungsverpflichtung des § 13 nach dessen Wortlaut nicht greift. Eine Höchstfrist für die Speicherung dieser Daten ist im PStSG wiederum nicht normiert.

Ebenso wenig findet sich im PStSG eine Höchstspeicherfrist für personenbezogene Daten von Vertrauenspersonen, die gemäß § 12 Abs. 7 in der Analysedatenbank verarbeitet wurden. Bemerkenswert ist, dass in diesem Fall keinerlei Einschränkungen zu speichernder Daten (wie in § 12 Abs. 1) vorgesehen sind. Die Höchstfrist des § 54b Abs. 3 SPG bezieht sich nur auf die Vertrauenspersonenevidenz nach dem SPG.

Zusammenfassung (Datenverarbeitung und Löschungsfristen):

Die Löschungsverpflichtungen und Fristen sind im PStSG unzureichend geregelt. Es gibt einige Ausnahmen, die geeignet sind, bestimmte Daten im rechtlichen Zusammenhang so einzuordnen, dass die Löschungsfristen relativ einfach umgangen werden können oder tatsächlich von vornherein nicht existieren. Die Regelungen sind außerdem mit einigen Verweisen, die teilweise auf Personenkategorien abstellen und teilweise an die Art der Aufgabe anknüpfen, sowie einer wenig konsequenten Systematik kaum verständlich.

Obwohl § 13, die einschlägige Bestimmung mit der Überschrift 'besondere Löschungsfristen' ist, finden sich in § 12 Abs. 3 nach einem Verweis auf § 13 ebenfalls besondere Löschungsfristen, die wiederum von § 13 Abs. 1 abweichen und zugleich Fragen nach der Reichweite des § 13 aufwerfen.

Insgesamt entsprechen die Bestimmungen zu den Löschungsfristen weder dem grundrechtlichen Determinierungsgebot noch dem Verhältnismäßigkeitsgrundsatz. Nach letzterem besteht eine Löschungsverpflichtung nicht mehr benötigter Daten auch dann, wenn die Höchstdauer noch nicht erreicht ist. Dazu müsste aber entweder eine Möglichkeit Betroffener bestehen, die Löschung selbst zu beantragen oder ein Mechanismus eingerichtet sein, der es erlaubt, die Speicherung von Daten in regelmäßigen Abständen auf ihre Verhältnismäßigkeit hin zu überprüfen. lm PStSG ist beides nicht normiert.

### 7.8 § 54 Abs. 3 SPG - Vertrauenspersonen

Das Bundesgesetz vom 26.02.2016, BGBl. I Nr. 5/2016, mit dem das Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz — PStSG) erlassen und das Sicherheitspolizeigesetz geändert werden, enthält in Artikel 2 folgende Novellierungsanordnung für das SPG:

[…]

Da die ursprünglich im Ministerialentwurf ausdrücklich im PStSG vorgeschlagene Vertrauenspersonenevidenz (ehemaliger § 13) gestrichen wurde, findet sich im PStSG ein Hinweis auf Vertrauenspersonen nur noch im Zusammenhang mit Begründungspflichten zu deren Einsatz gegenüber dem Rechtsschutzbeauftragten. Die ausdrücklichen Regelungen finden sich nach der Regierungsvorlage nunmehr in § 54 Abs. 3 und Abs. 3a SPG — die auch für die Staatsschutzorgane maßgeblich sind. Abs. 3 reguliert ausdrücklich die Zulässigkeit von verdeckten Ermittlungen durch Vertrauenspersonen im Auftrag der Sicherheitsbehörden. Der schon im Begutachtungsentwurf komplett neu vorgeschlagene § 54 Abs. 3a SPG war ursprünglich auf die Dokumentation und Kontrolle beim Einsatz von verdeckten Ermittlern gerichtet.

Die Bestimmungen zur Vertrauenspersonenevidenz sind auch für den Aufgabenbereich des Staatsschutzes im (bestehenden) § 54b SPG zu finden. Dort ist schon bisher ausdrücklich normiert, dass solche Vertrauenspersonen den Sicherheitsbehörden Informationen gegen Zusage einer Belohnung preisgeben. Neu hinzugekommen ist nun mit der Novellierung des § 54 Abs. 3 und 3a SPG, dass bezahlte Vertrauenspersonen ausdrücklich mit verdeckten Ermittlungen beauftragt werden dürfen.

Die Legalisierung staatlicher bezahlter 'V-Leute' für Ermittlung oder Prävention von Straftaten birgt zunächst ein systematisches Problem: Bezahlte Spitzel kommen zumeist aus dem Kreise des kriminellen Umfelds, gegen das ermittelt wird. Woher weiß man nun, ob der 'Spitzel' tatsächlich 'die Seiten gewechselt' hat — er könnte auch bewusst mit der Polizei bzw. dem BVT kooperieren, einige kriminelle Konkurrenten tatsächlich 'ausliefern' und ansonsten systematisch falsche Informationen zum Vorteil der Organisation streuen oder Informationen aus dem Kreise der Ermittler weitergeben. In diesem Zusammenhang ist daher die detaillierte Begründung wesentlich, weshalb die Ermittler eine konkrete Person in einem konkreten Zusammenhang für zuverlässig halten. Allerdings mangelt es hierzu schon an formalen Begründungspflichten im Rahmen effektiver begleitender Sicherungsmechanismen zur Wahrung des Rechtsschutzes. Hierzu wäre nicht nur eine richterliche Kontrolle erforderlich, notwendig wäre überdies ein detailliertet Katalog von Zulässigkeitsvoraussetzungen und Begründungspflichten. Solche 'Safeguards' sind nicht einmal im Ansatz verwirklicht.

Ein konkretes Problem besteht darüber hinaus im potentiellen Spannungsverhältnis zum 'Recht auf ein faires Verfahren' gemäß Art 6 EMRK. Um dies zu verstehen, muss man die Ermittlungen der 'Staatsschutzorgane' im Erfolgsfall bis zu Ende denken: Im besten Fall mündet die Amtshandlung in eine abgewehrte

Sicherheitsbedrohung und in ein Strafverfahren gegen konkrete Beschuldigte. Sobald V-Leute und verdeckte Ermittler ins Spiel kommen, sind in der Praxis bestimmte Probleme typisch, allen voran das Verbot der Tatprovokation, weiches in § 5 Abs. 3 StPO ausdrücklich verankert ist. Eine solche Tatprovokation und die Verwertung derartig erlangter Beweise im Strafprozess stellt grundsätzlich eine Verletzung des Rechts auf ein faires Verfahren dar.[…]

Ein System staatlich bezahlter Spitzel birgt hier zunächst auch das Problem der Zurechnung zum Staat: Wenn ein V-Mann bezahlt wird, muss sich der Staat dessen Handlungen (z.B. eine Tatprovokation) auch zurechnen lassen. Wenn nun der Beschuldigte in einem Strafverfahren substantiiert eine Tatprovokation behauptet, trifft den Staatsanwalt die Beweislast, diese Behauptung zu widerlegen. Das Gericht hat dann eingehend zu untersuchen, ob die polizeilichen Organe innerhalb der gesetzlichen Grenzen agiert haben:[…] In so einem Fall wird man den V-Mann regelmäßig als Zeugen benötigen. Allerdings gibt es keine Rechtsgrundlage, auf der ein Gericht das BM.I zwingen kann, die Identität eines V-Manns oder eines verdeckten Ermittlers offen zu legen.
Auch wird ein solcher 'Spitzel' häufig eine wichtige Rolle im Beweisverfahren in der Hauptverhandlung haben. Wenn hier — wie regelmäßig zu erwarten — ebenso die Identität nicht preisgegeben wird, kann der Zeuge nicht unmittelbar vom Gericht und vor allein nicht vom Angeklagten befragt werden. Mit Blick auf den Unmittelbarkeitsgrundsatz (§ 13 StPO) und das in Art 6 Abs. 3 lit d EMRK verbriefte Recht, Fragen an die Belastungszeugen zu stellen oder stellen zu lassen, qualifiziert der OGH zB die Vernehmung einer Verhörsperson über die ihr gegenüber getätigten Angaben eines namentlich nicht bekannt gegebenen verdeckten Ermittlers als (Nichtigkeit begründende) Umgehung des Verlesungsverbotes (§ 252 Abs. 1 StPO). Eine auf die Amtsverschwiegenheit zum Schutz eines (anonymen) Zeugen gestützte Verlesung iSd § 252 Abs. 1 Z 1 StPO ist nur in sehr engen Grenzen denkbar zulässig, etwa bei besonders schwer wiegenden Straftaten, wenn die in Rede stehende Zeugenaussage unverzichtbar ist und die Gefährdungslage durch andere geeignete Maßnahmen (§§ 162, 229, 250 Abs. 1 StPO) nicht beseitigt werden kann.[…]

Aus diesen Gründen sollte schon beim Einsatz von verdeckten Ermittlern und V-Leuten bedacht werden, inwieweit diese Methoden lediglich einen Zwischenschritt zur Gewinnung anderer Beweismittel (Hausdurchsuchung, Überwachung der Telekommunikation etc.) darstellen sollen, widrigenfalls deren (ausschließliche) Verwertung im Wege anonymer Zeugenaussagen im Hauptverfahren iSd dargestellten Judikatur Probleme bereiten kann. Sind weitere Erkenntnisquellen nicht in Sicht, sollte dies im Einzelfall — zumal bei nicht eindeutig gewahrter Verhältnismäßigkeit — im Zweifel unzulässig sein. Der Gesetzeswortlaut und die Erläuterungen zeigen nicht einmal ansatzweise, dass die beschriebenen Herausforderungen bedacht und reflektiert wurden.

Die hier bekämpfte Bestimmung verletzt das Rechtsstaatliche Prinzip und perpetuiert schwere Probleme im Hinblick auf eine spätere Wahrung eines fairen Verfahrens nach Art 6 EMRK. Der Einsatz bezahlter Vertrauenspersonen als verdeckte Ermittler schafft nicht nur ein gesellschaftsschädliches Spitzelwesen,

er bewirkt auch unverhältnismäßige Eingriffe in Art 8 EMRK für sich und in Verbindung mit Art 13 EMRK. Die dargelegten Bedenken zeigen, dass die Regelung außerdem unsachlich ist, zumal sie die Strafverfolgung selbst unter den dargelegten Umständen behindern kann. Die Norm verletzt durch diese Unsachlichkeit auch Art 7 B-VG und ist aus den genannten Gründen verfassungswidrig.

7.9 § 4 (Das BVT als Zentralstelle)

[…]

In § 4 Z 1 und Z 5 normiert der Gesetzgeber einen Interessenkonflikt des BVT, der die Österreicherinnen und Österreicher in ihrer Grundrechtssphäre nachteilig berührt.

Gemäß § 4 Z 5 PStSG ist das BVT für die internationale Zusammenarbeit auf dem Gebiet des Staatschutzes zuständig. Dies umfasst die Zusammenarbeit mit Nachrichtendiensten anderer Staaten. Eine solche Zusammenarbeit bestand bereits bisher und spielt in der Praxis eine wichtige Rolle.[…] Das BVT ist — nicht zuletzt aufgrund seiner Größe sowie der Größe der Republik Österreich — auf die Zusammenarbeit mit den Nachrichtendiensten anderer Staaten angewiesen, um seinen Aufgaben nachkommen zu können.

Zu diesen Aufgaben des BVT zählt der Schutz der verfassungsmäßigen Einrichtungen, der Vertreter ausländischer Staaten, internationaler Organisationen und anderer Völkerrechtssubjekte, kritischer Infrastruktur und der Bevölkerung der Republik Österreich vor Gefährdungen durch Spionage sowie vor nachrichtendienstlicher Tätigkeit (§ 1 Abs. 2).

Das BVT arbeitet im Zuge seiner Tätigkeit zum Teil mit Nachrichtendiensten von Staaten zusammen, die zugleich Spionage gegen Organe der Republik Österreich, Organe der Europäischen Union und/oder Vertreter ausländischer Staaten und internationaler Organisationen in Österreich betreiben. Nachweislich ist dies zB beim US-Nachrichtendienst NSA der Fall.[…]

Zugleich obliegt den Organisationseinheiten nach § 1 Abs. 3 PStSG durch die Definition des 'verfassungsgefährdenden Angriffs' in § 6 Abs. 2 PStSG auch die Aufgabe der Spionageabwehr.

Zu den Instrumenten der Spionage und nachrichtendienstlichen Tätigkeit zählen Angriffe auf Computersysteme von verfassungsmäßigen Einrichtungen, zB um Inhalte von Kommunikation oder Datenträgern zu erlangen und auszuwerten. Gemäß § 4 Z 1 PStSG erfüllt das BVT die Funktion der operativen Koordinierungsstelle für Meldungen über jede Form von Angriffen auf Computersysteme von verfassungsmäßigen Einrichtungen sowie kritischen Infrastrukturen.

In dieser Rolle als operative Koordinierungsstelle besteht jedoch für das BVT die Gefahr, von einem ausländischen Nachrichtendienst – insbesondere einem mächtigen und gut informierten Dienst — unter Druck gesetzt zu werden, dessen

Angriffe auf Computersysteme zu tolerieren, und/oder diesbezügliche Meldungen nicht pflichtgemäß zu behandeln, widrigenfalls er seine — für die Erfüllung der Aufgaben des BVT wichtige — Zusammenarbeit einschränken oder einstellen würde. Sollte eine solche Drohung nicht tatsächlich ausgesprochen werden, bestünde nichtsdestotrotz für das BVT ein Anreiz, gegen Angriffe ausländischer Nachrichtendienste von Staaten, mit denen eine Zusammenarbeit besteht, nicht effektiv vorzugehen, um die Kooperation nicht zu gefährden. Somit bringt die Zuweisung der Funktion der operativen Koordinierungsstelle zum BVT durch § 4 Z 1 das BVT in einen Interessenkonflikt und schafft für einen ausländischen Dienst, mit dem Kooperation besteht, einen geradezu offensichtlichen Anreiz, das BVT wie beschrieben unter Druck zu setzen.

Die Regelung des § 4 Z 1 hat auf diese Weise das Potenzial, Angriffe auf Computersysteme von verfassungsmäßigen Einrichtungen sowie kritischen Infrastrukturen und damit einhergehende Eingriffe in verfassungsmäßig geschützte Rechtsgüter zu begünstigen. Ein drastisches Beispiel dafür, dass solche Angriffe durch 'befreundete' Nachrichtendienste in der Praxis tatsächlich vorkommen, ist der öffentlich bekannte Fall des Abhörens des Mobiltelefons der deutschen Bundeskanzlerin durch US-Nachrichtendienste. Doch gerade auch im Lichte der präventiven Funktion einer operativen Koordinierungsstelle für Meldungen über Angriffe auf Computersysteme zeigt sich der beschriebene Interessenkonflikt schon bisher und auf viel breiterer Ebene: Obwohl durch die Enthüllungen von Edward Snowden die massenhafte Überwachung der Internetaktivität evident wurde, scheint wenig dagegen unternommen zu werden, und es drängt sich der Verdacht auf, dass dies aus Rücksicht auf die Kooperation mit eben jenen Nachrichtendiensten nicht erfolgt, die die Überwachung durchführen.

Die Schaffung einer operativen Koordinierungsstelle für Meldungen über Angriffe auf Computersysteme ist Gegentand der vom EU-Rat am 17. Mai 2016 beschlossenen NIS-Richtlinie[…] zur Stärkung der Netzwerk- und Informationssicherheit, deren Inkrafttreten für August 2016 erwartet wird.

Zu dieser Frage läuft derzeit ein vom BM.I initiierter, breit angelegter zivilgesellschaftlicher Prozess, in dem diskutiert wird bzw. werden sollte, wo eine solche Stelle in Österreich angesiedelt sein sollte. Wenn diese Stelle außerhalb des BVT angesiedelt wäre —was aber nicht bedeuten muss, außerhalb der Zuständigkeit des BM.I – könnte der beschriebene Interessenkonflikt und damit das Potenzial ausländischer Nachrichtendienste, diesen wie beschrieben auszunützen, minimiert werden.

Nicht nur hinsichtlich der Funktion als Koordinierungsstelle für Meldungen über Angriffe auf Computersysteme von verfassungsmäßigen Einrichtungen sowie kritischen Infrastrukturen sondern ganz allgemein befindet sich das BVT in einem Interessenkonflikt, wenn es für die Kooperation mit ausländischen Nachrichtendiensten zuständig und auf diese angewiesen ist, zugleich aber für den Schutz vor Spionage und nachrichtendienstlicher Tätigkeit durch ausländische Nachrichtendienste zuständig ist. Will das BVT letzterer Aufgabe effektiv nachkommen, muss

es gegen solche Tätigkeiten eines ausländischen Nachrichtendienstes aktiv vorgehen, wenn ihm diese bekannt werden.

Auch hier könnte das BVT unter Druck kommen: Die Konsequenz eines Vorgehens gegen einen ausländischen Nachrichtendienst, mit dem das BVT kooperiert, könnte sein, dass dieser die Kooperation einstellt oder einschränkt und dass das BVT insbesondere Informationen über aktuelle, die Republik Österreich betreffende — z.B. terroristische — Bedrohungen von diesem Nachrichtendienst nicht mehr erhält.

Somit stünde das BVT vor der Wahl, entweder Eingriffe in verfassungsmäßig geschützte Rechtsgüter durch einen ausländischen Nachrichtendienst in Kauf zu nehmen oder gegen diese vorzugehen und damit das Risiko einzugehen, aktuellen Bedrohungen gegen verfassungsmäßig geschützte Rechtsgüter z.B. durch einen terroristischen Angriff weniger effektiv begegnen zu können, weil es von diesem ausländischen Nachrichtendienst möglicherweise nicht die volle Unterstützung erhält.

In der Festlegung der Zuständigkeiten des BVT im PStSG wird dieser Interessenkonflikt für das BVT angelegt sowie für einen ausländischen Dienst, mit dem Kooperation besteht, ein geradezu offensichtlicher Anreiz geschaffen, das BVT wie beschrieben unter Druck zu setzen. Somit wird systeminhärent eine Situation geschaffen, in der die oben beschriebenen Eingriffe — in der einen oder anderen Weise — nicht effektiv verhindert werden können. Der Interessenkonflikt und somit potenzielle Eingriffe könnten vermieden werden, wenn eine andere Stelle, auf deren Entscheidungen das BVT keinen Einfluss nehmen kann, für die Spionageabwehr zuständig wäre.

Dies entspricht der Organisation des Nachrichtendienstewesens beim österreichischen Bundesheer, das zwei voneinander unabhängige Nachrichtendienste besitzt:

Das Heeresnachrichtenamt (HNaA) ist für die strategische Auslandsaufklärung zuständig. Es kooperiert dabei mit ausländischen Nachrichtendiensten.

Das Abwehramt (AbwA) ist zuständig für die Abwehr von Gefahren für die militärische Sicherheit und somit auch Für die Spionageabwehr sowie die 'Elektronische Abwehr' und die IKT[…]-Sicherheit.

Die Situation, dass ein Nachrichtendienst gegen Aktivitäten eines ausländischen Nachrichtendienstes vorgehen muss, und zugleich mit diesem kooperiert und auf dessen Zusammenarbeit und Informationen angewiesen ist, und der sich daraus ergebende Interessenkonflikt können somit aufgrund dieser Trennung in zwei Nachrichtendienste nur in deutlich reduzierter Form eintreten. Hier soll nicht der Eindruck erweckt werden, dass eine perfekte Trennung möglich wäre und es einen Nachrichtendienst geben könne, der überhaupt nicht mit anderen Nachrichtendiensten kooperiert. Während aber der beschriebene Interessenkonflikt

im PStSG unmittelbar angelegt ist, kann dieser durch eine Regelung wie im MBG wesentlich entschärft werden."

2. Die Bundesregierung erstattete eine Äußerung, in der im Wesentlichen Folgendes ausgeführt wird (Zitat ohne im Original enthaltene Hervorhebungen): 6

"Zu den Prozessvoraussetzungen:

1. Zum Anfechtungsgegenstand:

1.1. […]
1.2. Die Antragsteller begehren mit dem (Haupt)Antrag 1 sowie den (Eventual)Anträgen 2, 3, 4 und 5 jeweils die Aufhebung des Artikels 1 und mit dem (Haupt)Antrag 1 sowie den (Eventual)Anträgen 2, 3, 4, 5 und 7 jeweils die Aufhebung bestimmter Teile des Artikels 2 des Bundesgesetzes, mit dem das Bundesgesetz über Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz – PStSG) erlassen und das Sicherheitspolizeigesetz geändert werden, BGBl. I Nr. 5/2016.

1.3. Beim Bundesgesetz BGBl. I Nr. 5/2016 handelt es sich um ein Sammelgesetz, das aus zwei Artikeln besteht: Artikel 1 enthält das – neu erlassene – PStSG, Artikel 2 enthält Änderungen des SPG.

Die Antragsteller fechten mit dem (Haupt)Antrag 1 sowie den (Eventual)Anträgen 2, 3, 4 und 5 jeweils nur den Artikel 1 – und damit eine Gliederungseinheit – des Bundesgesetzes BGBl. I Nr. 5/2016, nicht jedoch das PStSG selbst an. Außerdem fechten sie mit dem (Haupt)Antrag 1 sowie den (Eventual)Anträgen 2, 3, 4, 5 und 7 einzelne Novellierungsanordnungen in Artikel 2 des Bundesgesetzes BGBl. I Nr. 5/2016, nicht jedoch die als verfassungswidrig gerügten Bestimmungen des SPG an.

1.4. Nach der ständigen Rechtsprechung des Verfassungsgerichtshofes ist die Anfechtung einer Novellierungsanordnung nur dann zulässig, wenn eine Bestimmung durch die betreffende Novelle aufgehoben worden ist und sich das Bedenken gegen diese Aufhebung richtet, die Verfassungswidrigkeit also auf keinem anderen Wege beseitigt werden kann (vgl. VfGH 9.6.2016, G 56/2016; VfSlg. 19.658/2012 mwN zur Vorjudikatur).

Diese Voraussetzung ist im vorliegenden Fall allerdings nicht erfüllt:

1.4.1. Die im Hinblick auf Artikel 2 des Bundesgesetzes BGBl. I Nr. 5/2016 behaupteten Verfassungswidrigkeiten ergeben sich nämlich jeweils ausschließlich aus den mit den angefochtenen Artikeln geänderten Bestimmungen des SPG. Sie sind somit eine Folge des Umstandes, dass in das SPG neue Bestimmungen eingefügt bzw. geltende Bestimmungen geändert wurden. Es wäre daher grundsätzlich möglich, jeweils die neu eingefügten bzw. die geänderten Bestimmungen des SPG als verfassungswidrig anzufechten (vgl. VfGH 9.6.2016, G 56/2016).

1.4.2. Gleiches gilt nach Auffassung der Bundesregierung hinsichtlich der beantragten Aufhebung des Artikel 1, hätten doch die Antragsteller das PStSG selbst und nicht Artikel 1 des Sammelgesetzes BGBl. I Nr. 5/2016 anfechten können.

1.4.3. Der (Haupt)Antrag 1 sowie die (Eventual)Anträge 2 bis 5 und 6 [gemeint wohl: 7] sind sohin schon aus diesem Grund als unzulässig zurückzuweisen.

2. Zum Anfechtungsumfang:

[…]

2.1., 2.2. […]

2.3. Der (Eventual)Antrag 6, der sich u.a. gegen einzelne Bestimmungen des PStSG richtet, erweist sich […] nach Auffassung der Bundesregierung insbesondere aus folgenden Gründen als zu eng gefasst:

2.3.1. Durch die mit Punkt 6.2. – 6.4. des Antrags begehrte Aufhebung des § 6 Abs. 1 Z 1 bis 3 PStSG würde in § 6 Abs. 1 lediglich die Wortfolge 'Den Organisationseinheiten gemäß § 1 Abs. 3 obliegen' übrig bleiben. Insofern verbliebe ein unverständlicher Torso.

Zudem bliebe in § 6 Abs. 2 PStSG lediglich die Definition des 'verfassungsgefährdenden Angriffs' übrig, der sich auf die Aufgaben nach § 6 Abs. 1 Z 2 und 3 PStSG bezieht. Die Aufhebung des § 6 Abs. 1 Z 1 bis 3 PStSG würde die Bestimmung daher unvollziehbar machen.

2.3.2. Nach der Rechtsprechung des Verfassungsgerichtshofs ist auch ein Verweis auf aufgehobene Vorschriften zu eliminieren, wenn dieser Verweis die Norm sonst unvollziehbar machen würde (VfSlg. 16.678/2002).

Der nicht angefochtene § 10 Abs. 3 und 4 PStSG regelt besondere Ermittlungsbefugnisse, die jedoch auf die 'Aufgaben nach [§ 10] Abs. 1 Z 1 und 2' eingeschränkt sind. Die Aufhebung des angefochtenen § 10 Abs. 1 Z 1 und 2 würde also § 10 Abs. 3 und 4 PStSG unvollziehbar machen. Der (Eventual)Antrag 6 hätte daher auch den Antrag auf Aufhebung des § 10 Abs. 3 und 4 PStSG enthalten müssen.

Aus demselben Grund hätte der Antrag aus diesem Grund auch die Aufhebung von (Teilen der) folgenden Bestimmungen enthalten müssen:

- § 13 Abs. 1 wegen Verweises auf den angefochtenen § 6 Abs. 1 Z 1 und 2 PStSG;
- § 14 wegen Verweises auf die angefochtenen § 6 Abs. 1 Z 1 und 2, § 12 Abs. 6, § 11 Abs. 1 Z 2 und 7 PStSG;
- § 15 Abs. 1 und 3 wegen Verweises auf die angefochtenen § 12 Abs. 1 und § 6 Abs. 1 Z 1 und 2 PStSG;
- § 16 Abs. 1 und 2 wegen Verweises auf § 6 Abs. 1 Z 1 und 2 PStSG.

[…]

In der Sache:

[…]

5. Zu den Bedenken im Hinblick auf das rechtsstaatliche Prinzip:

5.1. Die Bedenken der Antragsteller hinsichtlich der mangelnden Determiniertheit richten sich in erster Linie gegen Teile des § 6 PStSG: Zentrale Begriffe wie 'Gruppierung' (§ 6 Abs. 1 Z 1), 'ideologisch motivierte Kriminalität' (§ 6 Abs. 2 Z 2), 'ideologisch motivierte Gewalt' (§ 6 Abs. 1 Z 1) oder 'begründeter Gefahrenverdacht' (§ 6 Abs. 1 Z 2) seien nicht hinreichend bestimmt (Antrag S. 21, 35 ff).

5.2. Das in Art. 18 Abs. 1 B-VG verankerte Rechtsstaatsprinzip gebietet, dass Gesetze einen Inhalt haben, durch den das Verhalten der Behörde vorherbestimmt ist. Es ist jedoch verfassungsgesetzlich zulässig, wenn der einfache Gesetzgeber bei der Beschreibung und Formulierung dieser Kriterien unbestimmte Gesetzesbegriffe verwendet, dadurch zwangsläufig Unschärfen in Kauf nimmt und von einer exakten Determinierung des Vollziehungshandelns Abstand nimmt, falls dies im Hinblick auf den Regelungsgegenstand erforderlich ist (vgl. VfSlg. 13.785/1994; VfGH 15.6.2016, G 25/2016 ua mwN). Der Verfassungsgerichtshof hält in ständiger Rechtsprechung fest, dass sich die Beurteilung, ob eine Norm diesem rechtsstaatlichen Bestimmtheitsgebot entspricht, nicht nur nach ihrem Wortlaut, sondern auch nach ihrer Entstehungsgeschichte, dem Inhalt und dem Zweck der Regelung richtet. Bei der Ermittlung des Inhalts einer gesetzlichen Regelung sind daher alle der Auslegung zur Verfügung stehenden Möglichkeiten auszuschöpfen. Eine Regelung verletzt die in Art. 18 B-VG enthaltenen rechtsstaatlichen Erfordernisse nur dann, wenn nach Heranziehung sämtlicher Interpretationsmethoden nicht beurteilt werden kann, wozu das Gesetz ermächtigt (vgl. VfSlg. 18.738/2009; 19.530/2011 jeweils mwN).

5.3. § 6 PStSG entspricht vor diesem Hintergrund dem Bestimmtheitsgebot des Art. 18 Abs. 1 B-VG:

Die Bundesregierung verweist zunächst auf die Ausführungen unter Punkt I. 3.2.1. und I 3.2.2., im Rahmen derer die wesentlichen Elemente der Aufgaben 'erweiterte Gefahrenerforschung' (vgl. dazu im Besonderen Punkt I. 3.2.1.1. und I 3.2.1.2.) und 'vorbeugender Schutz vor verfassungsgefährdenden Angriffen' (vgl. dazu im Besonderen Punkt I. 3.2.2.2.) ausführlich dargelegt wurden. Daraus ergibt sich etwa bereits, dass die Aufgabe der erweiterten Gefahrenerforschung gemäß § 6 Abs. 1 Z 1 PStSG lediglich zur Beobachtung einer Gruppierung als solcher und nicht auch zur Beobachtung von Einzelpersonen innerhalb dieser Gruppierung ermächtigt.

Darüber hinaus wird auf Folgendes hingewiesen:

5.3.1. Schon auf Grund einer Auslegung des Begriffes 'Gruppierung' nach dem allgemeinen Sprachgebrauch ergibt sich, dass es sich dabei um mehrere Personen handelt, die aufgrund bestimmter Gemeinsamkeiten zusammengehören, etwa weil sie sich zur Verfolgung bestimmter Ziele zusammengeschlossen haben oder eine bestimmte gemeinsame Linie vertreten. Eine Gruppierung zeichnet sich somit durch übereinstimmende Vorstellungen und in der Regel ein gemeinsames Wirken und Auftreten der dazu gehörenden Personen aus. Entgegen der Auffassung der Antragsteller (Antrag S 37) ergibt sich somit aus dem Wortlaut des § 6 Abs. 1 Z 1 PStSG eindeutig, dass das Verhalten eines einzelnen Mitgliedes nicht ausreicht, um auf das Vorliegen der Voraussetzungen für die Beobachtung einer Gruppe im Rahmen der erweiterten Gefahrenerforschung zu schließen.

Daneben wird die Aufgabe gemäß § 6 Abs. 1 Z 1 PStSG auch durch die Verknüpfung mit der Prognose, dass 'im Hinblick auf deren Struktur und auf zu gewärtigende Entwicklungen in deren Umfeld damit zu rechnen ist, dass es zu mit schwerer Gewalt für die öffentliche Sicherheit verbundener Kriminalität, insbesondere zu ideologisch oder religiös motivierter Gewalt kommt, näher bestimmt. Somit ist jeweils im Einzelfall zu beurteilen, ob die Struktur der Gruppierung und Entwicklungen in ihrem Umfeld Anlass zur Annahme geben, dass es zu mit schwerer Gewalt für die öffentliche Sicherheit verbundener Kriminalität kommt (vgl. dazu oben Punkt I 3.2.1.2 und 3.2.1.3). Vor diesem Hintergrund ist — sowohl im Hinblick auf den Wortlaut als auch im Hinblick auf den Zweck der erweiterten Gefahrenerforschung iSv. § 6 Abs. 1 Z 1 PStSG — eine pauschale Erfassung 'immer weiterer Kreise der Bevölkerung' ausgeschlossen.

5.3.2. Was die Bedenken der Antragsteller hinsichtlich der Verwendung des Begriffs 'ideologisch' betrifft, weist die Bundesregierung zunächst darauf hin, dass mit dem Begriff in § 6 Abs. 1 Z 1 PStSG lediglich beispielhaft ein — wenngleich wesentliches — Ziel der erweiterten Gefahrenerforschung verdeutlicht wird (vgl. dazu auch oben Punkt I. 3.2.1.1). Der Begriff der 'ideologisch motivierten Gewalt' steht insofern zudem in direktem Zusammenhang mit dem Tatbestandselement der 'mit schwerer Gefahr für die öffentliche Sicherheit verbundenen Kriminalität' (vgl. Salimi, JBl 2013, 700; Wimmer in Thanner/Vogl [Hrsg.] SPG$^{2}$ [2013] § 22 Anm. 24 ff).

Der Begriff der 'Ideologie' — bzw. der synonyme Begriff der 'Weltanschauung' — steht nach dem allgemeinen Sprachgebrauch für eine bestimmte Grundeinstellung, bestimmte Wertungen, Auffassungen, Denkweisen. Verknüpft mit dem Tatbestandselement der 'Kriminalität, die mit schwerer Gefahr für die öffentliche Sicherheit verbunden ist' (§ 6 Abs. 1 Z 1 PStSG) bzw. mit bestimmten strafbaren Handlungen (§ 6 Abs. 2 Z 2 PStSG), bringt der Ausdruck 'ideologisch motivierte Gewalt' bzw. 'ideologisch motiviert' nach Auffassung der Bundesregierung hinreichend deutlich zum Ausdruck, dass Verhaltensweisen bzw. Straftaten erfasst sind, deren Motiv darin besteht, die bestehende — demokratische und rechtsstaatliche — Ordnung zu gefährden.

Soweit die Antragsteller schließlich eine Verletzung des Determinierungsgebotes auch in der Schwierigkeit erblicken, anhand der 'inneren Motivation' des poten-

tiellen Täters festzustellen, ob eine Handlung ideologisch motiviert ist, verweist die Bundesregierung auf das oben unter Punkt I. 3.2.1.3 Ausgeführte: Die innere Motivation potentieller Gefährder lässt sich anhand objektiver Indikatoren — wie etwa einem bestimmten Auftreten, der Verwendung bestimmter Zeichen oder Symbole — die auf eine Ablehnung der bestehenden Ordnung hindeuten, feststellen und (unter Hinweis auf diese objektiven Indikatoren) begründen. Auch insofern liegt daher kein Verstoß gegen das Determinierungsgebot vor.

Darüber hinaus weist die Bundesregierung darauf hin, dass es dem Strafrecht keineswegs fremd ist, für die Begründung der Strafbarkeit eines Verhaltens — oder auch nur hinsichtlich der Strafhöhe — auf einen bestimmten Gesinnungsunwert abzustellen. Gemäß § 33 Abs. 1 Z 5 StGB ist es bei der Bemessung der Strafe als besonderer Erschwerungsgrund zu berücksichtigen, wenn der Täter aus 'rassistischen, fremdenfeindlichen oder anderen besonders verwerflichen Beweggründen [...] gehandelt hat'. Auch hier wird auf ein bestimmtes Tatmotiv und damit eine innere Einstellung abgestellt (vgl. Ebner in Höpfel/Ratz [Hrsg.] Wiener Kommentar zum StGB [115. Lfg. 2014] § 33 Rz. 17).

5.3.3. Was schließlich den Begriff des 'begründeten Gefahrenverdachts' nach § 6 Abs. 1 Z 2 PStSG betrifft, so ergibt sich dessen Inhalt bereits aus der Bedeutung des Wortes 'begründet' als 'einen Grund in etwas habend'. Daraus folgt, dass der Gefahrenverdacht durch Angabe von Gründen substantiiert sein muss. Die Erläuterungen sprechen insofern von 'hinreichenden Anhaltspunkten' (vgl. ErIRV 763 BlgNR 25. GP 4). Bloße Vermutungen reichen also nicht, vielmehr müssen konkrete Anhaltspunkte für einen verfassungsgefährdenden Angriff vorliegen. Für das Vorliegen eines begründeten Gefahrenverdachts bedarf es demnach eines Tatsachensubstrats, das eine bestimmte Straftat ernsthaft befürchten lässt. Der Angriff muss jedoch nicht bereits das Vorbereitungsstadium erreicht haben (vgl. dazu bereits ausführlich unter Punkt I. 3.2.2.2.). Dass den zur Wahrnehmung der Angelegenheiten des polizeilichen Staatsschutzes zuständigen Organisationseinheiten bzw. dem Rechtsschutzbeauftragten — der die Ermächtigung zur Durchführung einer an die Aufgabe geknüpften Maßnahme erteilt — in Bezug auf das Ausmaß der Begründetheit im dargelegten Sinne im Einzelfall ein gewisser Spielraum zukommt, macht die Regelung nicht unbestimmt (vgl. VfGH 15.6.2016, G 25/2016 ua).

5.4. Dem Vorbringen der Antragsteller, dass 'durch die Summe der schwerwiegenden Verletzungen des Rechtsstaatsprinzips durch die angefochtenen Normen des PStSG sowie des SPG[...] sich das Bundesgesetz [...] BGBl. I Nr. 5/2015 aber auch als Gesamtänderung der österreichischen Bundesverfassung im Sinne von Art. 44 Abs. 3 B-VG [erweist]', ist Folgendes entgegen zu halten:

Art. 44 Abs. 3 B-VG normiert besondere Erzeugungsbedingungen für Verfassungsgesetze oder in einfachen Gesetzen enthaltene Verfassungsbestimmungen iSd. Art. 44 Abs. 1 B-VG, mit denen eine bestimmte Wirkung verbunden ist (nämlich eine Gesamtänderung der Bundesverfassung). Eine verfassungswidrige (schleichende) Gesamtänderung kann daher nur dann vorliegen, wenn Verfassungsrecht unter Missachtung der Vorgaben des Art. 44 Abs. 3 B-VG zustande

gekommen ist. Das PStSG und das SPG bzw. die jeweils angefochtenen Bestimmungen dieser Gesetze (bzw. des Bundesgesetzes BGBl. I Nr. 5/2016) sind aber keine Verfassungsgesetze oder Verfassungsbestimmungen. Das diesbezügliche Vorbringen der Antragsteller geht daher von vornherein ins Leere.

6. Zu den Bedenken im Hinblick auf das Grundrecht auf Datenschutz (§ 1 DSG 2000) und des Rechts auf Achtung des Privat- und Familienlebens (Art. 8 EMRK) iVm. dem Recht auf eine wirksame Beschwerde (Art. 13 EMRK):

6.1. Gemäß § 1 Abs. 1 DSG 2000 hat jedermann, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

Beschränkungen des Geheimhaltungsanspruchs sind, soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, gemäß § 1 Abs. 2 DSG 2000 nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 EMRK genannten Gründen notwendig sind. Gesetzliche Beschränkungen müssen in einer Abwägung zwischen der Schwere des Eingriffs und dem Gewicht der mit ihnen verfolgten Ziele verhältnismäßig sein (vgl. VfSlg. 19.892/2014 mwN). Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Der Eingriff in das Grundrecht darf auch im Falle zulässiger Beschränkungen jeweils nur in der gelindesten zum Ziel führenden Art vorgenommen werden. Die Fälle zulässiger Eingriffe müssen durch das Gesetz entsprechend konkretisiert und begrenzt werden, so dass für jedermann vorhersehbar ist, unter welchen Voraussetzungen die Ermittlung bzw. die Verwendung personenbezogener Daten für die Wahrnehmung konkreter (Verwaltungs)Aufgaben erlaubt ist (vgl. VfSlg. 19.657/2012; 19.738/2013; 19.892/2014 jeweils mwN).

Neben dem Geheimhaltungsanspruch umfasst das Grundrecht auf Datenschutz das — durch die einfache Gesetzgebung auszugestaltende — Recht auf Auskunft, Richtigstellung und Löschung (§ 1 Abs. 3 DSG 2000).

6.2. Der EGMR hält zum Recht auf Achtung des Privat- und Familienlebens gemäß Art. 8 EMRK im Zusammenhang mit geheimen Maßnahmen in ständiger Rechtsprechung fest, dass die Voraussetzungen und Bedingungen, unter denen die Behörden Maßnahmen setzen dürfen, aus dem ermächtigenden Gesetz erkennbar sein müssen. Des Weiteren muss der Ermessensspielraum, der den Behörden bei der Ausübung entsprechender Maßnahmen eingeräumt ist, unter Berücksichtigung des jeweils verfolgten legitimen Zieles klar umschrieben sein. Schließlich

müssen ausreichende verfahrensmäßige Schutzvorkehrungen gegen einen Missbrauch der eingeräumten Ermächtigung bestehen (vgl. EGMR, Urteil vom 18.5.2010, Kennedy gegen Vereinigtes Königreich, Appl. 26839/05, Rz. 151 ff mwN). Mit anderen Worten: Dort, wo personenbezogene Daten im Interesse der nationalen Sicherheit und öffentlichen Ordnung ermittelt und verarbeitet werden, müssen angemessene und effektive Garantien gegen Missbrauch bestehen. Gemäß Art. 13 EMRK muss gegen Verletzungen der durch die EMRK geschützten Rechte eine 'wirksame Beschwerde' zur Verfügung stehen.

6.3. Nach Auffassung der Bundesregierung sind die Bedenken der Antragsteller betreffend § 1 DSG 2000 und Art. 8 (iVm. Art. 13) EMRK nicht stichhaltig:

Vorbemerkungen zur einfachgesetzlichen Rechtslage:

6.4.1. Einleitend wird darauf hingewiesen, dass die Antragsteller ihren verfassungsrechtlichen Bedenken an verschiedenen Stellen unzutreffende Annahmen von der einfachgesetzlichen Rechtslage zu Grunde legen, weshalb sich ihre entsprechenden verfassungsrechtlichen Bedenken insoweit von vornherein als unbegründet erweisen. Schlaglichtartig sollen dafür folgende Beispiele herausgegriffen werden:

6.4.2. Die Antragsteller gehen etwa in ihren Ausführungen zu § 11 Abs. 1 Z 3 PStSG davon aus, dass diese Bestimmung einen über die Ermächtigung der Parallelbestimmung des § 54 Abs. 4 SPG hinausgehenden Einsatz von Bild- und Tonaufzeichnungsgeräten erlaubt (Antrag S 54 f). Wie bereits oben unter Punkt 1.3.3.3.1. dargelegt, verkennen die Antragsteller dabei, dass durch den Klammerverweis auf § 54 Abs. 4 SPG eindeutig klargestellt ist, dass der Umfang der Ermächtigung des § 11 Abs. 1 Z 3 PStSG mit jenem des § 54 Abs. 4 SPG übereinstimmt. Dies ergibt sich auch eindeutig aus den Erläuterungen (vgl. ErIRV 763 BlgNR 25. GP 6).

6.4.3. Mit ihren Ausführungen zu § 12 Abs. 1 und 2 iVm § 12 Abs. 6 PStSG gehen die Antragsteller davon aus, dass die Kontrollbefugnisse des Rechtsschutzbeauftragten nicht auch etwaige Richtigstellungen von Daten erfassen würden, da unklar sei, ob solche Richtigstellungen Teil der Datenanwendung seien (Antrag S 62). § 12 Abs. 2 PStSG trifft seinem klaren Wortlaut und Sinn nach eine nähere Regelung zur Datenanwendung. Richtigstellungen sind daher Teil der Datenanwendung und unterliegen folglich auch der Kontrolle des Rechtsschutzbeauftragten. Gleiches gilt für die (Protokollierung von) Datenübermittlungen und [Daten]abfragen gemäß § 12 Abs. 4 PStSG.

6.4.4. Die Antragsteller behaupten weiters, dass § 9 Abs. 1 zweiter Satz PStSG 'den Eindruck erwecken könnte', dass bei nicht sensiblen Daten keine angemessenen Vorkehrungen zur Wahrung der Geheimhaltungsinteressen notwendig seien (Antrag S 46). Dabei übersehen sie Folgendes:

Zunächst verpflichtet bereits § 9 Abs. 1 erster Satz PStSG, beim Verwenden personenbezogener Daten die Verhältnismäßigkeit zu beachten; daher sind

schon auf Grund dieser Bestimmung bei jeder einzelnen Datenverwendung die den jeweiligen Daten entsprechenden Vorkehrungen zur Wahrung der Geheimhaltungsinteressen zu treffen. Darüber hinaus sind die zur Wahrnehmung des polizeilichen Staatsschutzes zuständigen Organisationseinheiten gemäß § 5 PStSG iVm. § 51 Abs. 2 SPG iVm. § 14 DSG 2000 bei jedem Verwenden personenbezogener Daten dazu verpflichtet, Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Dabei haben sie insbesondere auch sicherzustellen, dass die Daten Unbefugten nicht zugänglich sind (vgl. dazu im Detail oben Punkt I. 3.3.1.). Insofern ist gewährleistet, dass bei jeder Datenverwendung jeweils angemessene Geheimhaltungsvorkehrungen getroffen werden.

Vor diesem Hintergrund erscheint es nicht nachvollziehbar, inwiefern aus der — über diese für jede Datenverwendung geltenden Anordnungen hinausgehende — Verpflichtung zu 'angemessenen Vorkehrungen' in Bezug auf sensible und strafrechtlich relevante Daten gemäß § 9 Abs. 1 zweiter Satz PStSG der Schluss gezogen werden könnte, dass in Bezug auf nicht sensible oder strafrechtlich relevante Daten keine angemessenen Vorkehrungen zu treffen sind. Mit der Verpflichtung des § 9 Abs. 1 zweiter Satz PStSG wird vielmehr die besondere Sensibilität dieser Daten betont (vgl. ErIRV 1138 BIgNR 21. GP 28 zur entsprechenden Neufassung der Parallelbestimmung des § 51 Abs. 1 SPG). Die Verpflichtung trägt zudem § 1 Abs. 2 DSG 2000 Rechnung, der anordnet, dass für 'Daten, die ihrer Art nach besonders schutzwürdig sind' ('sensible Daten'), angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festzulegen sind. Die Unterscheidung zwischen 'besonders schutzwürdigen' bzw. 'sensiblen' und sonstigen personenbezogenen Daten und die verstärkte Betonung der Geheimhaltung sensibler Daten ist daher bereits in § 1 Abs. 2 DSG 2000 grundgelegt und geht — im Hinblick darauf, dass § 9 Abs. 1 zweiter Satz PStSG auch für strafrechtlich relevante Daten angemessene Vorkehrungen fordert — sogar darüber hinaus. In der Regelung manifestiert sich somit gerade die besondere Sensibilität der Gesetzgebung gegenüber den verwendeten Daten.

6.4.5. Wenn die Antragsteller schließlich vorbringen, dass § 9 Abs. 1 letzter Satz PStSG das Umgehungsverbot gesetzlicher Verschwiegenheitspflichten zu eng fasse, da die Bestimmung nur auf § 157 StPO betreffend Aussageverweigerungsrechte abstelle, ist ihnen gleichfalls das allgemeine Gebot der Wahrung der Verhältnismäßigkeit gemäß § 9 Abs. 1 erster Satz PStSG entgegen zu halten: Daraus ergibt sich, dass andere als die in § 9 Abs. 1 PStSG ausdrücklich genannten gesetzlichen Verschwiegenheitspflichten jedenfalls im Rahmen der in jedem Einzelfall vorzunehmenden Verhältnismäßigkeitsprüfung zu beachten und insofern bei der Entscheidung über die Zulässigkeit der Datenverwendung zu berücksichtigen sind. Der Umstand, dass bestimmte gesetzliche Verschwiegenheitspflichten durch absolute Ermittlungsverbote (wie jenes nach § 9 Abs. 1 letzter Satz PStSG) besonders geschützt werden, steht dem nicht entgegen. Auch insofern verkennen die Antragsteller also die Rechtslage.

In der Sache:

6.5. Die Antragsteller behaupten, dass einzelne Bestimmungen des PStSG — insbesondere §§ 6, 10, 11 und 12 PStSG — das Grundrecht auf Datenschutz verletzen, da sie (zu) weitgehende und daher unverhältnismäßige Eingriffe zuließen. Dem hält die Bundesregierung im Einzelnen Folgendes entgegen:

Zu den Aufgaben:

6.5.1.1. Ziel des polizeilichen Staatsschutzes ist es, die im Staatsgebiet lebenden Menschen und die verfassungsmäßige Grundordnung zu schützen (vgl. ErIRV 763 BIgNR 25. GP 1). Die in § 6 Abs. 1 PStSG genannten Aufgaben der zur Wahrnehmung der Angelegenheiten des polizeilichen Staatsschutzes zuständigen Organisationseinheiten dienen diesem Zweck. Zu diesen Aufgaben zählen insbesondere die erweiterte Gefahrenerforschung in Bezug auf eine Gruppierung (§ 6 Abs. 1 Z 1 PStSG) — das ist die Feststellung einer Gefahrenquelle und des für die Abwehr einer Gefahr sonst maßgeblichen Sachverhaltes — und der (vorbeugende) Schutz vor verfassungsgefährdenden Angriffen (§ 6 Abs. 1 Z 2 und Z 3 PStSG). Voraussetzung der erweiterten Gefahrenerforschung nach § 6 Abs. 1 Z 1 PStSG ist die Prognose, dass es zu mit schwerer Gefahr für die öffentliche Sicherheit verbundener Kriminalität kommt. Voraussetzung des vorbeugenden Schutzes vor verfassungsgefährdenden Angriffen nach § 6 Abs. 1 Z 2 PStSG ist der begründete Gefahrenverdacht, dass eine Person einen verfassungsgefährdenden Angriff begehen wird. Voraussetzung des Schutzes vor verfassungsgefährdenden Angriffen nach § 6 Abs. 1 Z 3 PStSG ist, dass eine Person im Verdacht steht, im Ausland einen Sachverhalt verwirklicht zu haben, der einem verfassungsgefährdenden Angriff entspricht.

6.5.1.2. Nach dem Antragsvorbringen scheinen die inhaltlichen Bedenken der Antragsteller zunächst im Wesentlichen darin zu bestehen, dass die Aufgabe des vorbeugenden Schutzes vor verfassungsgefährdenden Angriffen gemäß § 6 Abs. 1 Z 2 PStSG unbestimmt sei und weit im Vorfeld einer strafbaren Handlung ansetze sowie, dass die Definition des verfassungsgefährdenden Angriffs überschießend sei. Das PStSG würde damit in unverhältnismäßiger Weise Grundrechtseingriffe gestatten. Dem hält die Bundesregierung Folgendes entgegen:

6.5.1.2.1. Unter Punkt III. 5.3.2. wurde bereits dargelegt, dass der Begriff des 'begründeten Gefahrenverdachts', an den die Aufgabe des vorbeugenden Schutzes vor verfassungsgefährdenden Angriffen gemäß § 6 Abs. 1 Z 2 PStSG anknüpft, hinreichend bestimmt ist und damit klar geregelt ist, unter welchen Voraussetzungen ein Tätigwerden im Rahmen des vorbeugenden Schutzes vor verfassungsgefährdenden Angriffen zulässig ist.

6.5.1.2.2. § 6 Abs. 2 PStSG enthält die Definition des verfassungsgefährdenden Angriffs. Entgegen dem Vorbringen der Antragsteller (Antrag S 39 ff) ist eine Struktur des Straftatenkataloges klar erkennbar: Jede Ziffer umfasst Delikte, die bestimmten fachspezifischen Tätigkeitsbereichen des polizeilichen Staatsschutzes zugehören: Erfasst sind gerichtlich strafbare Handlungen, die — grob zusammengefasst — in Bezug zu Terrorismus (Z 1), Extremismus (Z 2), Handlungen gegen das Staatswesen (Z 3), der Abwehr nachrichtendienstlicher Tätigkeit,

Spionage, Waffenhandel und Proliferation (Z 4) und Cyberdelikten gegen verfassungsmäßige Einrichtungen und kritische Infrastrukturen (Z 5) stehen und damit ein großes Bedrohungspotential aufweisen (vgl. dazu die Ausführungen oben unter Punkt I 3.2.4.). Dass bei einigen Delikten — als einschränkendes Tatbestandsmerkmal — das Vorliegen einer bestimmten Motivation für ihre Begehung Voraussetzung ist, entspricht der Logik eines — eben auf bestimmte Bedrohungsszenarien – eingeschränkten Tätigkeitsfeldes des polizeilichen Staatsschutzes.

6.5.1.2.3. Die Definition des verfassungsgefährenden Angriffs ist daher ebenso wie jene des gefährlichen Angriffs gemäß § 16 Abs. 2 SPG streng strafrechtsakzessorisch. Im Unterschied zum gefährlichen Angriffs iSd. § 16 Abs. 2 SPG erfasst § 6 Abs. 2 PStSG jedoch nur einzelne, besondere Straftatbestände. Nach Auffassung der Bundesregierung kann kein Zweifel daran bestehen, dass eine solche strafrechtsakzessorische Festlegung polizeilicher Aufgabe verfassungsrechtlich an sich zulässig ist.

Die in § 6 Abs. 2 PStSG genannten Straftaten vermögen jede Einzelne auch eine gravierende Bedrohung der in Art. 8 Abs. 2 EMRK genannten Ziele darzustellen. Die Abwehr der Verwirklichung solcher Handlungen bzw. der von ihnen ausgehenden Gefahren stellt daher zweifellos eine Maßnahme dar, die gemäß Art. 8 Abs. 2 EMRK in einer demokratischen Gesellschaft — nämlich insbesondere für die nationale Sicherheit, die Verteidigung der Ordnung, zur Verhinderung von strafbaren Handlungen und zum Schutz der Rechte und Freiheiten anderer — notwendig ist (vgl. VfSlg. 19.892/2014). Es ist daher verfassungsrechtlich unbedenklich, wenn die Gesetzgebung zur Vorbeugung solcher Bedrohungsszenarien polizeiliche Aufgaben begründet.

6.5.1.2.4. § 6 Abs. 2 PStSG listet die einzelnen erfassten Straftaten — mitunter sogar differenziert nach gewissen Begehungsformen — auf und erfasst damit konkrete Fallgestaltungen, bei denen die Gesetzgebung von einem besonderen Bedrohungspotential ausgeht. Im Hinblick auf die von diesen Straftaten erfassten Schutzgüter (wie insbesondere das Leben und die körperliche Unversehrtheit von Menschen, die Funktionsfähigkeit des Staates oder die öffentliche Sicherheit) vermag die Bundesregierung keinen Grund zu erkennen, aus dem die Gesetzgebung mit dieser Wertung ihren rechtspolitischen Gestaltungsspielraum überschritten haben sollte.

Auch die von den Antragstellern als 'unsachlich' bezeichnete Differenzierung zwischen 'ideologisch oder religiös motivierter' und anderer Gewalt beruht auf der — insbesondere im Hinblick auf den Inhalt dieser Formulierung (s. oben Punkt III. 5.3.2.) gerechtfertigten — Annahme eines erhöhten Bedrohungspotentials von ideologisch oder religiös motivierter Gewalt. Sie ist daher ebenfalls das Ergebnis einer legitimen gesetzgeberischen Entscheidung.

Mit der konkreten Aufzählung jener Straftaten, deren Verwirklichung einen verfassungsgefährdenden Angriff darstellt, angesichts der Schwere dieser Straftaten und ihres besonderen Bedrohungspotentials sowie im Hinblick darauf, dass

mit hinreichender Bestimmtheit geregelt ist, unter welchen Voraussetzungen (und damit auch zu welchem Zeitpunkt) ein Tätigwerden zulässig ist (s. oben Punkt III. 6.6.1. sowie ausführlich Punkt I. 3.2.1.3., 3.2.2.2., 3.2.3.), hat die Gesetzgebung nach Auffassung der Bundesregierung daher den Anforderungen des § 1 Abs. 2 DSG 2000 bzw. Art. 8 Abs. 2 EMRK entsprechend sichergestellt, dass Eingriffe nur bei Vorliegen gewichtiger öffentlicher Interessen zulässig sind und die Schwere der drohenden Straftat im Einzelfall den Eingriff in die verfassungsgesetzlich gewährleisteten Rechte der Betroffenen rechtfertigen kann.

Zu den Befugnissen:

6.5.2. Die Antragsteller bringen der Sache nach vor, dass die in §§ 10, 11 und 12 PStSG vorgesehenen Befugnisse das Grundrecht auf Datenschutz und das Recht auf Achtung des Privat- und Familienlebens schon deshalb verletzen, weil sie die Zulässigkeit eines Eingriffes nicht abschließend regeln bzw. nicht näher konkretisieren. Dazu weist die Bundesregierung vorab auf Folgendes hin:

Gesetzliche Regelungen polizeilicher Ermittlungsbefugnisse folgen im Rechtsstaat immer demselben Muster. Es werden bestimmte abstrakt formulierte Gefahrensituationen beschrieben, in denen die Exekutivorgane im Rahmen einer — von ihnen ex ante vorzunehmenden — Verhältnismäßigkeitsprüfung zu beurteilen haben, ob die gesetzlich vorgesehene Befugnisausübung im konkreten Fall erforderlich und verhältnismäßig ist. Diesem Muster folgen auch die gesetzlichen Eingriffsermächtigungen des PStSG. Sie unterscheiden sich insoweit — hinsichtlich ihrer Struktur und ihres Determinierungsgrades — nicht von den Befugnissen des SPG oder der StPO.

Wie im Folgenden im Einzelnen dargelegt wird, sind die besonderen Ermittlungs- und Verarbeitungsbefugnisse der §§ 10, 11 und 12 PStSG zur Erfüllung der Aufgaben des polizeilichen Staatsschutzes geeignet, erforderlich und verhältnismäßig. Insbesondere hat die Gesetzgebung angemessene Garantien für die Verhältnismäßigkeit der jeweiligen Eingriffe sowie — durch die Einbindung des Rechtsschutzbeauftragten bzw. des Rechtsschutzsenats — einen Schutz gegen einen Missbrauch dieser Befugnisse vorgesehen.

6.5.2.1. Die Bundesregierung verweist zunächst auf die ausführliche Darstellung des Inhaltes und der Reichweite der Befugnisse gemäß §§ 10, 11 und 12 PStSG unter Punkt I. 3.3.2., 3.3.3. und 3.3.5. Daraus ergibt sich bereits, dass diese Befugnisse — insbesondere im Hinblick auf die Regelungen über die Voraussetzungen der Datenverwendung, die konkret betroffenen Personenkreise, des jeweils einzuhaltenden Verfahrens und der Aufbewahrungsdauer der Daten — jeweils den von Verfassungsgerichtshof und EGMR geforderten Bestimmtheitserfordernissen im Hinblick auf Eingriffe in das Grundrecht auf Datenschutz gemäß § 1 DSG 2000 bzw. in das Recht auf Achtung des Privat- und Familienlebens gemäß Art. 8 EMRK entsprechen. Auch die Datenarten, die dabei im Einzelfall ermittelt und verarbeitet werden dürfen, sind grundsätzlich zur Erfüllung der Aufgaben gemäß § 6 Abs. 1 PStSG bzw. zur Erreichung der Ziele des PStSG geeignet. Des Weiteren werden die Eingriffsbefugnisse sowie der bei der Wahrnehmung der

entsprechenden Maßnahmen jeweils eingeräumte Ermessensspielraum unter Berücksichtigung des jeweils konkret verfolgten Ziels klar umschrieben. Welche Datenarten für eine im konkreten Einzelfall zu erfüllende Aufgabe auf welche Art und Weise und für wie lange verwendet werden, ist außerdem stets nach den Vorgaben des Verhältnismäßigkeitsgebotes zu entscheiden.

6.5.2.2. Wie bereits oben unter Punkt I. 3.3.1. ausführlich dargelegt wurde, übernimmt das PStSG die — auch dem SPG systematisch zu Grunde liegende — Trennung von Aufgaben und Befugnisse und deren strikte Akzessorietät (vgl. dazu grundlegend Wiederin, Sicherheitspolizei [1998] Rz. 341: 'elementare rechtsstaatliche Errungenschaft'): Die in den §§ 10 und 11 PStSG geregelten Befugnisse dürfen daher ausschließlich im Rahmen der in § 6 Abs. 1 PStSG (bzw. in § 8 PStSG) genannten Aufgaben ausgeübt werden. Dieser Grundsatz wird in § 9 Abs. 2 PStSG auch ausdrücklich festgeschrieben. Eine Ermittlung personenbezogener Daten ohne Konnex zur Erfüllung einer aktuell vorliegenden Aufgabe des polizeilichen Staatsschutzes — somit gleichsam 'auf Vorrat' — ist damit jedenfalls ausgeschlossen.

6.5.2.3. § 9 PStSG knüpft die Zulässigkeit jeder Datenverwendung sowohl in zeitlicher als auch inhaltlicher Sicht an die Voraussetzung der Verhältnismäßigkeit und Erforderlichkeit der Maßnahme. Die zur Wahrnehmung der Angelegenheiten des polizeilichen Staatsschutzes zuständigen Organisationseinheiten dürfen daher ganz grundsätzlich immer nur das jeweils gelindeste Mittel ergreifen und auch das nur, wenn es in einem vertretbaren Verhältnis zum angestrebten Erfolg steht. Auch daraus ergibt sich also ein striktes Verbot der Ermittlung von Daten 'auf Vorrat'.

6.5.2.4. Hinsichtlich sensibler Daten gemäß § 4 Z 2 DSG 2000 zieht § 10 Abs. 1 PStSG — der festlegt, für welche Zwecke personenbezogene Daten ermittelt werden dürfen (vgl. oben Punkt I.3.3.2.1.) — eine weitere Erforderlichkeitsschranke ein: Diese dürfen nur insoweit ermittelt und verarbeitet werden, als sie für die Erfüllung der Aufgabe 'unbedingt erforderlich' sind. Entgegen der Auffassung der Antragsteller (Antrag S 49) dürfen sensible Daten daher nicht immer automatisch dann verarbeitet werden, wenn eine Zuständigkeit — gemeint wohl: Aufgabe — des BVT besteht. Vielmehr sind an die Zulässigkeit einer entsprechenden Datenverwendung erhöhte Anforderungen — eben ihre 'unbedingte Erforderlichkeit' — gestellt.

6.5.2.5. Abgestuft nach der Schwere des mit der Ermittlung und der (Weiter)Verarbeitung verbundenen Eingriffs schränken die §§ 10 und 11 PStSG einzelne Ermittlungs- oder Verarbeitungsermächtigungen des Weiteren auf bestimmte Aufgaben ein, binden sie zusätzlich an weitere Voraussetzungen oder beschränken ihre Dauer (s. dazu ausführlich bereits oben unter Punkt I 3.3.3., I 3.3.6): So dürfen beispielsweise besonders eingriffsintensive Maßnahmen wie die verdeckte Ermittlung oder die Einholung von Telekommunikationsdaten nur dann erfolgen, wenn die Erfüllung der Aufgabe durch den Einsatz anderer Ermittlungsmaßnahmen aussichtslos wäre (Z 2 und 5); die Zulässigkeit der Einholung bestimmter Telekommunikationsdaten ist weiters (inhaltlich) auf Fälle zur Vor-

beugung besonders gravierender verfassungsgefährdender Angriffe sowie (zeitlich) auf jenen Zeitraum eingeschränkt, der zur Erreichung des Zwecks voraussichtlich erforderlich ist (Z 7). Das PStSG nimmt somit schon selbst entsprechend dem 'ultima ratio' Gedanken eine Gewichtung der einzelnen Ermittlungsbefugnisse untereinander vor.

6.5.2.6. Mit den Aktualisierungs- und Löschungsverpflichtungen des § 12 Abs. 2 und 3 sowie des § 13 PStSG normiert das PStSG darüber hinaus zum einen Vorkehrungen dafür, dass die Richtigkeit der Daten während ihrer Verwendung gewährleistet ist, zum anderen weitere Beschränkungen für die zulässige Dauer der einzelnen Datenverwendung. Auch damit wird die Verhältnismäßigkeit der konkreten Datenverarbeitung (in einer Datenanwendung) gewährleistet.

Um die Einhaltung der Löschungsfristen des § 12 Abs. 3 PStSG in der Praxis zu garantieren, wurden automatisierte Wiedervorlagen vor Ablauf der gesetzlichen Maximalfrist programmiert: Bei der Anlegung eines Datensatzes in der Datenbank wird automatisiert das entsprechende Löschdatum mitprogrammiert; dieses kann vom Datenbanknutzer nicht beeinflusst werden und führt zur automatischen Löschung des betroffenen Datensatzes zu dem gesetzlich vorgesehenen Zeitpunkt.

Im Übrigen sind Daten, die nach den Bestimmungen des PStSG ermittelt und — nicht in einer Datenanwendung nach § 12 PStSG, sondern im Rahmen der allgemeinen Aktenverwaltung gemäß § 5 PStSG iVm. § 13a SPG — weiterverarbeitet wurden, nach § 5 PStSG iVm. § 13a SPG zu löschen.

6.5.2.7. Neben diese inhaltlichen und zeitlichen Beschränkungen der Datenverwendung treten Vorkehrungen zur Sicherheit der ermittelten und verarbeiteten Daten: Soweit Daten verwendet werden, sind gemäß § 5 PStSG iVm. § 51 Abs. 2 SPG iVm. § 14 DSG 2000 die entsprechenden Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Hinsichtlich sensibler und strafrechtlich relevanter Daten wird in § 9 Abs. 1 zweiter Satz PStSG besonders hervorgehoben, dass angemessene — dh. auf die besonderen Eigenschaften dieser Datenkategorien abgestimmte — Vorkehrungen zur Wahrung der Geheimhaltungsinteressen zu treffen sind (vgl. dazu oben I. 3.3.1.). Diese bestehen im Bereich des polizeilichen Staatschutzes insbesondere in Form eingeschränkter Zugriffsberechtigungen auf die eingesetzte Hard- und Software, eingeschränkter Zutrittsberechtigungen zu den betreffenden Räumlichkeiten sowie der Verschlüsselung sensibler Daten. Des Weiteren werden in Entsprechung der Verpflichtung des § 14 DSG 2000 alle tatsächlich durchgeführten Verwendungsvorgänge im System, wie insbesondere Änderungen, Abfragen und Übermittlungen, automationsunterstützt protokolliert und sind damit jederzeit nachvollziehbar.

6.5.2.8. Um die Einhaltung dieser Verpflichtungen sicherzustellen, wurden umfassende Schulungs- und Sensibilisierungsmaßnahmen getroffen. Zudem sieht die Verordnung des Bundesministers für Inneres über die spezielle Ausbildung für Verfassungsschutz und Terrorismusbekämpfung — AusbV-VT, BGBl. II Nr. 170/2016, für die gemäß § 2 Abs. 3 PStSG zu absolvierende spezielle Ausbildung

der Bediensteten der für Angelegenheiten des polizeilichen Staatsschutzes zuständigen Organisationseinheiten mindestens vier Unterrichtseinheiten zum Datenschutz vor.

6.5.2.9. Die Bundesregierung geht vor diesem Hintergrund davon aus, dass die Regelungen über die Ermittlungsbefugnisse gemäß §§ 10, 11 und 12 PStSG zur Erfüllung der Aufgaben gemäß § 6 PStSG weder gegen das Grundrecht auf Datenschutz gemäß § 1 DSG 2000 noch gegen Art. 8 Abs. 1 EMRK verstoßen.

Das Vorbringen der Antragstellerin Bezug auf andere Bestimmungen des PStSG vermag — soweit dabei konkrete Bedenken erkennbar sind — kein anderes Ergebnis zu begründen:

6.5.2.10. Soweit die Antragsteller behaupten, dass § 11 Abs. 1 Z 1 und 2 PStSG im Vergleich zu den Bestimmungen der StPO einen erleichterten Zugang zu den Ermittlungsinstrumenten der Observation und verdeckten Ermittlung zulasse und insofern unverhältnismäßig sei (Antrag S 53), verkennen sie die Rechtslage:

Zum einen ist die Zulässigkeit einer derartigen Ermittlungsmaßnahme nach § 11 Abs. 1 erster Satz PStSG — wie nach § 131 Abs. 1 StPO — an die Erforderlichkeit der Maßnahme zur Erfüllung der Aufgabe gebunden. Zum anderen bedarf sie einer Vorabgenehmigung, die im Bereich der StPO der Staatsanwalt (§ 133 Abs. 1 StPO), im Bereich des PStSG der weisungsfreie Rechtsschutzbeauftragte bzw. der Rechtsschutzsenat (§ 14 Abs. 2 und 3 PStSG) erteilt. Staatsanwalt wie Rechtsschutzbeauftragter bzw. Rechtsschutzsenat haben in jedem Einzelfall die Verhältnismäßigkeit der Maßnahme und — bei grundsätzlicher Bejahung ihrer Zulässigkeit — ihre höchstzulässige Dauer zu prüfen und dabei insbesondere abzuwägen, wie lange die Ermittlung voraussichtlich erforderlich sein wird (vgl. Zerbes, in Fuchs/Ratz [Hrsg.] Wiener Kommentar zur StPO [161. Lfg. 2011] § 133 Rz 6). In beiden Fällen ist zudem gesetzlich ausdrücklich angeordnet, dass Ermittlungsmaßnahmen zu beenden sind, sobald ihre Voraussetzungen wegfallen (vgl. § 133 Abs. 2 StPO und § 11 Abs. 1 letzter Satz PStSG). Dass die StPO eine Genehmigung jeweils nur (verlängerbar) für die Dauer von bis zu drei Monaten (§ 133 Abs. 2 StPO), das PStSG demgegenüber eine Ermächtigung (verlängerbar) für die Dauer von bis zu sechs Monaten (§ 14 Abs. 2 PStSG) zulässt, führt — schon im Hinblick darauf, dass es sich dabei um eine Höchstfrist handelt und die Bemessung der konkreten Frist nach dem Verhältnismäßigkeitsprinzip zu erfolgen hat — nicht zur Unverhältnismäßigkeit der Regelung.

6.5.2.11. Daneben erblicken die Antragsteller in der Möglichkeit des Einsatzes bezahlter Vertrauenspersonen als verdeckte Ermittler gemäß § 11 Abs. 1 Z 2 PStSG, der Einholung bestimmter Auskünfte von Betreibern öffentlicher Telekommunikationsdienste und sonstiger Diensteanbieter gemäß § 11 Abs. 1 Z 5 PStSG bzw. in den Ermittlungsbefugnissen gemäß § 11 Abs. 1 Z 7 PStSG jeweils einen unverhältnismäßigen Eingriff in Art. 8 EMRK bzw. § 1 DSG 2000.

Dazu verweist die Bundesregierung zunächst auf die obigen Ausführungen unter Punkt I.3.3.3. zu den Voraussetzungen der entsprechenden Maßnahmen und

ihrer höchstzulässigen Dauer sowie zur generellen Verpflichtung zur Beachtung der Verhältnismäßigkeit gemäß § 9 Abs. 1 PStSG und zur Einholung einer Ermächtigung des Rechtsschutzbeauftragten bzw. Rechtsschutzsenats vor Beginn der Aufgabenerfüllung. Bereits daraus ergibt sich, dass die entsprechenden Regelungen keinen unverhältnismäßigen Eingriff in § 1 DSG 2000 bzw. Art. 8 EMRK bewirken können. Ergänzend wird auf Folgendes hingewiesen:

6.5.2.12. Beim Einsatz einer Vertrauensperson als verdeckter Ermittler hat die zuständige Behörde gemäß § 11 Abs. 1 Z 2 PStSG iVm. § 54 Abs. 3a SPG die Verpflichtung, die Person zu führen, regelmäßig zu überwachen und den Einsatz und dessen nähere Umstände sowie Auskünfte und Mitteilungen, die durch sie erlangt werden, zu dokumentieren. Diese Verpflichtungen entsprechen jenen des § 131 Abs. 3 StPO. Sie stellen sicher, dass die zuständigen Behörden das Verhalten der Vertrauenspersonen während ihres Einsatzes kontrollieren und bei Bedarf auch effektiv beeinflussen können (vgl. ErIRV 763 BlgNR 25. GP 14). Damit wird der erforderliche behördliche Einfluss auf eine Vertrauensperson gewährleistet (vgl. Wiederin, Vertrauenspersonen als verdeckte Ermittler nach dem SPG und als Scheinkäufer nach der StPO in Reindl-Krauskopf/Zerbes/Brandstetter/Lewisch/Tipold [Hrsg.], Festschrift für Helmut Fuchs [2014] 657 [663).

6.5.2.13. Was die Einholung bestimmter Auskünfte von Betreibern öffentlicher Telekommunikationsdienste und sonstiger Diensteanbieter gemäß § 11 Abs. 1 Z 5 PStSG betrifft, wird zunächst auf das Erkenntnis des Verfassungsgerichtshofes VfSlg. 19.657/2012 hingewiesen. In diesem Erkenntnis hat der Verfassungsgerichtshof die entsprechende Regelung des § 53 Abs. 3a SPG — an die in § 11 Abs. 1 Z 5 PStSG angeknüpft wird — als verhältnismäßig qualifiziert. Ferner wird auf die Ausführungen des Verfassungsgerichtshofes zu Inhalt und Reichweite des § 53 Abs. 3b SPG — an den in § 11 Abs. 1 Z 5 PStSG ebenfalls angeknüpft wird — in den Erkenntnissen VfSlg. 18.830/2009 und 18.831/2009 hingewiesen.

Ergänzend wird auf die gleichzeitig mit der Erlassung des PStSG in Kraft getretene Änderung des § 94 Abs. 4 TKG 2005 durch die Novelle BGBl. I Nr. 6/2016 hingewiesen: Diese Bestimmung ordnet an, dass die Übermittlung von Verkehrs-, Standort- sowie Stammdaten, welche die Verarbeitung von Verkehrsdaten erfordern, über eine — die sichere Übermittlung gewährleistende — Durchlaufstelle zu erfolgen hat. Dadurch ist zum einen gewährleistet, dass die Dateneinholung und -beauskunftung über einen verschlüsselten Übertragungskanal erfolgt (gemäß § 9 Abs. 1 Datensicherheitsverordnung — TKG-DSVO ist die Durchlaufstelle ein elektronisches Postfachsystem zur Sicheren Abwicklung von Anfragen und Auskünften iSd. § 94 Abs. 4 TKG 2003). Da die Durchlaufstelle auch eine Funktion zur automatisierten Erfassung der statistischen Daten über sämtliche Auskunftsverlangen enthält und der Rechtsschutzbeauftragte gemäß §§ 14 Abs. 3 iVm. § 22 Abs. 4 TKG-DSVO zu Kontrollzwecken an die Durchlaufstelle angebunden wird, ist zum anderen sichergestellt, dass der Rechtsschutzbeauftragte überprüfen kann, ob für alle getätigten Abfragen auch eine Ermächtigung vorlag.

6.5.2.14. Hinsichtlich der Ermittlungsbefugnis nach § 11 Abs. 1 Z 7 PStSG (Rufdatenrückerfassung) weist die Bundesregierung darauf hin, dass ihre Inanspruchnahme — wie oben dargelegt wurde (s. Punkt I. 3.3.3.3.) — an besonders strenge Erforderlichkeitsanforderungen gebunden ist. Sie steht somit, entgegen dem Vorbringen der Antragsteller (Antrag S 60), keineswegs in jedem Fall des Vorliegens einer Aufgabe gemäß § 6 Abs. 1 Z 1 und 2 PStSG offen.

Insbesondere muss für eine solche Ermittlungsmaßnahme die vorherige Genehmigung des Rechtsschutzsenates eingeholt werden. Die Vorabkontrolle erfolgt in diesem Fall daher nicht bloß durch eine einzelne, besonders qualifizierte Person — nämlich den Rechtsschutzbeauftragten —, sondern durch das Zusammenwirken dreier besonders qualifizierter Personen (vgl. zur Vorabkontrolle durch den Rechtsschutzbeauftragten bzw. den Rechtsschutzsenat sogleich unter Punkt III. 6.6.5.).

Auch die Ermittlung dieser Daten hat gemäß § 94 Abs. 4 TKG 2003 über eine — die sichere Übermittlung gewährleistende — Durchlaufstelle zu erfolgen.

6.5.2.15. Soweit die Antragsteller schließlich die Unverhältnismäßigkeit der Datenanwendung gemäß § 12 Abs. 1 PStSG behaupten, verweist die Bundesregierung wiederum zunächst auf die Ausführungen unter Punkt I. 3.3.5. Ergänzend wird dem Bedenken Folgendes entgegen gehalten:

Die in § 12 Abs. 1 PStSG vorgesehene Verarbeitung und Analyse der Daten findet innerhalb einer einzigen Datenanwendung statt. Die Nutzung eines solchen Informationsverbundsystems stellt daher — entgegen den Behauptungen der Antragsteller (Antrag S 62) — keinen automationsunterstützten Datenabgleich im Sinne des § 141 StPO (sog. 'Rasterfahndung') dar.

Übermittlungen dürfen nur an die in § 12 Abs. 4 PStSG genannten Stellen erfolgen. Jede Abfrage und Übermittlung ist gemäß § 12 Abs. 5 PStSG zu protokollieren. Für Übermittlungen ins Ausland gelten zusätzlich die §§ 8 ff PolKG. Danach ist eine Übermittlung nur zulässig, wenn sie auch bei einem gleichgelagerten inländischen Sachverhalt an eine nationale Behörde erfolgen dürfte. Daraus folgt, dass auch Übermittlungen ins Ausland nur aus den in § 12 Abs. 4 PStSG taxativ genannten Zwecken zulässig sind. Weiters muss die Einhaltung der datenschutzrechtlichen Grundsätze auch im Ausland gewährleistet werden. Die Verpflichtung zur Protokollierung jeder Übermittlung dient auch dem Zweck, die gesetzlich vorgesehene Verständigung des Empfängers zu ermöglichen, wenn sich übermittelte Daten nachträglich als unrichtig erweisen. Alle Übermittlungen personenbezogener Daten werden automationsunterstützt dokumentiert, wodurch eine lückenlose Nachvollziehbarkeit dieser Vorgänge, die auch dem Einsichtsrecht des Rechtsschutzbeauftragten gemäß § 15 Abs. 1 PStSG unterliegt, gewährleistet wird.

Durch interne Dienstvorschriften wurden für die Datenverwendung umfassende Vorgaben hinsichtlich der Zulässigkeit der Verarbeitung einschließlich der Dauer der Speicherung der Daten und umfassende Kontrollmechanismen sowie Vor-

kehrungen zur Datensicherheit festgeschrieben: Die Zugriffsberechtigungen auf Daten und Programme sind stark eingeschränkt und sämtliche Verwendungsvorgänge — insbesondere Änderungen, Abfragen und Übermittlungen — werden protokolliert, wodurch gleichfalls eine lückenlose Nachvollziehbarkeit gewährleistet ist.

Gemäß § 12 Abs. 6 PStSG obliegt die Kontrolle der Datenanwendung gemäß § 12 Abs. 1 PStSG dem Rechtsschutzbeauftragten zunächst nach Maßgabe des § 91c Abs. 2 SPG. Danach ist die Errichtung einer Analysedatenbank bereits als Vorhaben dem Rechtsschutzbeauftragten zur Kenntnis zu bringen, wobei dieser das Recht hat, sich binnen drei Tagen dazu zu äußern. Die tatsächliche Durchführung der Maßnahme darf erst nach Ablauf dieser Frist oder bei Vorliegen einer entsprechenden Äußerung erfolgen.

6.5.2.16. Zusammenfassend ergibt sich somit, dass die Datenverwendungsbefugnisse gemäß §§ 10, 11 und 12 PStSG weder gegen das Grundrecht auf Datenschutz gemäß § 1 DSG 2000 noch gegen das Recht auf Achtung des Privat- und Familienlebens gemäß Art. 8 EMRK verstoßen.

6.5.3. Dieses Ergebnis wird durch die Regelungen des PStSG über die Kontrolle der Durchführung von Datenverwendungen gemäß den §§ 10, 11 und 12 PStSG — wie im Folgenden gezeigt wird — gestützt. Diese Regelungen verstoßen andererseits — entgegen dem Vorbringen der Antragstellers — auch nicht gegen das Recht auf eine wirksame Beschwerde im Hinblick auf das Recht auf Achtung des Privat- und Familienlebens:

6.5.4. Die Kontrolle der Datenverwendung:

Zur Vermeidung von Missbrauch der Datenermittlung und -verarbeitung tritt neben die gemäß §§ 9, 10, 11, 12 und 13 PStSG jeweils gesetzlich vorgeschriebenen zeitlichen und sachlichen Begrenzungen der Maßnahmen sowie neben die entsprechenden Vorkehrungen zur Datensicherheit die begleitende besondere Kontrolle durch den unabhängigen Rechtsschutzbeauftragten bzw., bei besonders eingriffsintensiven Maßnahmen, durch den Rechtsschutzsenat (vgl. dazu ausführlich oben unter Punkt I. 3.4.1.) sowie die nachprüfende Kontrolle durch die Datenschutzbehörde.

6.5.4.1. § 14 PStSG überträgt dem unabhängigen und weisungsfreien Rechtsschutzbeauftragten gemäß § 91a SPG bzw. dem Rechtsschutzsenat den besonderen Rechtsschutz bei Aufgaben nach § 6 Abs. 1 Z 1 und 2 PStSG (vgl. dazu ausführlich oben unter Punkt I. 3.4.1.)

6.5.4.2. Mit der Zuweisung des besonderen Rechtsschutzes an den Rechtsschutzbeauftragten gemäß § 91a SPG ist ein einheitliches Rechtsschutzsystem für die gesamte sicherheitspolizeiliche Aufgabenerfüllung gewährleistet. Für den Anwendungsbereich des PStSG wurde dieses etablierte Rechtsschutzsystem der Vorabbefassung des Rechtsschutzbeauftragten durch die Einrichtung eines

dreiköpfigen Rechtsschutzsenates für die Entscheidung in besonders sensiblen Bereichen sogar noch ausgebaut.

6.5.4.3. Das Gesetz stellt an die Qualifikation des Rechtsschutzbeauftragten — sowie seiner Stellvertreter — besondere Anforderungen: Sie müssen gemäß § 91b Abs. 1 SPG besondere Kenntnisse und Erfahrungen auf dem Gebiet der Grund- und Freiheitsrechte aufweisen und mindestens fünf Jahre in einem Beruf tätig gewesen sein, in dem der Abschluss des Studiums der Rechtswissenschaften Berufsvoraussetzung ist. Einer seiner Stellvertreter muss zumindest eine zehnjährige Erfahrung als Richter oder Staatsanwalt haben (§ 91a Abs. 2 SPG). Die persönlichen Qualifikationsvoraussetzungen sind damit — entgegen den Behauptungen der Antragsteller (Antrag S 30) — jenen eines unabhängigen Richters zumindest gleichwertig. Auch der Bestellmodus bietet Gewähr für die Bestellung besonders qualifizierter Personen und deren unabhängige Amtsausübung: Der Rechtsschutzbeauftragte und seine Stellvertreter werden gemäß § 91a Abs. 2 SPG vom Bundespräsidenten auf Vorschlag der Bundesregierung nach Anhörung der Präsidenten des Nationalrates sowie der Präsidenten des Verfassungsgerichtshofes und des Verwaltungsgerichtshofes für die Dauer von fünf Jahren ernannt. Damit ist auch hinsichtlich der Dauer der Bestellung den Anforderungen zur Sicherung der Unabhängigkeit eines Tribunals iSd. Art. 6 EMRK Rechnung getragen (vgl. VfSlg. 13.211/1992 mwN).

6.5.4.4. Vor der Durchführung einer konkreten Aufgabe haben die zur Wahrnehmung der Angelegenheiten des polizeilichen Staatsschutzes zuständigen Organisationseinheiten die Ermächtigung des Rechtsschutzbeauftragten — bzw. in den Fällen der besonderen Ermittlungsmaßnahmen des § 11 Abs. 1 Z 2 PStSG (verdeckte Ermittlung durch eine Vertrauensperson) und des § 11 Abs. 1 Z 7 PStSG (Auskunft über Verkehrs-, Zugangs- und Standortdaten) — des Rechtsschutzsenats einzuholen. Das Ersuchen um Ermächtigung ist entsprechend zu begründen, was es dem Rechtsschutzbeauftragten bzw. dem Rechtsschutzsenat ermöglicht, die gesetzliche Zulässigkeit der konkreten Maßnahme zu überprüfen. Die Ermächtigung darf nur in jenem Umfang und für jenen Zeitraum erteilt werden, der zur Erfüllung der Aufgabe voraussichtlich erforderlich ist, längstens jedoch für sechs Monate. Verlängerungen sind zulässig, was bei länger dauernden Maßnahmen eine regelmäßige Kontrolle durch den Rechtsschutzbeauftragten bzw. den Rechtsschutzsenat hinsichtlich ihrer (weiteren) Zulässigkeit gewährleistet. Entgegen dem Vorbringen der Antragsteller (Antrag S 31) ist mit der Zulässigkeit einer Verlängerung der Ermächtigung keineswegs eine 'Generalermächtigung [...], die auf den Grundsatz der Verhältnismäßigkeit keine Rücksicht nimmt' normiert: Maßstab der Überprüfung durch den Rechtsschutzbeauftragten bzw. den Rechtsschutzsenat ist die Übereinstimmung mit den gesetzlichen Vorgaben. In jedem Einzelfall ist daher auch die Einhaltung des Verhältnismäßigkeitsgebots des § 9 Abs. 1 PStSG zu prüfen, das eine auf den jeweiligen Einzelfall bezogene zeitliche Begrenzung der Maßnahmen erfordert.

Soweit die Antragsteller das Vorliegen eines effektiven Rechtsschutzes mit Verweis darauf verneinen, dass die Vorabkontrolle durch den Rechtsschutzbeauftragten keine richterliche Kontrolle darstellt (Antrag S 29), weist die Bundes-

regierung darauf hin, dass eine richterliche Genehmigung staatlicher Überwachungsmaßnahmen durch Art. 8 EMRK nicht geboten ist (vgl. VfSlg. 19.657/2012 mit Verweis auf EGMR, Urteil vom 10.2.2009, Iordachi ua gegen Moldawien, Appl. 25198/02, Z 40 mwN).

6.5.4.5. Durch die Verpflichtung zur Vorabbefassung des Rechtsschutzbeauftragten bzw. des Rechtsschutzsenates ist gesetzlich sichergestellt, dass ausnahmslos alle zur Erfüllung der Aufgaben gemäß § 6 Abs. 1 Z 1 und 2 PStSG durchzuführenden Ermittlungen dem Rechtsschutzbeauftragten oder dem Rechtsschutzsenat zur Kenntnis gelangen. Zusätzlich wurde für den Bereich des Staatsschutzes im Jahr 2012 ergänzend ein Kontrollsystem eingerichtet: Die Organisationseinheiten des BVT melden alle von ihnen durchgeführten Amtshandlungen an die dem Direktor des BVT unmittelbar unterstehende Rechtsabteilung. Diese — auch für die Erstattung der Meldungen an den Rechtsschutzbeauftragten zuständige, jedoch selbst nicht operativ tätige — Abteilung überprüft anhand ihrer Aufzeichnungen, ob die Verpflichtung zur Vorabbefassung des Rechtsschutzbeauftragten — bzw. des Rechtsschutzsenates — gemäß § 14 Abs. 2 und 3 PStSG vollständig eingehalten wurde. Das BVT berichtet dem Rechtsschutzbeauftragten vierteljährlich über die Ergebnisse dieser Kontrolle. Die Prüfung der Einhaltung der Meldedisziplin durch die jeweils für Verfassungsschutz zuständigen Organisationseinheiten der Landespolizeidirektionen erfolgt ebenfalls durch vierteljährlich zu erstattende Prüfberichte: Diese unter der Verantwortung der LPD erstellten Quartalsberichte beinhalten die stichprobenweise Prüfung der Meldedisziplin zu einer — je nach Bundesland unterschiedlich hohen — Anzahl von Ermittlungsakten. Die Prüfung von Maßnahmen, die im Ermittlungsbereich des Verfassungsschutzes liegen, ist dabei verpflichtend vorgesehen.

6.5.4.6. § 15 PStSG räumt dem Rechtsschutzbeauftragten darüber hinaus umfassende Einsichts-, Auskunfts-, Kontroll- und Überwachungsrechte ein, die lediglich für jene Fälle eingeschränkt sind, in denen die Identität einer Person gemäß § 162 StPO auch gegenüber dem erkennenden Gericht geheim bleiben kann (vgl. ausführlich oben Punkt I. 3.4.1.). Soweit die Antragsteller behaupten, die Befugnisse des Rechtsschutzbeauftragten seien eingeschränkt und seine Möglichkeiten zur Akteneinsicht unzureichend, da er niemals freien Zugang zu Akten habe (Antrag S 26 ff), gehen sie daher von falschen Prämissen aus und bringen der Sache nach im Übrigen lediglich Bedenken hinsichtlich der missbräuchlichen Vollziehung der genannten Bestimmungen vor.

Mindestens einmal jährlich unternimmt der Rechtsschutzbeauftragte Kontrollbesuche aller Dienststellen, die Ermächtigungen einzuholen haben. Dabei werden jeweils die vierteljährlich erstatteten Berichte erörtert sowie einzelne, als diskussionswürdig eingestufte Meldungsakte besprochen werden. Ersuchen um Ermächtigung besprochen. Weiters nimmt der Rechtsschutzbeauftragte regelmäßig Einsicht in die Dokumentation einzelner Fälle und prüft in Betrieb befindliche Videoüberwachungen. Insofern werden insbesondere der von den Kameras jeweils erfasste Bildausschnitt, die Dauer der Aufbewahrung der Bilddaten sowie die Maßnahmen, die zum Schutz unbeteiligter Dritter ergriffen wurden, überprüft. Durch die (Prüfung der) vierteljährlich zu erstattenden Berichte sowie die

jährlichen Kontrollbesuche finden daher — entgegen den Ausführungen der Antragsteller (Antrag S 31) — über die konkrete Fallprüfung zur Ermächtigungserteilung hinausgehende Maßnahmen zur Kontrolle der Rechtmäßigkeit von Ermittlungen im gesamten Bundesgebiet statt.

6.5.4.7. Die Einschränkung des besonderen Rechtsschutzes durch den Rechtsschutzbeauftragten bzw. den Rechtsschutzsenat auf Aufgaben nach § 6 Abs. 1 Z 1 und 2 PStSG hat ihren Grund darin, dass die Befugnisse zur Wahrnehmung der Aufgabe des § 6 Abs. 1 Z 3 PStSG im Wesentlichen auf die Entgegennahme von Informationen und deren Verarbeitung beschränkt sind (vgl. dazu oben Punkt I. 3.3.6.2.). Eingriffsintensive (besondere) Ermittlungsmaßnahmen stehen zur Erfüllung dieser Aufgabe demgegenüber nicht zur Verfügung, weshalb auch die Notwendigkeit einer Vorab-Ermächtigung durch den Rechtsschutzbeauftragten nicht gegeben ist. Auch in den Angelegenheiten des § 6 Abs. 1 Z 3 PStSG stehen einem Betroffenen aber die allgemeinen Auskunfts- und Löschungsrechte gemäß §§ 26 ff DSG 2000 und die Beschwerdemöglichkeit an die Datenschutzbehörde gemäß § 5 PStSG iVm. § 90 SPG zur Verfügung. Werden die Daten in einer Datenanwendung gemäß § 12 Abs. 1 PStSG (weiter)verarbeitet, bestehen zudem die besonderen Aktualisierungs- und Löschungsverpflichtungen gemäß § 12 Abs. 2 und 3 PStSG. Zudem unterliegt die Datenanwendung auch hinsichtlich der Daten, die zur Erfüllung der Aufgabe des § 6 Abs. 1 Z 3 PStSG verarbeitet werden, der Kontrolle des Rechtsschutzbeauftragten.

6.5.4.8. Nach Auffassung der Bundesregierung ist durch die Kontrolle des Rechtsschutzbeauftragten — die bereits im Vorfeld der Ermittlungsmaßnahme und, in Form umfassender Einsichts- und Überprüfungsbefugnisse, auch während ihrer Durchführung besteht — ein effektiver Schutz gegen Missbrauch der Datenverwendungsbefugnisse gemäß §§ 10, 11 und 12 PStSG gewährleistet.

6.5.4.9. Dem Schutz gegen Missbrauch dienen daneben auch die Informationspflichten des Rechtsschutzbeauftragten gemäß § 16 Abs. 1 sowie der zur Wahrnehmung der Angelegenheiten des polizeilichen Staatsschutzes zuständigen Organisationseinheiten gemäß § 16 Abs. 2 PStSG nach Ende der Ermittlungen. § 16 PStSG stellt damit nicht nur sicher, dass Betroffene von Datenermittlungsmaßnahmen zur Besorgung der Aufgaben nach § 6 Abs. 1 Z 1 und 2 PStSG Kenntnis erlangen. Die von solchen Ermittlungen Betroffenen werden dadurch in die Lage versetzt, eine Beschwerde bei der Datenschutzbehörde oder beim zuständigen Landesverwaltungsgericht zu erheben (§ 5 PStSG iVm §§ 88 und 90 SPG). Die Bestimmung dient insofern ebenfalls einem effektiven Rechtsschutz der Betroffenen. Die Einhaltung der Verpflichtung der der zur Wahrnehmung der Angelegenheiten des polizeilichen Staatsschutzes zuständigen Organisationseinheiten gemäß § 16 Abs. 2 PStSG unterliegt wiederum der Kontrolle durch den Rechtsschutzbeauftragten. Kann eine Information des Betroffenen aus den Gründen des § 26 Abs. 2 DSG 2000 — weil etwa überwiegende öffentliche Interessen der Information entgegen stehen — nicht erfolgen, greift ein kommissarischer Rechtsschutz durch den Rechtsschutzbeauftragten: Gemäß § 16 Abs. 1 PStSG ist der Rechtsschutzbeauftragte in diesen Fällen zur Erhebung einer Be-

schwerde an die Datenschutzbehörde verpflichtet, wenn Rechte von Betroffenen einer Aufgabe nach § 6 Abs. 1 Z 1 oder 2 PStSG verletzt worden sind.

6.5.4.10. Durch den kommissarischen Rechtsschutz durch den Rechtsschutzbeauftragten, die Vorkehrungen zur Information der einzelnen Betroffenen sowie die umfassenden Überprüfungszuständigkeiten der Datenschutzbehörde (vgl. dazu oben Punkt I. 3.4.2.) wird das Recht auf eine wirksame Beschwerde effektiv gewährleistet. Es liegt insofern daher — entgegen den Ausführungen der Antragsteller (Antrag S 33) — keine Verletzung des Art. 13 iVm. Art. 8 EMRK vor.

6.5.5. Zusammenfassend bieten die Regelungen des PStSG nach Auffassung der Bundesregierung ausreichend Gewähr dafür, dass konkret erfolgende Ermittlungsmaßnahmen auf Grundlage dieses Gesetzes das erforderliche Maß nicht überschreiten und die Schwere des dadurch erfolgenden Eingriffs Gewicht und Bedeutung der damit verfolgten Ziele jeweils nicht übersteigt, sondern zu diesen in einem angemessenen Verhältnis steht. Zudem ist insbesondere sichergestellt, dass bei Fallgestaltungen mit bloß geringem Bedrohungspotential keine Eingriffe erfolgen können. Eine Ermittlung von Daten auf Vorrat erfolgt nicht.

Die Einhaltung der jeweils vorgesehenen Voraussetzungen und Bedingungen sowie die allgemeine Verpflichtung zur Wahrung des Verhältnismäßigkeitsgebotes ist nicht allein der Verantwortung der handelnden Behörden überlassen, sondern unterliegt außerdem — soweit es sich um eingriffsintensive Ermittlungsmaßnahmen handelt — einer umfassenden ex-ante-, begleitenden und ex-post-Kontrolle durch den Rechtsschutzbeauftragten bzw. den Rechtsschutzsenat. Vor diesem Hintergrund erweisen sich die Bedenken der Antragsteller hinsichtlich der Anwendung der angefochtenen Bestimmungen — wann etwa ein 'ideologisches oder religiöses' Motiv einem verfassungsgefährdenden Angriffs zu Grunde liegt (Antrag S 41), welches Verhalten Anlass zur Befürchtung einer zukünftigen Verhetzung geben kann (Antrag S 42 und 43) oder wann ein Verhalten die zukünftige Begehung eines Cyberdelikts gegen verfassungsmäßige Einrichtungen und kritische Infrastrukturen befürchten lässt (Antrag S 43) — nach Auffassung der Bundesregierung von vornherein als unbegründet. Insbesondere im Hinblick auf die Verpflichtung zur Beachtung des Verhältnismäßigkeitsgebotes ist auch ausgeschlossen, dass — wie die Antragsteller behaupten — bereits eine 'sachliche aber scharfe Kritik an einer der in § 283 Abs. 1 Z 1 StGB genannten Gruppen als eine Vorstufe zu einer späteren Verbreitung von Gewaltaufrufen' gedeutet wird (vgl. die Ausführungen im Antrag S 42). Nur der Vollständigkeit halber merkt die Bundesregierung an, dass es sich dabei im Verfahren nach Art. 140 B-VG nicht um zulässige Bedenken gegen das Gesetz handelt.

Im Hinblick auf den kommissarischen Rechtsschutz durch den Rechtsschutzbeauftragten, die Vorkehrungen zur Information der einzelnen Betroffenen sowie die umfassenden Überprüfungszuständigkeiten der Datenschutzbehörde liegt auch kein Verstoß gegen das Recht auf eine wirksame Beschwerde gemäß Art. 13 iVm Art. 8 EMRK vor.

7. Zu den Bedenken im Hinblick auf das Sachlichkeitsgebot:

7.1. Die Antragsteller erblicken eine Verletzung des Art. 7 B-VG insbesondere darin, dass der Rechtsschutz im PStSG im Vergleich zum Rechtsschutz nach der StPO ineffizient ausgestaltet sei (Antrag S 34, 52 f).

7.2. Der Verfassungsgerichtshof sieht es in ständiger Rechtsprechung als sachlich gerechtfertigt an, in unterschiedlichen Verfahrensbereichen unterschiedliche Ordnungssysteme vorzusehen, die deren jeweiligen Erfordernissen und Besonderheiten Rechnung tragen, sofern nur die betreffenden Verfahrensgesetze in sich gleichheitskonform gestaltet sind (vgl. zB VfSlg. 15.190/1998 mwH).

Es liegt daher grundsätzlich im rechtspolitischen Gestaltungsspielraum der Gesetzgebung, den Rechtsschutz im Bereich des polizeilichen Staatsschutzes anders auszugestalten als im Bereich des Strafprozesses. Weder bilden Regelungen aus anderen Verfahrensordnungen daher einen indirekten Maßstab für die Gleichheitskonformität der für die Ermittlungen im PStSG geltenden Regelungen noch ist dies umgekehrt der Fall; es kommt lediglich darauf an, dass die Regelungen des jeweiligen Ordnungssystems in sich sachlich sind.

7.3. Letzteres ist vorliegend der Fall: Wie oben unter Punkt III. 6.6.5. dargelegt wurde, bietet der im PStSG vorgesehene Rechtsschutz durch den Rechtsschutzbeauftragten bzw. den Rechtsschutzsenat — und dabei insbesondere die Vorabkontrolle jeder Datenermittlung sowie die begleitende Überwachung der Datenermittlung bei Erfüllung der Aufgaben gemäß § 6 Abs. 1 Z 1 und 2 PStSG — umfassende Gewähr für eine rechtmäßige Inanspruchnahme der vorgesehenen Ermittlungsbefugnisse. Umfassende Verpflichtungen zur Information der Betroffenen stellen zudem sicher, dass diese von Ermittlungsmaßnahmen Kenntnis erlangen und ihnen damit ein effektiver Zugang zum Rechtsschutz durch Erhebung einer Beschwerde bei der Datenschutzbehörde eröffnet ist. Hinsichtlich der — deutlich weniger eingriffsintensiven — Ermächtigungen zur Erfüllung einer Aufgabe nach § 6 Abs. 1 Z 3 PStSG stehen einem Betroffenen die allgemeinen Auskunfts- und Löschungsrechte gemäß §§ 26 ff DSG 2000 und die Beschwerdemöglichkeit an die Datenschutzbehörde gemäß § 5 PStSG iVm. § 90 SPG zur Verfügung. Werden die Daten in einer Datenanwendung gemäß § 12 Abs. 1 PStSG (weiter)verarbeitet, bestehen zudem die besonderen Aktualisierungs- und Löschungsverpflichtungen gemäß § 12 Abs. 2 und 3 PStSG. Zudem unterliegt die Datenanwendung selbst dann, wenn Daten zur Erfüllung der Aufgabe des § 6 Abs. 1 Z 3 PStSG verarbeitet werden, der Kontrolle des Rechtsschutzbeauftragten gemäß § 12 Abs. 6 PStSG.

7.4. Vor dem Hintergrund dieser Rechtsprechung geht auch das Vorbringen der Antragsteller, wonach die 'Staatschutzorgane' im Hinblick auf die Befugnisse nach §§ 10 und 11 PStSG 'fast alles (dürfen), was der Kriminalpolizei nach der StPO an Befugnissen zur Verfügung' stehe (Antrag S 22), ins Leere.

8. Zu den übrigen Bedenken:

8.1. Die Antragsteller behaupten eine Verletzung der Verfassungsbestimmung des § 91a Abs. 3 SPG mit der Begründung, dass die Befugnisse des Rechtsschutzbeauftragten im Hinblick auf die Aufgabe des § 6 Abs. 1 Z 3 SPG (Schutz vor verfassungsgefährdenden Angriffen aufgrund von Informationen bestimmter Stellen) im Vergleich zur bisherigen Rechtslage (§ 21 Abs. 3 SPG in der Fassung vor dem Bundesgesetz BGBl. I Nr. 5/2016) beschränkt worden seien. Es sei nämlich die bisher in § 21 Abs. 3 SPG geregelte Aufgabe der erweiterten Gefahrenerforschung einschließlich der damit verbundenen Befugnisse ins PStSG übernommen worden, wobei die Befugnisse des Rechtsschutzbeauftragten aber eine Einschränkung erfahren würden (Antrag S 29 f).

8.1.1. Die Bundesregierung weist zunächst darauf hin, dass sich das Vorbringen der Antragsteller lediglich auf die Aufgabe des § 6 Abs. 1 Z 3 PStSG (Schutz vor verfassungsgefährdenden Angriffen aufgrund von Informationen bestimmter Stellen) und nur auf die bisherigen 'Befugnisse' des Rechtsschutzbeauftragten, also offenbar auf die in § 91c SPG (in der Fassung vor dem Bundesgesetz BGBl. I Nr. 5/2016) geregelte Befassung des Rechtsschutzbeauftragten bezieht (vgl. auch § 91a Abs. 3 SPG: 'Befugnisse nach § 91c'). Nur dazu nimmt die Bundesregierung im Folgenden Stellung:

8.1.2. Die Verfassungsbestimmung des § 91a Abs. 3 SPG, wonach eine Einschränkung der Befugnisse des Rechtsschutzbeauftragten gemäß § 91c SPG im Nationalrat nur mit erhöhten Quoren beschlossen werden darf, wurde durch die SPG-Novelle 2006, BGBl. I Nr. 158/2005, erlassen und ist mit 1 Jänner 2006 in Kraft getreten. In den Erläuterungen wird dazu ausgeführt, dass 'Einschränkungen seiner Befugnisse, Rechte und Pflichten nur mit Zweidrittelmehrheit vom Nationalrat beschlossen werden können, hingegen ist die Übertragung weitergehender Kontrollbefugnisse für den verbesserten Rechtsschutz weiterhin mit einfacher Mehrheit möglich' (ErIRV 1188 BlgNR 22. GP 9). Das erhöhte Quorum bezieht sich nur auf den Bestand an Befugnissen wie sie in § 91c SPG in der Fassung der SPG-Novelle 2006 enthalten waren und nicht auch auf spätere einfachgesetzliche Erweiterungen dieser Bestimmung (Hauer/Keplinger, Sicherheitspolizeigesetz[4] [2011] § 91a SPG, Anm 4). Die Verfassungsbestimmung des § 91a Abs. 3 SPG kann überdies nicht so verstanden werden, dass die durch das erhöhte Quorum abgesicherten Befugnisse nur in einer als '§ 91c' bezeichneten Gliederungseinheit des SPG geregelt sein dürfen. Durch das erhöhte Quorum abgesichert ist lediglich der normative Inhalt dieser Bestimmung.

8.1.3. Zum Zeitpunkt des Inkrafttretens der SPG-Novelle 2006 stand § 21 Abs. 3 SPG in der Fassung des Bundesgesetzes BGBl. I Nr. 85/2000 in Kraft und sah die Aufgabe der erweiterten Gefahrenerforschung nur hinsichtlich von Gruppierungen vor. Erst durch die SPG-Novelle 2011, BGBl. I Nr. 13/2012, wurde in § 21 Abs. 3 SPG in dessen Z 1 die erweiterte Gefahrenerforschung im Hinblick auf Einzelpersonen vorgesehen; im Hinblick auf Gruppierungen wurde sie — inhaltlich unverändert — in dessen Z 2 übernommen. Durch das Bundesgesetz BGBl. I Nr. 5/2016 wurde § 21 Abs. 3 SPG aufgehoben und die Aufgabe der erweiterten Gefahrenerforschung im Hinblick auf Gruppierungen — wiederum inhaltlich unverändert — in § 6 Abs. 1 Z 1 PStSG übernommen; die erweiterte Gefahrenerforschung im

Hinblick auf Einzelpersonen wurde — mit verändertem Inhalt — als vorbeugender Schutz vor verfassungsgefährdenden Angriffen in § 6 Abs. 1 Z 2 PStSG überführt; die Aufgabe des Schutzes vor verfassungsgefährdenden Angriffen aufgrund von Informationen bestimmter Stellen wurde in § 6 Abs. 1 Z 3 PStSG neu geschaffen (ErlRV 763 BlgNR 25. GP 3 f; s. dazu oben Punkt I. 3.2.1., I. 3.2.2.1.).

§ 91c Abs. 3 SPG idF der SPG-Novelle 2006 regelte die Vorabbefassung des Rechtsschutzbeauftragten in Bezug auf die Durchführung der Aufgabe und die Ausübung von Befugnissen im Zusammenhang mit der erweiterten Gefahrenerforschung; durch die SPG-Novelle 2011 wurde diese Befugnis konkretisiert. § 91c Abs. 3 SPG wurde durch das Bundesgesetz BGBl. I Nr. 5/2016 aufgehoben und die Vorabbefassung des Rechtsschutzbeauftragten hinsichtlich der Aufgaben des § 6 Abs. 1 Z 1 und 2 PStSG (erweiterte Gefahrenerforschung im Hinblick auf Gruppierungen und vorbeugender Schutz vor verfassungsgefährdenden Angriffen) in § 14 Abs. 2 und 3 PStSG übernommen (vgl. ErlRV 763 BlgNR 25. GP 10).

8.1.4. Wie zuvor […] ausgeführt, bezieht sich das erhöhte Quorum des § 91a Abs. 3 SPG nur auf jenen Bestand an Befugnissen des Rechtsschutzbeauftragten, wie er zum Zeitpunkt des Inkrafttretens der SPG-Novelle 2006 vorgesehen war. § 91a Abs. 3 SPG bezieht sich daher nur auf die bisherigen Befugnisse des Rechtsschutzbeauftragten in Bezug auf die erweiterte Gefahrenerforschung im Hinblick auf Gruppierungen, nicht hingegen auf die — erst durch die SPG-Novelle 2011 eingeführte — erweiterte Gefahrenerforschung im Hinblick auf Einzelpersonen und schon denkmöglich nicht auf die — erst durch das PStSG eingeführte — Aufgabe des Schutzes vor verfassungsgefährdenden Angriffen aufgrund von Informationen von bestimmten Stellen.

Die Befugnisse des Rechtsschutzbeauftragten in Bezug auf die erweiterte Gefahrenerforschung im Hinblick auf Gruppierungen bestehen aber in jenem Umfang, wie sie im Zeitpunkt der SPG-Novelle 2006 bestanden haben, unverändert in § 14 Abs. 2 und 3 PStSG. Zu einer 'Einschränkung' der Befugnisse des Rechtsschutzbeauftragten iSd. § 91a Abs. 3 SPG ist es daher nicht gekommen. Das Vorbringen der Antragsteller geht daher ins Leere.

8.2. Die Antragsteller behaupten ferner, dass die in § 11 Abs. 1 Z 7 PStSG vorgesehene Befugnis zur Ermittlung von Verkehrs-, Zugangs- und Standortdaten das Fernmeldegeheimnis des Art. 10a StGG verletze (Antrag S 57 ff).

Auch dieses Vorbringen ist nicht begründet:

Das Fernmeldegeheimnis schützt die Vertraulichkeit der auf einem bestimmten Kommunikationsweg übermittelten Informationen. Die Staat soll grundsätzlich nicht die Möglichkeit haben, sich Kenntnis vom Inhalt der über Fernmeldeanlagen abgewickelten mündlichen oder schriftlichen Informations- und Gedankenaustausches zu verschaffen (vgl. Vašek/Wiederin, Art 10a StGG in Korinek/Holoubek et al [Hrsg.], Österreichisches Bundesverfassungsrecht [12. Lfg. 2016] Rz. 3).

Nach der Judikatur des Verfassungsgerichtshofes (VfSlg. 18.830/2009; 19.657/2012) sowie nach herrschender Lehre (vgl. die Nachweise bei Vašek/Wiederin, aa0 Rz. 12) gewährleistet Art. 10a StGG die Vertraulichkeit der Telekommunikation, nicht aber auch sämtlicher anderer damit in Zusammenhang stehender Daten. Art. 10a StGG schützt also den Inhalt einer im Wege der Telekommunikation weitergegebenen Information, nicht jedoch die äußeren Aspekte des Kommunikationsprozesses. Gegenstand des Fernmeldegeheimnisses sind damit zwar alle Inhaltsdaten, nicht aber der gesamte Telekommunikationsverkehr schlechthin. Die im Rahmen einer Kommunikation anfallenden Verbindungsdaten — darunter Verkehrs-, Zugangs- und Standortdaten — sind daher nicht vom Schutz des Art. 10a StGG umfasst.

Der behauptete Eingriff in das Fernmeldegeheimnis liegt daher nicht vor.

8.3. Die Antragsteller behaupten schließlich eine Verletzung des Rechts auf Kommunikationsfreiheit gemäß Art. 10 EMRK durch die 'weitreichende(n) Befugnisse zur Überwachung des Verhaltens und der Kommunikation' nach dem PStSG (Antrag S 18). Diese Bedenken sind jedoch wiederum im Wesentlichen auf eine mutmaßliche missbräuchliche Vollziehung der betroffenen Normen gestützt.

Der Vollständigkeit halber weist die Bundesregierung auf Folgendes hin:

Wie oben unter Punkt I.3.3. und III. 6.6.3.2. dargelegt, geht das PStSG von einer strikten Akzessorietät von Aufgaben nach § 6 PStSG und Ermittlungsbefugnissen aus. Nur wenn eine Aufgabe vorliegt, darf eine der Befugnisse ausgeübt werden. Damit ist sichergestellt, dass eine Ermittlung von Daten nur punktuell und anlassbezogen im Hinblick auf ein konkretes Verhalten erfolgen darf. Darin liegt auch der wesentliche Unterschied zu einer Vorratsdatenspeicherung, von der regelmäßig fast ausschließlich Personen erfasst werden, die durch eigenes Verhalten keinerlei Anlass für die Speicherung ihrer Daten gesetzt haben (vgl. dazu VfSlg. 19.892/2014).

Hinsichtlich der Verhältnismäßigkeit der im PStSG vorgesehenen anlassbezogenen Datenermittlungsbefugnisse wird im Übrigen auf die Ausführungen unter Punkt III. 6.6.3. verwiesen."

3. Auf die Äußerung der Bundesregierung hin erstatteten die Antragsteller eine Replik. 7

## IV. Erwägungen

### A. Zur Zulässigkeit des Antrages

1. Gemäß Art. 140 Abs. 1 Z 2 B-VG erkennt der Verfassungsgerichtshof über die Verfassungswidrigkeit eines Bundesgesetzes auch auf Antrag eines Drittels der Mitglieder des Nationalrates. Die einschreitenden 61 Abgeordneten verkörperten im Zeitpunkt der Antragstellung genau ein Drittel der 183 Mitglieder des Nationalrates (vgl. § 1 Abs. 1 Nationalrats-Wahlordnung 1992). Dem in Art. 140 Abs. 1 Z 2 B-VG normierten Erfordernis ist daher entsprochen. Der Umstand des späteren Ausscheidens eines oder mehrerer Antragsteller aus dem Nationalrat ändert daran nichts. Bei einem Gesetzesprüfungsverfahren, das auf Antrag eines Drittels der Mitglieder des Nationalrates durchgeführt wird, handelt es sich um ein Verfahren sui generis, in dem sich die Prüfung der Legitimation – in Abweichung von der grundsätzlichen verfahrensrechtlichen Regel, nach der es bei der Beurteilung der Prozessvoraussetzungen auf den Zeitpunkt der Entscheidung ankommt – auf den Zeitpunkt der Antragstellung zu beziehen hat (ständige Judikatur des Verfassungsgerichtshofes beginnend mit VfSlg. 8644/1979; zum Tiroler Landtag jüngst VfGH 13.10.2016, G 219/2015). 8

2. Ein von mindestens einem Drittel der Nationalratsabgeordneten gestellter Antrag ist zulässig, sobald das Gesetz rechtswirksam erlassen wurde, und zwar auch schon dann, wenn es noch nicht in Wirksamkeit getreten ist (vgl. zB VfSlg. 16.911/2003 mwN). Das Bundesgesetz, mit dem das Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz – PStSG) erlassen und das Sicherheitspolizeigesetz geändert werden, wurde am 26. Februar 2016 im Bundesgesetzblatt (BGBl. I 5/2016) kundgemacht, also erlassen. Ungeachtet des Umstandes, dass § 18 Abs. 1 PStSG und § 94 Abs. 39 erster Satz SPG das Inkrafttreten erst mit 1. Juli 2016 anordnen, ist der am 28. Juni 2016 beim Verfassungsgerichtshof eingelangte Antrag daher nicht aus diesem Grund zurückzuweisen, sind die in Rede stehenden Bestimmungen doch schon erlassen. 9

3. Der Antrag erweist sich aber aus folgenden Gründen nur teilweise als zulässig: 10

3.1. Die Grenzen der Aufhebung einer auf ihre Verfassungsmäßigkeit hin zu prüfenden Gesetzesbestimmung sind, wie der Verfassungsgerichtshof sowohl für von Amts wegen als auch für auf Antrag eingeleitete Gesetzesprüfungsverfahren schon wiederholt dargelegt hat (VfSlg. 13.965/1994 mwN, 16.542/2002, 16.911/2003), notwendig so zu ziehen, dass einerseits der verbleibende Gesetzesteil nicht einen völlig veränderten Inhalt bekommt und dass andererseits die mit der aufzuhebenden Gesetzesstelle untrennbar zusammenhängenden Bestimmungen auch erfasst werden. 11

Dieser Grundposition folgend hat der Gerichtshof die Rechtsauffassung entwickelt, dass im Gesetzesprüfungsverfahren der Anfechtungsumfang der in Prüfung gezogenen Norm bei sonstiger Unzulässigkeit des Prüfungsantrages nicht zu eng gewählt werden darf (vgl. zB VfSlg. 8155/1977, 12.235/1989, 13.915/1994, 14.131/1995, 14.498/1996, 14.890/1997, 16.212/2001). Unter dem Aspekt einer nicht trennbaren Einheit in Prüfung zu ziehender Vorschriften ergibt sich ferner, dass ein Prozesshindernis auch dann vorliegt, wenn es auf Grund der Bindung an den gestellten Antrag zu einer in der Weise isolierten Aufhebung einer Bestimmung käme, dass Schwierigkeiten bezüglich der Anwendbarkeit der im Rechtsbestand verbleibenden Vorschriften entstünden, und zwar in der Weise, dass der Wegfall der angefochtenen (Teile einer) Gesetzesbestimmung den verbleibenden Rest unverständlich oder auch unanwendbar werden ließe. Letzteres liegt dann vor, wenn nicht mehr mit Bestimmtheit beurteilt werden könnte, ob ein der verbliebenen Vorschrift zu unterstellender Fall vorliegt (VfSlg. 16.869/2003 mwN). 12

Wie der Verfassungsgerichtshof im Zusammenhang mit Anträgen nach Art. 140 Abs. 1 Z 1 lit. c B-VG sowie zu Anträgen nach Art. 140 Abs. 1 Z 1 lit. a B-VG bereits ausgesprochen hat, macht eine zu weite Fassung des Antrages diesen nicht in jedem Fall unzulässig. Soweit die unmittelbare und aktuelle Betroffenheit durch alle von einem Antrag nach Art. 140 Abs. 1 Z 1 lit. c B-VG erfassten Bestimmungen gegeben ist oder der Antrag mit solchen untrennbar zusammenhängende Bestimmungen erfasst, führt dies, ist der Antrag in der Sache begründet, im Fall der Aufhebung nur eines Teils der angefochtenen Bestimmungen im Übrigen zu seiner teilweisen Abweisung (siehe VfGH 5.3.2014, G 79/2013, V 68/2013 ua.; vgl. zu auf Art. 140 Abs. 1 Z 1 lit. a B-VG gestützten Anträgen von Gerichten, die, soweit die Präjudizialität für den gesamten Antrag gegeben ist, im Fall der Auf- 13

hebung nur eines Teils der angefochtenen Bestimmungen im übrigen Teil abzuweisen sind, VfSlg. 19.746/2013 und 19.905/2014). Umfasst ein Antrag nach Art. 140 Abs. 1 Z 1 lit. c B-VG auch Bestimmungen, die den Antragsteller nicht unmittelbar und aktuell in seiner Rechtssphäre betreffen, führt dies – wenn die angefochtenen Bestimmungen insoweit trennbar sind – im Hinblick auf diese Bestimmungen zur partiellen Zurückweisung des Antrages (VfGH 9.12.2014, G 73/2014; VfSlg. 19.942/2014; siehe auch VfSlg. 18.298/2007, 18.486/2008). Anträge von Gerichten nach Art. 140 Abs. 1 Z 1 lit. a B-VG sind nach dieser Rechtsprechung dann partiell zurückzuweisen, wenn der Antrag auch Bestimmungen umfasst, die für das antragstellende Gericht offenkundig nicht präjudiziell sind, und die angefochtenen Bestimmungen insoweit offensichtlich trennbar sind (VfSlg. 19.939/2014).

Diese Überlegungen sind auf Anträge auf abstrakte Normenkontrolle gemäß Art. 140 Abs. 1 Z 3 B-VG zu übertragen (vgl. VfSlg. 20.000/2015; VfGH 13.10.2016, G 219/2015). Soweit ein solcher Antrag die Aufhebung von Bestimmungen begehrt, gegen die im Einzelnen konkrete Bedenken in schlüssiger und überprüfbarer Weise dargelegt werden (siehe zur abstrakten Normenkontrolle VfSlg. 14.802/1997, 17.102/2004 und im Übrigen etwa VfSlg. 11.888/1988, 12.223/1989; VfGH 11.6.2012, G 120/11; VfSlg. 19.938/2014; zuletzt VfGH 2.3.2015, G 140/2014 ua.), oder mit solchen untrennbar zusammenhängende Bestimmungen erfasst, ist der Antrag daher, wenn auch die übrigen Prozessvoraussetzungen vorliegen, zulässig. 14

3.2. Gemäß § 62 Abs. 1 VfGG hat der Antrag, ein Gesetz als verfassungswidrig aufzuheben, die gegen das Gesetz sprechenden Bedenken im Einzelnen darzulegen. Die Gründe der behaupteten Verfassungswidrigkeit sind präzise zu umschreiben, die Bedenken sind schlüssig und überprüfbar darzulegen (VfSlg. 11.888/1988, 12.223/1989). Dem Antrag muss mit hinreichender Deutlichkeit entnehmbar sein, zu welcher Rechtsvorschrift die zur Aufhebung beantragte Norm in Widerspruch stehen soll und welche Gründe für diese These sprechen (VfSlg. 14.802/1997, 17.752/2006). Es ist nicht Aufgabe des Verfassungsgerichtshofes, pauschal vorgetragene Bedenken einzelnen Bestimmungen zuzuordnen und – gleichsam stellvertretend – das Vorbringen für den Antragsteller zu präzisieren (vgl. VfSlg. 17.099/2003, 17.102/2003, 19.825/2013; 19.832/2013; 19.870/2014, VfGH 24.11.2016, G 120/2016). 15

3.3. Zu den Anträgen 1. bis 5.: 16

3.3.1. Die Antragsteller beantragen mit ihrem Hauptantrag 1. sowie den in eventu gestellten Anträgen 2. bis 5. jeweils zum einen die Aufhebung des Art. 1 des Sammelgesetzes zur Gänze, zum anderen die Aufhebung einzelner Ziffern in dessen Art. 2, nämlich von Novellierungsanordnungen, die Änderungen des SPG in der Fassung der Kundmachung BGBl. I 97/2014 betreffen. Insbesondere machen sie wörtlich Folgendes geltend: 17

"Unter dem Aspekt einer 'Überwachungs-Gesamtrechnung' wiederum kann das PStSG sowie die komplementären Bestimmungen des SPG als eine jener partiellen wirkenden Maßnahmen im Sinne der Judikatur des Verfassungsgerichtshofes gelten, die in Summe bzw. im Ergebnis mit den zahlreichen, seit dem 11.9.2001 erlassenen Überwachungsnormen zu einer 'schleichenden Gesamtänderung' der österreichischen Bundesverfassung im Sinne von Art. 44 Abs. 3 B-VG, sodass das gesamte PStSG sowie die angefochtenen Normen des SPG als verfassungswidrig aufzuheben sind."

3.3.2. Was die Anfechtung des Art. 1 des Sammelgesetzes zur Gänze betrifft, so ist vorerst festzuhalten, dass die von den Antragstellern vorgebrachten Bedenken sich zwar gegen Regelungen des 2., 3. und 4. Hauptstückes des durch Art. 1 des Sammelgesetzes erlassenen PStSG richten, hingegen nicht gegen die übrigen Bestimmungen des PStSG. So werden etwa weder gegen die Organisation des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung (§§ 2, 3 und 4 PStSG) noch gegen dessen Aufgaben (und der im jeweiligen Bundesland für den Verfassungsschutz zuständigen Organisationseinheiten der Landespolizeidirektionen) im Zusammenhang mit der polizeilich staatsschutzrelevanten Beratung (§ 7 PStSG) sowie der Information verfassungsmäßiger Einrichtungen (§ 8 PStSG) noch gegen die Regelungen betreffend die Erstellung eines jährlichen Berichtes (§ 17 Abs. 1 PStSG) Bedenken vorgebracht. 18

Da sonst die verfassungsrechtlichen Bedenken in pauschaler Weise gegen das Gesetz schlechthin vorgebracht werden und es nicht Aufgabe des Verfassungsgerichtshofes ist, Bedenken, die in einem gegen ein neues Gesetz gerichteten Antrag pauschal vorgetragen werden, den jeweiligen Bestimmungen zuzuordnen, dh. gleichsam den Antrag auf das zutreffende Maß zu reduzieren, sind der Hauptantrag und die dazu gestellten Eventualanträge 2. bis 5., soweit sie sich auf 19

Art. 1 des Sammelgesetzes beziehen, zurückzuweisen (vgl. VfGH 2.3.2015, G 140/2014 ua.).

3.3.3. Darüber hinaus hält der Verfassungsgerichtshof fest, dass in den zu 1. bis 5. gestellten Anträgen ausdrücklich jeweils auch nicht die geltenden Bestimmungen des SPG, dh. das SPG idF der Novelle BGBl. I 5/2016, angefochten werden, sondern bloß die Novellierungsanordnungen des Art. 2 des Sammelgesetzes selbst. 20

3.3.3.1. Im Sinne der ständigen Rechtsprechung des Verfassungsgerichtshofes ist die Anfechtung einer Novellierungsanordnung nur zulässig, wenn sich eine Gesetzesnovelle in der Aufhebung von Bestimmungen erschöpft und gegen diese Aufhebung verfassungsrechtliche Bedenken bestehen, die behauptete Verfassungswidrigkeit auf anderem Wege also nicht beseitigt werden kann (vgl. zB VfSlg. 16.588/2002, 16.764/2002, 19.522/2011, 19.658/2012, 19.909/2014; VfGH 9.6.2016, G 56/2016). 21

3.3.3.2. Das Vorliegen einer Ausnahme iSd oben zitierten Judikatur wird von den Antragstellern nicht behauptet und ist für den Verfassungsgerichtshof auch nicht ersichtlich. Daher sind diese Anträge auch zurückzuweisen, soweit sie sich auf (Teile des) Art. 2 des Sammelgesetzes beziehen. 22

3.4. In ihrem 6. Eventualantrag, der durch das Wort "sowie" mit dem 7. Eventualantrag verbunden ist, beantragen die Antragsteller die Aufhebung einzelner Bestimmungen im PStSG sowie die Aufhebung einzelner Ziffern (Novellierungsanordnungen) in Art. 2 des Sammelgesetzes, die die Änderung des SPG betreffen. 23

3.4.1. Zum 6. Eventualantrag: 24

3.4.1.1. Mit dem Antrag zu 6.1. beantragen die Antragsteller die Aufhebung des § 4 Z 1 PStSG zur Gänze mit der – auf das Wesentliche zusammengefassten – Begründung, dass, weil das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung operative Koordinierungsstelle für Meldungen über jede Form von Angriffen auf Computersysteme von verfassungsmäßigen Einrichtungen sowie kritischen Infrastrukturen sei und es gemäß § 4 Z 5 PStSG auch als für die internationale Zusammenarbeit auf dem Gebiet des Staatsschutzes zuständige Stelle 25

genannt werde, ein Interessenkonflikt bewirkt werde. Es bestehe die Gefahr, dass das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung von einem ausländischen kooperierenden Nachrichtendienst unter Druck gesetzt werden könnte, sodass ein Anreiz bestünde, gegen Angriffe eines solchen Nachrichtendienstes nicht effektiv vorzugehen.

Damit bringen sie jedoch keine verfassungsrechtlichen Bedenken gegen die angefochtene Bestimmung vor, weshalb schon deswegen der Antrag 6.1. zurückzuweisen ist. 26

3.4.1.2. Mit den Punkten 6.2. und 6.3. beantragen die antragstellenden Abgeordneten die Aufhebung des § 6 Abs. 1 Z 1 und Z 2 PStSG zur Gänze sowie näher bezeichneter Bestimmungen bzw. Wortfolgen in den §§ 10, 11 und 12 PStSG wegen "untrennbarer Verbundenheit". 27

3.4.1.2.1. Sie begründen dies im Wesentlichen damit, dass die durch den Gesetzgeber verwendeten Begriffe, also die "äußerst unscharfen Begriffe als wesentliche Voraussetzung für den Einsatz weitgehender Eingriffsbefugnisse unter dem Deckmantel der nationalen Sicherheit und Terrorbekämpfung", "extrem anfällig für Missbrauch" seien. Die "Unklarheit, ab welcher Schwelle der Konkretisierung einer Verdachtslage die Aufgabe vorliegt" – so beispielsweise erörtert zum Begriff "vorbeugender Schutz vor verfassungsgefährdenden Angriffen durch eine Person" im bekämpften § 6 Abs. 1 Z 2 PStSG, – bewirke derart "weitgehende Eingriffe in die Grundrechte nach § 1 DSG 2000, Art. 8 und 10 EMRK", dass die "Unverhältnismäßigkeit und damit die Verfassungswidrigkeit dieser Bestimmung" einhergehe. 28

Diese Bedenken scheinen die Antragsteller auf die im § 10 Abs. 1 PStSG enthaltene Ermächtigung zur Datenermittlung, die im Einleitungssatz des § 11 Abs. 1 PStSG enthaltenen besonderen Bestimmungen zu Methoden der Datenermittlung für ebendiese Aufgaben sowie die entsprechende Ermächtigung, die für diese Zwecke erhobenen Daten weiterzugeben und zu verarbeiten (Wortfolgen in § 12 Abs. 7 PStSG), übertragen wissen zu wollen. 29

3.4.1.2.2. Die Bundesregierung bestreitet mit näherer Begründung auch die Zulässigkeit dieser Anträge. 30

3.4.1.2.3. Was die Anfechtung des § 6 Abs. 1 Z 1 und Z 2 PStSG betrifft, ist vorauszuschicken, dass nach der Judikatur des Verfassungsgerichtshofes einer Legaldefinition in der Regel keine eigenständige normative Bedeutung zukommt, denn eine solche wird vielmehr in der Regel erst im Zusammenhang mit anderen Regelungen, die diesen Begriff verwenden, bewirkt (vgl. VfSlg. 17.340/2004, 18.087/2007; VfGH 12.12.2016, G 105/2016). 31

Die antragstellenden Abgeordneten beantragen "wegen untrennbarer Verbundenheit" auch die Aufhebung diverser Regelungen, die diese Begriffe verwenden, da sie anscheinend meinen, die verfassungswidrige Unbestimmtheit der in § 6 Abs. 1 Z 1 und Z 2 PStSG verwendeten Begriffe schlage auf diese Regelungen durch. 32

Die Frage, ob über die als verfassungswidrig erachteten Bestimmungen hinaus auch alle Regelungen im 3. Hauptstück des PStSG – da aus Sicht der Antragsteller "untrennbar verbunden" – tatsächlich jeweils in einem im verfassungsrechtlichen Sinn untrennbaren Zusammenhang stehen, muss nicht hier im Rahmen der Zulässigkeit beantwortet werden; die Bedenken richten sich nämlich im Kern bloß gegen die Bestimmung des § 6 Abs. 1 Z 1 PStSG selbst, welche die Aufgabe der erweiterten Gefahrenerforschung festlegt, weshalb diese Anträge diesbezüglich zulässig sind. Allein der Umstand, dass im Falle einer erwiesenen Verfassungswidrigkeit diese Begriffe in anderen Normen weiter in Geltung stünden (sowohl in solchen, die als untrennbar verbunden im Antrag genannt werden, als auch in solchen, die im Antrag nicht genannt werden), schadet nicht. 33

Daher sind die unter Pkt. 6.2. und 6.3. des Antrages gestellten Anträge zulässig. 34

3.4.1.3. Zu § 6 Abs. 1 Z 3 PStSG (Pkt. 6.4. des Antrages) hegen die Antragsteller das Bedenken, dass die in der Bestimmung beschriebene Aufgabe keiner Genehmigung durch den Rechtsschutzbeauftragten bedürfe und die "besonderen Löschfristen" nicht anwendbar seien. Diese Bestimmungen – gemeint sind offenbar die §§ 13 ff. PStSG – fechten die Antragsteller, die darin selbst das "Hauptproblem dieser Bestimmung" erblicken, jedoch in diesem Zusammenhang nicht mit an. 35

Soweit die Antragsteller monieren, dass "die Einschränkung eines begründeten Gefahrenverdachts" fehle, bleiben sie eine nähere Begründung schuldig, inwiefern sie diese Voraussetzung für erforderlich halten und welche Verfassungsbestimmung sie durch das Fehlen verletzt sehen. 36

Daher ist dieser Antrag unzulässig. 37

3.4.1.4. Die unter Pkt. 6.5., 6.6. und 6.7. gestellten Anträge richten sich gegen die Wortfolgen "§ 274 Abs. 2 erster Fall" und "oder in § 278c StGB genannten" (jeweils § 6 Abs. 2 Z 2 PStSG) und die Zeichenfolge "124," (§ 6 Abs. 2 Z 4 PStSG) und damit auch hier ausschließlich gegen Elemente einer Legaldefinition, der – wie soeben erläutert – selbst keine eigenständige Bedeutung zukommt. Damit im Zusammenhang stehende Normen, die den Begriff des verfassungsgefährdenden Angriffs verwenden, werden hier nicht mitangefochten. Zudem wurden wesentliche Ausführungen zum – nicht angefochtenen – Einleitungssatz, mit dem erst die Präsizisierung der Definition des verfassungsgefährdenden Angriffs erfolgt, in pauschaler Weise vorgebracht. 38

Darüber hinaus hat der Verfassungsgerichtshof aber auch in ständiger Judikatur ausgesprochen, dass auch in von Amts wegen eingeleiteten Normenprüfungsverfahren der Umfang der zu prüfenden und allenfalls aufzuhebenden Bestimmungen derart abzugrenzen ist, dass einerseits nicht mehr aus dem Rechtsbestand ausgeschieden wird, als Voraussetzung für den Anlassfall ist, dass aber andererseits der verbleibende Teil keine Veränderung seiner Bedeutung erfährt; da beide Ziele gleichzeitig niemals vollständig erreicht werden können, ist in jedem Einzelfall abzuwägen, ob und inwieweit diesem oder jenem Ziel der Vorrang vor dem anderen gebührt (VfSlg. 7376/1974, 9374/1982, 11.506/1987, 15.599/1999, 16.195/2001, jüngst VfGH 27.6.2017, G 386/2016). 39

Daraus hat der Verfassungsgerichtshof gefolgert, dass die Anfechtung von einzelnen Bestandteilen einer Legaldefinition dann zulässig sein kann, wenn die Beseitigung dieser Bestandteile hinreichen würde, um die Rechtslage so weit zu bereinigen, dass die geltend gemachten Bedenken nicht mehr bestünden. Voraussetzung hiefür ist allerdings, dass einerseits weder die Legaldefinition noch die übrigen sich auf diese beziehenden Regelungen nach der hypothetischen Bereinigung der Rechtslage einen anderen Sinngehalt erhielten und der Antrag- 40

steller all diese Regelungen auch nicht für verfassungswidrig hält (vgl. VfSlg. 19.703/2012).

Dies trifft auf den vorliegenden Antrag nicht zu: Die Antragsteller erblicken die behaupteten Verfassungswidrigkeiten gerade im Zusammenspiel mit anderen Bestimmungen und Elementen der Legaldefinition etwa im Hinblick auf die Wortfolge "sofern diese ideologisch oder religiös motiviert ist" in § 6 Abs. 2 Z 2 PStSG am Ende oder auf das "mangelhafte[…] Kontroll- und Rechtsschutzsystem". Eine nähere Begründung, warum dennoch die Beseitigung der angefochtenen Wort- und Ziffernfolgen zur Bereinigung der Rechtslage ausreichend sein könnte, bleiben die Antragsteller schuldig. Insbesondere vermag der pauschale Hinweis auf zuvor "unter Punkt 6. genannte[…] verfassungsgesetzlich gewährleistete Rechte" diesen Anforderungen nicht zu entsprechen. 41

Aus diesen Gründen sind die Anträge 6.5., 6.6. und 6.7. zurückzuweisen. 42

3.4.1.5. Mit Pkt. 6.8. des Antrages wird die Aufhebung des zweiten Satzes des § 9 Abs. 1 PStSG begehrt; mit Pkt. 6.9. die Aufhebung einer Wortfolge im Abs. 1 des § 10 PStSG, der sich generell mit der Ermittlung und Weiterverarbeitung personenbezogener Daten beschäftigt, und mit Pkt. 6.10. die Aufhebung des § 10 Abs. 5 PStSG zur Gänze. 43

3.4.1.5.1. Auf das Wesentliche zusammengefasst hegen die Antragsteller das Bedenken, dass die angefochtenen Bestimmungen im Hinblick auf das Verwenden sensibler und strafrechtlich relevanter Daten lediglich den gesetzlich angeordneten Schutz wiederholten, der für personenbezogene Daten im Allgemeinen gelte. Hiedurch werde suggeriert, dass sensible Daten iSd § 4 Z 2 DSG 2000 nicht entsprechend geschützt seien. Zudem verabsäume der Gesetzgeber zu regeln, inwiefern "angemessene Vorkehrungen" iSd § 9 Abs. 1 zweiter Satz PStSG getroffen werden könnten. Auch weisen die Antragsteller darauf hin, dass "dieses Problem mit der Beseitigung der bekämpften Wortfolge auch nicht behoben wird". 44

Die Auffassung, das Vorbringen soll "auch als weiterer Beitrag zur Begründung der notwendigen Gesamtaufhebung des PStSG zu sehen" sein, vermag den 45

Anforderungen, die verfassungsrechtlichen Bedenken iSd § 62 Abs. 1 VfGG gegen die angefochtene Norm vorzubringen, nicht zu entsprechen.

Die Anträge 6.8. und 6.9. sind zurückzuweisen, da es nicht Aufgabe des Verfassungsgerichtshofes ist, gleichsam stellvertretend für die Antragsteller die im Antrag pauschal geäußerten verfassungsrechtlichen Bedenken iSd § 62 Abs. 1 VfGG zuzuordnen. 46

3.4.1.5.2. In 6.10. beantragen die antragstellenden Abgeordneten die Aufhebung des § 10 Abs. 5 PStSG zur Gänze. 47

Dies mit der Begründung, "dass auch die Sammlung und Aufbewahrung allgemein zugänglicher Quellen wie Artikel in Zeitschriften einen Eingriff in das Privatleben darstellt, soferne sie systematisch durch Behörden (Geheimdienste, Verfassungsschutz) erfolgt". Zur Ermittlung von im Internet öffentlich zugänglicher Daten und Informationen gebe es überhaupt keine Grenzen im Hinblick auf die daraus entstehende systematische Informationssammlung sowie die technischen Möglichkeiten selbst. Daraus resultiere im Hinblick auf fehlenden Rechtsschutz eine Verletzung des Art. 8 EMRK und auch des § 1 DSG 2000. 48

Da die vorgebrachten verfassungsrechtlichen Bedenken zugeordnet werden können und diese Bestimmung in keinem untrennbaren Zusammenhang mit sonstigen Bestimmungen des PStSG steht ist dieser Antrag (6.10.) zulässig. 49

3.4.1.6. Mit den Anträgen 6.11. bis 6.16. werden jeweils die Z 1 bis Z 3 und Z 5 bis Z 7 des § 11 Abs. 1 PStSG einzeln, in eventu jedoch auch § 11 PStSG zur Gänze angefochten; damit sind mit den Eventualanträgen die in den Hauptanträgen unangefochten gebliebene Einleitung sowie der letzte Satz des Abs. 1 und die Abs. 2 und 3 des § 11 PStSG ebenfalls angefochten. 50

Zu diesen Anträgen ist Folgendes festzuhalten: 51

Begründete Bedenken werden – neben allgemeinen rechtspolitischen Ausführungen – bloß zu § 11 Abs. 1 Z 2, Z 3, Z 5 und Z 7 PStSG vorgebracht. Die Bedenken betreffen – auf das Wesentliche zusammengefasst – den Umstand, dass – vor dem Hintergrund der im Einleitungssatz beschriebenen Zwecke (erweiterte 52

Gefahrenerforschung, vorbeugender Schutz vor verfassungsgefährdenden Angriffen) – Ermittlungsmethoden vom Gesetzgeber erlaubt werden, die – verglichen mit den Regelungen der StPO – unverhältnismäßig seien. Dies auch deshalb, weil das Rechtsschutzsystem im PStSG schwach ausgebildet sei. Dem Antrag ist an dieser Stelle zu entnehmen, dass die antragstellenden Abgeordneten eine Verletzung des Art. 7 B-VG, § 1 DSG 2000, Art. 8 EMRK sowie Art. 13 EMRK geltend machen.

Da die einzelnen Ziffern jeweils für sich betrachtet eine Ermächtigung zum Einsatz bestimmter Ermittlungsmethoden für die im Einleitungssatz genannten Zwecke sind, stehen sie in keinem untrennbaren Zusammenhang, weshalb der Antrag hinsichtlich der Z 2, Z 3, Z 5 und Z 7 des § 11 Abs. 1 PStSG zulässig ist. 53

Die Anträge 6.12. bis 6.14. und 6.16. sind daher zulässig. Unzulässig sind die Anträge 6.11. und 6.15. sowie – da sämtliche zuordenbare und auch sonst zulässige Bedenken sich gegen die auch in keinem konkreten Regelungszusammenhang stehenden Z 2, 3, 5 und 7 des § 11 PStSG richten – der diesbezüglich gestellte Eventualantrag auf Aufhebung des § 11 PStSG zur Gänze. 54

3.4.1.7. Schließlich wird in Pkt. 6.17. des Antrages § 12 PStSG zur Gänze und in weiteren diesbezüglichen Eventualanträgen in dessen Abs. 1 die Z 1 und Z 4 zur Gänze bzw. der letzte Satz des Abs. 1 zur Gänze angefochten. 55

3.4.1.7.1. Erst äußern die Antragsteller das Bedenken, dass "[d]urch § 12 iVm § 10 und 11 [PStSG] eine äußerst mächtige Datenbank geschaffen [wird], deren Eingriffsintensität sehr hoch ist, während ihre Kontrolle und der diesbezügliche Rechtsschutz unzureichend ausgestaltet sind". Neben einer weitschweifenden Darstellung zu technischen Möglichkeiten, die die Skepsis gegenüber der Ermächtigung zur Erstellung dieser Datenbank und – auf das verfassungsgerichtliche Verfahren übertragen – anscheinend den Hauptantrag, § 12 PStSG zur Gänze aufzuheben, zu begründen sucht, präzisieren die Antragsteller ihre Bedenken jedoch nicht hinreichend. 56

Insoweit sie § 12 Abs. 4 PStSG als zu unbestimmt erachten, bleiben sie eine nähere Begründung schuldig; vor dem Hintergrund der Formulierung in § 12 Abs. 4 PStSG "[…], soweit dies eine wesentliche Voraussetzung zur Wahrneh- 57

mung einer ihr gesetzlich übertragenen Aufgabe ist, […]" reicht es nicht aus, zu behaupten, es seien keine Kriterien für die Übermittlungsbefugnis vorhanden. Soweit die Antragsteller das Fehlen eines "effektiven Rechtsschutzes" behaupten (Abs. 1 und Abs. 6) übersehen sie, dass sie selbst ins Treffen führen, dass selbst nach einer allfälligen Beseitigung des § 12 Abs. 6 PStSG die nicht mitangefochtene Regelung des SPG, nämlich § 91c Abs. 2 SPG, sowie § 15 PStSG – gegen die sich jedoch die Bedenken im Kern richten – verblieben und damit die geltend gemachte Verfassungswidrigkeit nicht beseitigt würde.

3.4.1.7.2. Die zusammenfassende Begründung des Aufhebungsantrages, dass die "[…] gesonderte Anfechtung des § 12 […] im Rahmen der Eventualbegehren [erfolgt], wobei § 12 auf Grund der zahlreichen strukturellen Mängel zunächst zur Gänze angefochten wird", die Regelung des § 12 Abs. 1 Z 1 PStSG schon auf Grund der Unbestimmtheit des Begriffs "Gruppierung" unverhältnismäßig sei und "die Datensammlung zu Kontakt- und Begleitpersonen nach Z 4 durch die Akzessorietät im Prinzip durch dasselbe Problem Gefahr läuft, uferlos zu werden", macht zwar deutlich, dass die Antragsteller meinen, die Ermächtigungen würden in verfassungswidriger Weise Eingriffe in grundrechtlich verbürgte Garantien erlauben, doch begründen sie dies nicht hinreichend konkret. Daher sind auch diese Anträge zurückzuweisen. 58

3.4.1.8. Gleiches gilt für die unter 6.18. beantragte Aufhebung des § 15 Abs. 1 zweiter Satz PStSG. 59

3.4.2. Was die unter Pkt. 7. erneut beantragte Aufhebung der Novellierungsanordnungen des SPG betrifft, genügt es, auf die Ausführungen in Punkt 3.3.3. zu verweisen. 60

4. Zusammenfassend ist also festzustellen, dass die unter den Punkten 6.2., 6.3., 6.10., 6.12. bis 6.14. und 6.16. gestellten Anträge auf Aufhebung des § 6 Abs. 1 Z 1 und Z 2 PStSG, des § 10 Abs. 5 PStSG zur Gänze sowie des § 11 Abs. 1 Z 2, Z 3, Z 5 und Z 7 PStSG zulässig sind, im Übrigen der Antrag jedoch als unzulässig zurückzuweisen ist. 61

**B. In der Sache**

1. Der Verfassungsgerichtshof hat sich in einem auf Antrag eingeleiteten Verfahren zur Prüfung der Verfassungsmäßigkeit eines Gesetzes gemäß Art. 140 B-VG auf die Erörterung der aufgeworfenen Fragen zu beschränken (vgl. VfSlg. 12.691/1991, 13.471/1993, 14.895/1997, 16.824/2003). Er hat sohin ausschließlich zu beurteilen, ob die angefochtene Bestimmung aus den in der Begründung des Antrages dargelegten Gründen verfassungswidrig ist (VfSlg. 15.193/1998, 16.374/2001, 16.538/2002, 16.929/2003, 20.001/2015). 62

2. § 6 Abs. 1 Z 1 PStSG 63

2.1. Die dieser Bestimmung zuordenbaren Bedenken der Antragsteller richten sich zum einen gegen die Wortfolge "ideologisch oder religiös motivierter Gewalt", zum anderen gegen das Wort "Gruppierung". Beide Begriffe seien mit dem Bestimmtheitsgebot des Art. 18 B-VG nicht vereinbar, was zur Aufhebung des § 6 Abs. 1 Z 1 PStSG und weiterer damit im Zusammenhang stehender Regelungen führen müsse. 64

2.1.1. Begründend führen die Antragsteller – auf das Wesentliche zusammengefasst – aus, dass der Gesetzgeber präzisere Formulierungen als "ideologisch oder religiös motivierte Gewalt" wählen sollte, um den Anwendungsbereich des Gesetzes auf die Aktivitäten von Personen einzuschränken, die die demokratische bzw. rechtsstaatliche Ordnung gefährden würden. Bereits in der politischen Debatte während des Gesetzgebungsprozesses sei insbesondere der im Gesetzesentwurf enthaltene Begriff "weltanschaulich motivierte Gewalt" als zu unbestimmt und missbrauchsanfällig kritisiert worden; der Gesetzgeber habe daraufhin den Begriff "weltanschaulich" durch das aus dem Griechischen stammende Synonym "ideologisch" ersetzt. Dies sei "reiner Etikettenschwindel". 65

2.1.2. Hinsichtlich des Begriffs "Gruppierung" monieren die Antragsteller, dass durch das gesetzte strafbare Verhalten Einzelner eine "Mehrheit Eingriffe in ihre Freiheit hinnehmen muss, ohne einen Anlass dazu gegeben zu haben". 66

2.2. Damit sind die Antragsteller nicht im Recht: 67

2.2.1. Im Hinblick auf die Wortfolge "ideologisch oder religiös motivierter Gewalt" verkennen die Antragsteller, dass mit dieser Wortfolge lediglich ein Beispiel für Kriminalität iSd § 6 Abs. 1 Z 1 PStSG, die mit schwerer Gefahr für die öffentliche Sicherheit verbunden ist, gegeben wird. Wenn eine Gruppierung – nach Prognose durch die Behörde – zu schwerer Gefahr für die öffentliche Sicherheit durch kriminelle Akte zu werden droht, wird die Zuständigkeit der Behörde für die Abwendung dieser Gefahr als Aufgabe auf dem Gebiet des polizeilichen Staatsschutzes festgelegt. Die beispielhafte Präzisierung – um nicht zu sagen Etikettierung – der befürchteten Gewaltakte spielt nur insofern eine Rolle, als klargestellt wird, dass nicht jede Art von zu erwartenden Gewaltakten – mögen sie nun aus ideologischen oder religiösen oder anderen Gründen erfolgen – einen Gegenstand der erweiterten Gefahrenerforschung darstellt. 68

2.2.2. Auch was den Begriff "Gruppierung" anlangt, vermag der Verfassungsgerichtshof die von den Antragstellern behauptete unzureichende Bestimmtheit nicht zu erkennen, und zwar aus folgenden Gründen: 69

Als der Gesetzgeber den Begriff der Gruppierung mit BGBl. I 85/2000 in das SPG einführte, intendierte er, bisher fehlende Ermittlungsbefugnisse im Vorfeld der Bildung einer kriminellen Verbindung zu schaffen. Die Sicherheitsbehörden sollten so in die Lage versetzt werden, Organisationen zu beobachten, "wenn auf Grund bestimmter Tatsachen […] anzunehmen ist, dass […] eine ernste Gefahr eines plötzlichen Umschlagens in die Tätigkeit krimineller Verbindungen besteht" (RV 81 BlgNR 21. GP, 6). Organisationen oder Gruppierungen wie auch kriminelle Verbindungen haben gemein, dass sie – wenn auch kein hoher Organisationsgrad verlangt wird – einen gemeinsamen Zweck verfolgen. 70

Das in Art. 18 Abs. 1 B-VG verankerte Legalitätsprinzip gebietet, dass Gesetze einen Inhalt haben müssen, durch den das Verhalten der Vollziehung vorherbestimmt ist. Es ist jedoch verfassungsgesetzlich zulässig, wenn der einfache Gesetzgeber bei der Beschreibung und Formulierung dieser Kriterien unbestimmte Gesetzesbegriffe verwendet, dadurch zwangsläufig Unschärfen in Kauf nimmt und von einer exakten Determinierung des Vollziehungshandelns Abstand nimmt, falls dies im Hinblick auf den Regelungsgegenstand erforderlich ist (vgl. VfSlg. 13.785/1994; 20.032/2015, dort Pkt. IV.2.4.2.). 71

Da der Begriff "Gruppierung" einer Auslegung im Sinne der Judikatur des Verfassungsgerichtshofes zu Art. 18 B-VG (vgl. VfSlg. 13.785/1994, 20.065/2016) zugänglich ist, erweist er sich als hinreichend bestimmt. 72

3. § 6 Abs. 1 Z 2 PStSG 73

3.1. Die Antragsteller sind der Auffassung, dass aus § 6 Abs. 1 Z 2 PStSG nicht klar hervorgehe, ab welcher Schwelle der Konkretisierung einer Verdachtslage die Behörde zuständig ist, zum vorbeugenden Schutz vor verfassungsgefährdenden Angriffen durch eine Person – so ein begründeter Gefahrenverdacht besteht – Maßnahmen nach dem PStSG zu ergreifen. Problematisch sei auch, dass die "Befugnisse nach diesem Bundesgesetz bereits weit im Vorfeld einer strafbaren Handlung ausgelöst" werden würden. Diese Unklarheiten würden "weitgehende Eingriffe in die Grundrechte nach § 1 DSG 2000, Art 8 und 10 EMRK" erlauben und die Unverhältnismäßigkeit dieser Bestimmung begründen. 74

3.2. Der Verfassungsgerichtshof teilt die Auffassung der Antragsteller nicht: 75

Zwar ist den Antragstellern zuzugestehen, dass sich mit dem Begriff des "vorbeugenden Schutzes vor verfassungsgefährdenden Angriffen", der wiederum basierend auf der Legaldefinition des § 6 Abs. 2 PStSG an die Verwirklichung bestimmter Straftatbestände geknüpft ist, Aufgaben des Staatsschutzes bereits dann ergeben, wenn noch kein strafbares Verhalten gesetzt wurde. Dass der Gesetzgeber das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung oder von diesem beauftragte Sicherheitsbehörden mit Aufgaben und damit verbundenen Ermittlungsbefugnissen ausstattet, die bereits im Vorfeld strafbarer Handlungen durch Gruppierungen oder einzelne Personen eingesetzt werden können, ist aber nicht schon deshalb verfassungswidrig, weil die Straftat erst im Planungsstadium ist. Der Gesetzgeber verfolgt – wie auch bei der allgemeinen Gefahrenabwehr – zum Schutze der öffentlichen Sicherheit damit einen legitimen Zweck, nämlich bei entsprechender Verdachtslage Bedrohungen des Rechtsstaates, wie etwa durch terroristische Anschläge, schon im Vorfeld zu vereiteln. Nur so kann — wenn überhaupt — gewährleistet werden, dass nicht die Vorbereitung einer Straftat bis knapp vor deren Ausführung gediehen sein muss, um Maßnahmen setzen zu dürfen, um eben jene zu verhindern. 76

Auch muss eine Verdachtslage gemäß § 6 Abs. 1 Z 2 PStSG vorliegen, das heißt, es muss bereits ein begründeter Verdacht der Gefahr eines verfassungsgefährdenden Angriffs bei der Behörde herrschen. Dies untermauert der nicht anders zu verstehende Verweis auf § 22 Abs. 2 SPG, der ebenfalls davon ausgeht, dass – in naher Zukunft – ein verfassungsgefährdender Angriff zu erwarten ist. Auch die Gesetzesmaterialien bestätigen diese Interpretation, wenn sie zu dieser Bestimmung Folgendes ausführen: 77

"Das Erfordernis eines begründeten Gefahrenverdachts bedeutet dabei mehr als die bloße Möglichkeit oder Nichtausschließbarkeit eines Angriffes, aber weniger als mit Gewissheit zu erwarten […]." (RV 763 BlgNR 25. GP, 4)

Es trifft zwar zu, dass den mit der Vollziehung betrauten Behörden hier im Einzelfall im Rahmen der Beurteilung, ab wann sie die Befugnisse in Anspruch nehmen können, notwendigerweise ein gewisser Beurteilungsspielraum eingeräumt ist; dieser ist jedoch jeweils vor dem Hintergrund, dass Eingriffe in Grundrechte erfolgen, dahingehend auszuüben, dass die erforderlichen Eingriffe nur bei der Verwirklichung bestimmter, taxativ aufgezählter Strafrechtsdelikte unter Wahrung des Prinzips der Verhältnismäßigkeit (vgl. auch § 9 PStSG) zulässig sind. Zusammenfassend ist daher hier bloß festzuhalten, dass auch § 6 Abs. 1 Z 2 PStSG entgegen den Bedenken der Antragsteller einer Interpretation iS des Art. 18 B-VG und auch im Lichte der in § 1 DSG 2000 sowie der in Art. 8 und 10 EMRK enthaltenen Eingriffsschranken zugänglich ist. 78

4. § 10 Abs. 5 PStSG 79

4.1. Die Antragsteller hegen – auf das Wesentliche zusammengefasst – das Bedenken, § 10 Abs. 5 PStSG sei verfassungswidrig, weil er eine unverhältnismäßige Ermittlung und Weiterverarbeitung personenbezogener Daten erlaube. Zur Ermittlung von im Internet öffentlich zugänglichen Daten und Informationen gebe es überhaupt keine Grenzen im Hinblick auf die daraus entstehende systematische Informationssammlung sowie die technischen Möglichkeiten zur Ermittlung selbst. Die Unzulässigkeit der Rasterfahndung (§ 141 StPO) sei "zwar normiert, wird aber durch die weiteren Befugnisse zur Datensammlung und Zusammenführung in einem Informationsverbundsystem ad absurdum geführt". Insbesondere hochspezialisierte Suchmaschinentools ermöglichten systematisch, 80

auf Basis bestimmter Algorithmen alle im Internet zugänglichen Daten zu durchsuchen, um daraus Informationen zu gewinnen.

4.2. Die Bundesregierung hält dem entgegen, dass die Ermächtigung nach § 10 Abs. 5 PStSG – entgegen dem Anschein ihres Wortlautes – keine unbegrenzte Befugnis darstelle. Die Ausübung dieser Befugnis sei auf den durch die Rechtsordnung vorgegebenen Rahmen – und daher auch durch etwaige Geheimhaltungsregeln in anderen Vorschriften – beschränkt. Daher könnten damit auch nicht die im PStSG enthaltenen spezielleren Ermittlungsbefugnisse unterlaufen werden. § 10 Abs. 5 PStSG stelle lediglich die ausdrückliche gesetzliche Grundlage gemäß Art. 18 Abs. 1 B-VG dafür dar, dass die zur Wahrnehmung der Angelegenheiten des polizeilichen Staatsschutzes zuständigen Organisationseinheiten auch all jene Mittel der Informationsgewinnung einsetzen dürften, die privaten natürlichen und juristischen Personen im Rahmen der Rechtsordnung offen stünden. Ein automationsunterstützter Datenabgleich iSd § 141 StPO sei ausdrücklich ausgeschlossen. 81

4.3. Der Verfassungsgerichtshof teilt die gegen § 10 Abs. 5 PStSG vorgebrachten Bedenken der Antragsteller nicht: 82

Den Antragstellern ist zwar zuzugestehen, dass – ungeachtet der sich aus der Verordnung (EU) Nr. 679/2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) ergebenden staatlichen Verpflichtungen – selbst die Ermittlung und Weiterverarbeitung von öffentlich zugänglichen personenbezogenen Daten durch staatliche Stellen eine Verletzung in verfassungsgesetzlich gewährleisteten Rechten bewirken kann, und zwar jedenfalls dann, wenn diese systematisch gesammelt, katalogisiert oder mit anderen personenbezogenen Daten verknüpft werden (vgl. auch die Entscheidung des deutschen Bundesverfassungsgerichtes BVerfG 10.3.2008, 1 BvR 2388/03). Entscheidet sich die Vollziehung dazu, in systematischer Weise auch öffentlich zugängliche Quellen zu nutzen, bedarf es einer ausdrücklichen gesetzlichen Grundlage, die in verfassungsrechtlich unbedenklicher Weise dazu ermächtigt. Denn auch die Ermittlung und Weiterverarbeitung öffentlich zugänglicher personenbezogener Daten unterliegt dem verfassungsgesetzlich gewährleisteten Auskunftsanspruch gemäß § 1 Abs. 3 DSG 2000, zumal für den 83

Einzelnen mitunter kaum noch nachvollziehbar ist, welche Daten über ihn öffentlich verfügbar sind. Somit ist für den Einzelfall gewährleistet, dass derjenige, der eine ihn betreffende Maßnahme gemäß § 10 Abs. 5 PStSG vermutet, grundsätzlich davon Kenntnis erlangen kann. Dies freilich unter der Prämisse, dass der Auskunft darüber wichtige öffentliche Interessen iSd § 1 Abs. 2 DSG 2000 nicht im Wege stehen.

§ 10 Abs. 5 PStSG genügt diesen Anforderungen: 84

Vorauszuschicken ist, dass sichtlich mit Abs. 5 des § 10 PStSG die Organisationseinheiten ermächtigt werden, für Zwecke der erweiterten Gefahrenerforschung, den vorbeugenden Schutz vor verfassungsgefährdenden Angriffen im Sinne des § 10 Abs. 1 Z 1 bis Z 3 PStSG sowie zur Information verfassungsmäßiger Einrichtungen (§ 10 Abs. 1 Z 4 PStSG) über die konkret in den Abs. 2 bis 4 genannten Quellen hinausgehenden "personenbezogene Daten aus allen anderen verfügbaren Quellen durch Einsatz geeigneter Mittel, insbesondere durch Zugriff etwa auf im Internet öffentlich zugängliche Daten, zu ermitteln und weiterzuverarbeiten". 85

Wenngleich der Wortlaut eine schrankenlose Ermächtigung vorzusehen scheint, wird der vom Gesetzgeber intendierte Sinn dieser Regelung (erst) durch die Gesetzesmaterialien deutlich (RV 763 BlgNR 25. GP, 6): 86

"Abs. 5 übernimmt mit einer geringfügigen Änderung im Wortlaut die Bestimmung des § 53 Abs. 4 SPG ins PStSG. Mit dem geänderten Wortlaut wird explizit auf Ermittlungen im Internet Bedacht genommen und zwar insoweit, als es sich um die Ermittlung von im Internet öffentlich zugänglichen Daten handelt. Damit soll hinsichtlich der Terminologie eine Parallele zu den öffentlichen Orten gemäß § 27 Abs. 2 SPG hergestellt werden. Unter 'öffentlich zugänglichen Daten' sind all jene zu verstehen, die einem nicht von vornherein bestimmten Personenkreis im Internet zugänglich sind. Das bedeutet, dass von der Ermittlungsermächtigung jedenfalls die Ermittlung all jener Daten umfasst ist, die beim Surfen im Netz, in offenen Foren, Blogs oder Newsgroups jedermann zugänglich sind."

Versteht man also diese Ermächtigung in diesem engen Sinn und bedenkt man – wie die Bundesregierung in ihrer Äußerung auch selbst zugesteht –, dass bei Ausübung dieser Befugnis alle in der Rechtsordnung bestehenden rechtlichen Rahmen weiterhin zu beachten sind, so bedeutet dies, dass selbst bei öffentlich zugänglichen Daten – und nur um diese handelt es sich hier – auch die Einhaltung sämtlicher Aktualisierungs- und Löschungsverpflichtungen des § 12 Abs. 2 und 3 87

PStSG sowie des § 13 PStSG zu gewährleisten ist. Durch die Verweisung auf Abs. 2 zweiter Satz des § 10 PStSG in dessen Abs. 5 wird zudem – entgegen der Annahme der Antragsteller – ausdrücklich ein automationsunterstützter Datenabgleich iSd § 141 StPO verboten.

Bei diesem Verständnis der Ermächtigung zur rechtlich zulässigen Generierung öffentlich zugänglicher Daten bestehen keine verfassungsrechtlichen Bedenken dahingehend, dass diese unverhältnismäßig sei. 88

Nicht näher einzugehen ist hier auf die Frage, ob der Betroffene bei Verweigerung des Auskunftsanspruchs über Maßnahmen gemäß § 10 Abs. 5 PStSG rechtsstaatlichen Erfordernissen entsprechenden Rechtsschutz in Anspruch nehmen kann, da die Antragsteller insoweit keine Bedenken vorgebracht haben. 89

5. § 11 Abs. 1 Z 2 PStSG 90

5.1. Diese Bestimmung erlaubt die verdeckte Ermittlung, das ist das Einholen von Auskünften durch die Sicherheitsbehörde oder im Auftrag der Sicherheitsbehörde durch andere Personen (vgl. § 11 Abs. 1 Z 2 PStSG iVm § 54 Abs. 3 SPG), auch für die erweiterte Gefahrenerforschung und zum vorbeugenden Schutz vor verfassungsgefährdenden Angriffen nach § 6 Abs. 1 Z 1 und 2 PStSG. Der Einsatz von Privatpersonen ("Vertrauenspersonen") im Auftrag der Sicherheitsbehörden im Rahmen der verdeckten Ermittlung wurde somit – neben dem SPG – auch auf diesen Bereich erstreckt. 91

5.2. Gegen § 11 Abs. 1 Z 2 PStSG bringen die Antragsteller im Wesentlichen vor, dass die verdeckte Ermittlung gemäß § 131 StPO strengere Zulässigkeitsvoraussetzungen enthalte als die verdeckte Ermittlung gemäß § 11 Abs. 1 Z 2 PStSG, da für diese eine Ermächtigung für einen Zeitraum von sechs Monaten erteilt werden könne, jene nach der StPO hingegen auf die Dauer von drei Monaten begrenzt sei. Der "im Vergleich zur StPO erleichterte Zugang zu diesem Ermittlungsinstrument in Verbindung mit einem gleichzeitig sehr schwachen Rechtsschutzsystem" bewirke die Unverhältnismäßigkeit der Regelung, die zudem im Hinblick auf die StPO unsachlich sei. 92

5.3. Die Bundesregierung ist dagegen der Auffassung, dass Ermittlungsmaßnahmen nach den genannten Bestimmungen jeweils an die Erforderlichkeit der Maßnahme zur Erfüllung der Aufgabe gebunden seien. In beiden Fällen werde bei der Anordnung, Aufrechterhaltung und Beendigung der Maßnahme das Verhältnismäßigkeitsprinzip beachtet. Allein die gemäß § 14 Abs. 2 PStSG angeordnete zulässige Höchstdauer von sechs Monaten gegenüber der dreimonatigen zulässigen Höchstdauer gemäß § 133 Abs. 2 StPO führe daher nicht zur Unverhältnismäßigkeit der Regelung. 93

5.4. Nach der ständigen Rechtsprechung des Verfassungsgerichtshofes steht es dem Gesetzgeber im Rahmen seines rechtspolitischen Gestaltungsspielraumes grundsätzlich frei, sich in unterschiedlichen Verfahrensbereichen für eigenständige Ordnungssysteme zu entscheiden, die deren jeweiligen Erfordernissen und Besonderheiten Rechnung tragen, sofern die betreffenden Verfahrensgesetze in sich gleichheitskonform gestaltet sind (vgl. zB VfGH 14.3.2017, G 249/2016 ua. mwN). Daher widersprechen etwa unterschiedliche Sanktionensysteme in verschiedenen Verfahrensbereichen – mögen diese auch miteinander eine gewisse Verwandtschaft aufweisen – für sich allein in der Regel noch nicht dem Gleichheitsgrundsatz (VfSlg. 19.831/2013). 94

Vor diesem Hintergrund gelingt es den Antragstellern nicht, die behauptete Verfassungswidrigkeit aufzuzeigen; es liegt grundsätzlich im rechtspolitischen Gestaltungsspielraum des Gesetzgebers, auch im Bereich des vorbeugenden Schutzes vor Gefahren das Ermittlungsinstrument "verdeckte Ermittlung" vorzusehen und hier auch anders auszugestalten. Daraus ergibt sich, dass durch den Vergleich der beiden Instrumente in verschiedenen Rechtsbereichen eine Verfassungswidrigkeit nicht abgeleitet werden kann. Ungeachtet der Möglichkeit, die Ermächtigung vom Rechtsschutzsenat für die Dauer von sechs Monaten einzuholen, unterliegt die Maßnahme der verdeckten Ermittlung nach dem PStSG einer fortwährenden Überprüfung im Hinblick auf ihre Verhältnismäßigkeit. 95

Auch ist die Regelung nicht unsachlich, bedient sich der Gesetzgeber doch auch hier der dem Gesetz insgesamt innewohnenden Technik, die bei der Ausübung des eingeräumten Ermessens zu beachtenden Schranken durch Verweisungen in die Ermächtigungsnorm zu integrieren. 96

Wird also zur Gewährleistung der im Einleitungssatz genannten Ziele (erweiterte Gefahrenerforschung und vorbeugender Schutz vor verfassungsgefährdenden Angriffen) auch auf die Methode der verdeckten Ermittlung gemäß § 11 Abs. 1 Z 2 PStSG zurückgegriffen, bedeutet das, dass durch die Verweisung auf § 9 PStSG — die Erforderlichkeit vorausgesetzt — die Verhältnismäßigkeit dauerhaft gegeben sein muss, zudem das Geheimhaltungsinteresse des von der Ermittlung Betroffenen zu wahren und sicherzustellen und vor Einsatz der Methode der verdeckten Ermittlung die Ermächtigung durch den Rechtsschutzsenat einzuholen ist. 97

Dass gerade die verdeckte Ermittlung in einem demokratischen Rechtsstaat nur in ganz engen Grenzen eingesetzt werden soll, hat auch der Europäische Gerichtshof für Menschenrechte (EGMR 9.6.1998 (GK), Fall *Teixeira de Castro*, Appl. 25.829/94 und EGMR 5.2.2008, Fall *Ramanauskas*, Appl. 74.420/01) verdeutlicht. 98

6. § 11 Abs. 1 Z 3 PStSG 99

6.1. Nach Auffassung der Antragsteller fehle in § 11 Abs. 1 Z 3 PStSG im Vergleich zu § 54 Abs. 4 dritter Satz SPG eine ausdrücklich normierte Beschränkung, die eine Abgrenzung zur optischen und akustischen Überwachung von Personen gemäß § 136 StPO ("vulgo 'Späh- und Lauschangriff'") erlaube. Dass die in § 54 Abs. 4 dritter Satz SPG enthaltene Beschränkung (Unzulässigkeit des Einsatzes von Ton- und Bildaufzeichnungsgeräten, um nichtöffentliche Äußerungen aufzuzeichnen) in § 11 Abs. 1 Z 3 PStSG nicht aufgenommen worden sei, ansonsten aber auf die "Parallelbestimmung" verwiesen werde, zeige, dass der Gesetzgeber beabsichtigt habe, besagte Einschränkung im PStSG gerade nicht zu normieren. Hierin liege ein schwerer Eingriff in die Privatsphäre, wodurch § 1 DSG 2000 und Art. 8 EMRK sowie – da im Vergleich zu § 54 Abs. 4 SPG sachlich nicht gerechtfertigt – Art. 7 B-VG verletzt seien. Auch bewirke die Regelung "[d]urch den mangelhaften Rechtsschutz […] eine hohe Missbrauchsgefahr." 100

6.2. Dieser Interpretation der Antragsteller stehen die Gesetzesmaterialien zu § 11 PStSG entgegen, in denen der Wille des Gesetzgebers verdeutlicht wird. 101

Wörtlich wird dazu ausgeführt: 102

"Die Ermittlungsmaßnahmen nach den Z 1 bis 3 entsprechen den derzeit bereits im Rahmen der Aufgabenerfüllung der erweiterten Gefahrenerforschung nach § 21 Abs. 3 SPG vorgesehenen Ermächtigungen. Durch den Verweis auf die Bestimmungen des SPG soll vermieden werden, Definitionen und alle weiteren Voraussetzungen sowie Einschränkungen, die sich bereits aus dem SPG ergeben, im PStSG neuerlich zu nennen." (RV 763 BlgNR 25. GP, 6)

Angesichts dessen geht der Verfassungsgerichtshof davon aus, dass die in § 54 Abs. 4 dritter Satz SPG enthaltenen Beschränkungen dem Willen des Gesetzgebers entsprechend auch für alle Maßnahmen nach § 11 Abs. 1 Z 3 PStSG gelten. § 11 Abs. 1 Z 3 PStSG wiederholt also im Ergebnis bloß, was an sich ohnehin bereits durch § 54 Abs. 4 SPG, inklusive der Einschränkung des dritten Satzes, erlaubt ist. Mit Blick auf die Gesetzesmaterialien ist demnach davon auszugehen, dass aus bloß legistischen Gründen die ausdrückliche Normierung der Einschränkungen zu Gunsten eines pauschalen Verweises auf das SPG unterblieb. 103

Wesentlich ist hier, dass diese Ermittlungsmethoden nun nicht nur für die Abwehr gefährlicher Angriffe oder krimineller Verbindungen eingesetzt werden, sondern – unter Einhaltung aller Einschränkungen – auch für Zwecke der erweiterten Gefahrenerforschung und zum vorbeugenden Schutz vor verfassungsgefährdenden Angriffen. 104

Da schon die Prämisse der Antragsteller nicht zutrifft, tragen auch die verfassungsrechtlichen Bedenken nicht; dies trifft auch auf die dargestellte Erweiterung des Anwendungsbereiches des § 54 Abs. 4 SPG im Sinne des § 11 Abs. 1 Z 3 PStSG zu. 105

7. § 11 Abs. 1 Z 5 PStSG 106

7.1. Die Antragsteller halten – auf das Wesentliche zusammengefasst – § 11 Abs. 1 Z 5 PStSG für verfassungswidrig, weil diese Regelung in unverhältnismäßiger Weise in Art. 8 EMRK eingreife, der "den Menschen auch den Anspruch gewährt, sich auch im öffentlichen Raum grundsätzlich unbeobachtet von staatlichen Organen zu bewegen". Sie eröffne die Möglichkeit, die "systematische Beobachtung von Bürgern unangemessen auszudehnen", da der Kreis der Betroffenen insbesondere im Falle der Beobachtung einer Gruppierung "in der Praxis stark anwachsen" werde und eine Ausdehnung der Einholung von Auskünften auch auf Kontakt- oder Begleitpersonen erfolge. Durch die Erfassung der 107

Auskunftsergebnisse in einer Datenbank liege auch ein Eingriff in das Datenschutzgrundrecht des § 1 DSG 2000 vor, der insbesondere "auch aufgrund des mangelhaften Rechtsschutzes ungerechtfertigt" sei. Da die Maßnahme der Standortdatenermittlung durch den Rechtsschutzbeauftragten "laufend" genehmigt und "pro futuro immer wieder fortgesetzt" werden könne, könnten vollständige Bewegungsprofile ohne richterliche Genehmigung erstellt werden.

7.2. Die Bundesregierung sieht dagegen § 11 Abs. 1 Z 5 PStSG im Einklang mit der diesbezüglich einschlägigen Judikatur des Verfassungsgerichtshofes. Sie stellt insbesondere heraus, dass eine sichere Datenübermittlung gewährleistet sei sowie dass der Rechtsschutzbeauftragte überprüfen könne, ob für alle getätigten Abfragen tatsächlich eine Ermächtigung vorlag. 108

7.3. § 11 Abs. 1 Z 5 PStSG ermächtigt zur erweiterten Gefahrenerforschung und zum vorbeugenden Schutz vor verfassungsgefährdenden Angriffen zum Einholen von Auskünften nach §§ 53 Abs. 3a Z 1 bis Z 3 und § 53 Abs. 3b SPG zu einer Gruppierung (§ 6 Abs. 1 Z 1 PStSG) oder zu einer Person, von der "begründeter Gefahrenverdacht" eines "verfassungsgefährdenden Angriffes" auszugehen scheint (§ 6 Abs. 1 Z 2 PStSG), sowie zu deren jeweiligen "Kontakt- oder Begleitpersonen" von Telekommunikationseinrichtungen. 109

Im Erkenntnis VfSlg. 19.657/2012 prüfte der Verfassungsgerichtshof, ob die Ermächtigung der Sicherheitsbehörden, auf Basis einer bestimmten Nachricht die dazugehörige (statische oder dynamische) IP-Adresse samt deren Verwendungszeit nach § 53 Abs. 3a SPG sowie anhand einer bestimmten IP-Adresse den Namen und die Anschrift des Nutzers des Endgerätes, dem die IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, zu ermitteln, verfassungskonform ist. 110

Der Verfassungsgerichtshof hatte im Ergebnis gegen § 53 Abs. 3a SPG — ausgehend von dem Verständnis, dass keine Inhaltsdaten iSd. Art. 10a StGG ermittelt werden – keine verfassungsrechtlichen Bedenken. 111

Was den Eingriff in das verfassungsgesetzlich gewährleistete Recht auf Datenschutz gemäß § 1 DSG 2000 iVm Art. 8 EMRK betrifft, fasste der Verfassungsgerichtshof seine Beurteilung wie folgt zusammen: 112

"[…]Eine solche ausdrückliche gesetzliche Ermächtigung zur Ermittlung der IP-Adresse sowie von Namen und Anschrift des Benutzers des Endgerätes, dem eine bestimmte IP-Adresse zugeordnet ist, enthält § 53 Abs 3a Z 2 und 3 SPG. Der Eingriff ist auf die bloße Auskunftserteilung über die erfragten Daten beschränkt. Angesichts des im öffentlichen Interesse gelegenen Aufgabengebietes der Sicherheitsbehörden betreffend die Abwehr gefährlicher Angriffe, insbesondere iZm der Verhinderung der Verwirklichung unmittelbar bevorstehender Vorsatztaten nach dem StGB, dem Verbotsgesetz, dem Fremdenpolizeigesetz und dem Suchtmittelgesetz (§§ 16 Abs 2 und 3, 21 Abs 2 SPG), ist es auch nicht unverhältnismäßig, den Sicherheitsbehörden bei Vorliegen einer bestimmten Nachricht, welche die Annahme einer konkreten Gefahrensituation rechtfertigt, die Ermittlung der in Rede stehenden Daten im Wege des Betreibers oder sonstigen Diensteanbieters gemäß § 53 Abs 3a Z 2 und 3 SPG (unter den Kautelen des kommissarischen Rechtsschutzes durch den weisungsfreien Rechtsschutzbeauftragten [§§ 91c ff. SPG] sowie konkreter Löschungsverpflichtungen [§ 63 SPG] - vgl. VfSlg. 18.831/2009 [S 1137 f.]) zu ermöglichen."

Von dieser Auffassung abzugehen, besteht kein Grund. 113

Der Verfassungsgerichtshof hat in dem im Vorerkenntnis dargestellten Rahmen keine Bedenken dagegen, dass nun auch das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung und die zuständigen Organisationseinheiten der Landespolizeidirektionen zum Zwecke des polizeilichen Staatsschutzes, nämlich zur erweiterten Gefahrenerforschung und zum vorbeugenden Schutz vor verfassungsgefährdenden Angriffen nach § 6 Abs. 1 Z 1 und Z 2 PStSG, auf diese Möglichkeiten zurückgreifen, "wenn die Erfüllung der Aufgabe durch Einsatz anderer Ermittlungsmaßnahmen aussichtslos wäre". 114

Wie die Gesetzesmaterialien überdies belegen (RV 763 BlgNR 25. GP, 7), hat der Gesetzgeber jedenfalls damit weder eine permanente noch regelmäßige Erlaubnis zur Standortabfrage gegeben. 115

Damit ist ein Eingriff für Zwecke der im öffentlichen Interesse liegenden erweiterten Gefahrenerforschungund den vorbeugenden Schutz vor verfassungsgefährdenden Angriffen – wie beschrieben, beschränkt auf die punktuelle Ermittlung von Standortdaten, – notwendig iSd Art. 8 EMRK. 116

7.4. Offen bleibt — vor dem Hintergrund der Rechtsprechung des Verfassungsgerichtshofes — die Frage, ob es zulässig ist, diese Ermittlungsmethode auch auf Kontakt- oder Begleitpersonen von Gruppierungen oder Betroffenen nach § 6 117

Abs. 1 Z 1 und 2 PStSG zu erstrecken, auf die ihrerseits die Voraussetzungen zur Aufnahme von Ermittlungen nach dem PStSG nicht zutreffen; denn einen Eingriff in ihr Recht auf Datenschutz gemäß § 1 DSG 2000 und Art. 8 EMRK ermöglicht diese Bestimmung in der Tat.

Neben Gruppierungen gemäß § 6 Abs. 1 Z 1 PStSG sowie Betroffenen gemäß § 6 Abs. 1 Z 2 PStSG erstreckt sich diese Ermittlungsmethode auf Kontakt- oder Begleitpersonen, die in § 12 Abs. 1 Z 4 PStSG näher definiert sind. Demnach ist eine unmittelbare und nicht nur zufällige Verbindung ebenso erforderlich wie eine berechtigte Annahme, dass über die Kontakt- oder Begleitperson relevante Informationen zur Aufgabenerfüllung der erweiterten Gefahrenerforschung bzw. des vorbeugenden Schutzes vor verfassungsgefährdenden Angriffen beschafft werden könnten. 118

Den Gesetzesmaterialien ist außerdem zu entnehmen, dass "die Ermittler ausdrücklich angehalten [sind], den 'Status' dieser Personen möglichst rasch zu klären und ihre Daten zu löschen, wenn keine Gründe für die Annahme mehr vorliegen, dass über sie ermittlungsrelevante Informationen beschafft werden können" (RV 763 BlgNR 25. GP, 8). Damit ist klargestellt, dass das bloße Vorliegen von (flüchtigen) Kontakten keine Ermittlungsmaßnahmen gegen das gesamte Umfeld einer Gruppierung (§ 6 Abs. 1 Z 1 PStSG) oder eines Betroffenen (§ 6 Abs. 1 Z 2 PStSG) "ins Blaue hinein" rechtfertigt, um erst auf diesem Wege in Erfahrung zu bringen, ob ein engerer Zusammenhang oder Kenntnis von bestimmten Informationen besteht. 119

Vor dem Hintergrund dieser Vorgaben, der verhältnismäßig geringen Eingriffsschwere des nur punktuell zulässigen Auskunftsbegehrens, das der Ermächtigung durch den Rechtsschutzbeauftragten bedarf (§ 14 Abs. 2 PStSG), sowie des Ausschlusses weiterer Personen etwa iSd § 12 Abs. 1 Z 5 PStSG kann die von den Antragstellern befürchtete Gefahr einer systematischen Beobachtung "immer weitere[r] Kreise der Bevölkerung" so nicht angenommen werden; selbst wenn weitere Kreise betroffen sein mögen, ist mit Blick auf die Zielsetzung des polizeilichen Staatsschutzes und der relativ geringen Eingriffsintensität der punktuellen Auskunft über Standortdaten dem Gesetzgeber aus verfassungsrechtlicher Sicht noch nicht entgegenzutreten. 120

8. Gleiches gilt für § 11 Abs. 1 Z 7 PStSG: 121

8.1. Die Antragsteller erblicken in erster Linie mit näherer Begründung eine Verletzung in Art. 10a StGG, da die hier normierte Eingriffsbefugnis ohne Richtervorbehalt erfolge. Zudem gehen sie davon aus, dass bedingt durch das "mangelhafte Kontroll- und Rechtschutzsystem" ein extensiver Gebrauch dieser Befugnis möglich wäre, womit "auch § 1 DSG 2000 sowie Art. 8 EMRK für sich und in Verbindung mit Art. 13 EMRK" verletzt werden würden. Auch sei die Regelung, insbesondere im Vergleich zur StPO, sachlich nicht gerechtfertigt und verletze daher Art. 7 B-VG. 122

8.2. Demgegenüber bestreitet die Bundesregierung diese Auffassung und verweist — auf das Wesentliche zusammengefasst — neben allgemeinen Ausführungen zu den Ermittlungsvoraussetzungen auf die Entscheidungen des Verfassungsgerichtshofes VfSlg. 18.830/2009, 18.831/2009 und 19.657/2012. 123

8.3. § 11 Abs. 1 Z 7 PStSG ermächtigt im Rahmen der erweiterten Gefahrenerforschung bzw. des vorbeugenden Schutzes vor verfassungsgefährdenden Angriffen zum Einholen von Auskünften über Verkehrs-, Zugangs- und Standortdaten zu einer zu beobachtenden Gruppierung oder zu einem Gefährder. Die Bestimmung erlaubt die Ermittlung "wer, wann, mit wem, von wo aus über einen bestimmten Zeitraum" — so die Bundesregierung bestätigend – "kommuniziert hat". 124

8.3.1. Zunächst stellt sich unter dem Blickwinkel der vorgebrachten Bedenken die Frage, ob diese Daten überhaupt durch Art. 10a StGG geschützt sind. 125

Der Verfassungsgerichtshof hat zuletzt in seinem Erkenntnis VfSlg. 19.657/2012 bekräftigt, dass das Fernmeldegeheimnis Inhaltsdaten, nicht aber im Hinblick auf Verkehrsdaten den Telekommunikationsverkehr schlechthin schützt. 126

Nun ist den Antragstellern zuzugestehen, dass sich die durch § 11 Abs. 1 Z 7 PStSG eröffneten Möglichkeiten, Verkehrsdaten, und nur um solche handelt es sich hier, in einer Weise und über einen Zeitraum so zu verknüpfen, dass im Ergebnis Inhalte der Kommunikation (ermittlungstechnisch) vermutet werden können. Dennoch sind diese Daten (Telefonnummern, statische oder dynamische IP-Adressen, Zeitpunkt und Dauer der Kommunikation, die Stammdaten uä.) 127

nicht solche, die als eine von Art. 10a StGG geschützte Kommunikation zu qualifizieren sind.

Der Verfassungsgerichtshof hat dies in VfSlg. 19.657/2012 wie folgt zusammengefasst: 128

"Art. 10a StGG gewährleistet somit die Vertraulichkeit der Telekommunikation, schützt also jedenfalls den Inhalt einer auf diesem Weg weitergegebenen Nachricht, nicht aber sämtliche anderen damit zusammenhängenden Daten; Gegenstand des Fernmeldegeheimnisses sind somit alle Inhaltsdaten, nicht aber der gesamte Telekommunikationsverkehr schlechthin (vgl. auch *Wiederin*, aaO [in: Korinek/Holoubek, [Hrsg], Österreichisches Bundesverfassungsrecht, 2001, Art. 10a StGG], Rz 11)."

Von dieser Auffassung abzugehen, sieht sich der Verfassungsgerichtshof nicht veranlasst. 129

8.3.2. Hingegen greift die Bestimmung des § 11 Abs. 1 Z 7 PStSG in das verfassungsgesetzlich gewährleistete Recht auf Datenschutz gem. § 1 Abs. 1 DSG 2000 iVm Art. 8 EMRK ein, verletzt dieses jedoch nicht. 130

Nach § 1 Abs. 1 DSG 2000 hat jedermann Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit er daran ein schutzwürdiges Interesse, insbesondere im Hinblick auf die Achtung des Privat- und Familienlebens, hat. 131

Beschränkungen dieses Grundrechts sind nach dem Gesetzesvorbehalt des § 1 Abs. 2 DSG 2000 (abgesehen von lebenswichtigen Interessen des Betroffenen an der Verwendung personenbezogener Daten oder seiner Zustimmung hiezu) bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen zulässig, die aus den in Art. 8 Abs. 2 EMRK genannten Gründen notwendig sind und die ausreichend präzise, also für jedermann vorhersehbar regeln, unter welchen Voraussetzungen die Ermittlung bzw. die Verwendung personenbezogener Daten für die Wahrnehmung konkreter Verwaltungsaufgaben erlaubt ist (vgl. VfSlg. 16.369/2001, 18.146/2007, 18.963/2009, 18.975/2009). Der jeweilige Gesetzgeber muss somit nach den Vorgaben des § 1 Abs. 2 DSG 2000 eine materienspezifische Regelung in dem Sinn vorsehen, dass die Fälle zulässiger Eingriffe in das 132

Grundrecht auf Datenschutz konkretisiert und begrenzt werden (VfSlg. 18.643/2008).

Eine solche ausdrückliche gesetzliche Ermächtigung zur Ermittlung von Verkehrsdaten, Zugangs- und Standortdaten liegt hier vor. 133

Ausgehend davon, dass der Gesetzgeber damit das öffentliche Interesse verfolgt, die Allgemeinheit präventiv vor einem verfassungsgefährdenden Angriff zu schützen, und dies auf Basis einer verdichteten Gefahrenprognose durch die zuständige Behörde erst nach Befassung des Rechtsschutzsenates (§ 14 Abs. 3 PStSG) erlaubt ist, ist es nicht unsachlich, in diesen Konstellationen als ultima ratio (wenn überhaupt erforderlich) diese Ermittlungsmethode einzusetzen. 134

Da Art. 8 EMRK staatliche Überwachungsmaßnahmen auch ohne richterliche Genehmigung erlaubt (vgl. EGMR 10.2.2009, Fall *Iordachi*, Appl. 25.198/02), liegt auch diesbezüglich keine Verfassungswidrigkeit vor; ebenso ist die Erfassung von diesen technischen Daten einer Kommunikation noch kein unverhältnismäßiger Eingriff, da diese Daten – über kriminalistische Mutmaßungen hinaus – nicht geeignet sind, Rückschlüsse auf die Inhalte der Kommunikation der von der Maßnahme Betroffenen zu erlauben. 135

Insoweit kommt der Verfassungsgerichtshof auch hier zum Ergebnis, dass der Eingriff, gemessen an dem damit verfolgten öffentlichen Interesse, nicht derart schwer wiegt, dass eine Verletzung in verfassungsgesetzlich gewährleisteten Rechten vorliegt. 136

Im Ergebnis ist daher – vor dem Hintergrund der zulässig vorgebrachten Bedenken – der Antrag zur Gänze abzuweisen. 137

## V. Ergebnis

1. Der Antrag ist abzuweisen, soweit er sich gegen § 6 Abs. 1 Z 1 und Z 2, § 10 Abs. 5 sowie § 11 Abs. 1 Z 2, Z 3, Z 5 und Z 7 PStSG richtet, im Übrigen zurückzuweisen. 138

2. Diese Entscheidung konnte gemäß § 19 Abs. 4 VfGG ohne mündliche Verhandlung in nichtöffentlicher Sitzung getroffen werden. 139

Wien, am 29. November 2017
Der Präsident:
Dr. HOLZINGER

Schriftführerin:
Dr. PAVLIDIS