VERFASSUNGSGERICHTSHOF
Freyung 8
1010 Wien

Per webERV

160627/Grüne/FPÖ/ems_ct/mg

Antragsteller:

1. **Abg.z.NR Dr. Peter Pilz**
   p.A. Parlament, Grüner Klub
   1017 Wien, Dr. Karl Renner Ring 3

2. **Abg.z.NR Mag. Gernot Darmann**
   p.A. Parlament,
   Freiheitlicher Parlamentsklub - FPÖ
   1017 Wien, Dr. Karl Renner Ring 3

3. **bis 62. Antragsteller/in**
   gemäß beiliegender Unterschriftenliste

alle vertreten durch:
SCHEUCHER Rechtsanwalt GmbH
Lindengasse 39
A-1070 Wien
Code P131306

wegen:
Polizeiliches Staatsschutzgesetz – PStSG u.a.,
(BGBl. I Nr. 5/2016)

ANTRAG
gemäß Art 140 Abs.1 Z 2 B-VG
auf Gesetzesprüfung

des Bundesgesetzes 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

sowie

einzelner Bestimmungen des Bundesgesetzes über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei Sicherheitspolizeigesetz – SPG), Stammfassung BGBl. Nr. 566/1991 in der Fassung von BGBl. I Nr. 5/2016

1-fach
1 Anlage
Einzahlungsbeleg EUR 220,00

INHALTSVERZEICHNIS

1 Vollmachtsbekanntgabe, Liste der Antragsteller/innen

Eine vollständige Liste mit den Namen und den Unterschriften der 3. bis 62. Antragsteller/innen wird dem Verfassungsgerichtshof als Anlage ./A zu diesem Schriftsatz vorgelegt. Im Rubrum namentlich angeführt werden der Erst- und der Zweitantragsteller, die in ihrer Funktion als Nationalratsabgeordnete diesen Antrag organisiert und prominent öffentlich vertreten haben.

Dem Rechtsvertreter wurde von sämtlichen Antragsteller/innen Vollmacht erteilt, auf welche er sich ausdrücklich beruft.

2 Anträge im Überblick

Die Antragsteller stellen durch ihren bevollmächtigten Vertreter gemäß Art 140 Abs.1 Z 2 B-VG und §§ 62 ff VfGG die

ANTRÄGE,

der Verfassungsgerichtshof möge als verfassungswidrig aufheben

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;

(Zusammengefasst:
Das primäre Antragsbegehren geht am weitesten und fordert die vollständige Aufhebung des PStSG, wobei die mit der Novelle normierte Aufhebung der „erweiterten Gefahrenerforschung" im SPG gleichzeitig nicht rückgängig gemacht werden soll;

im SPG Aufhebung: Akteneinsichtsbeschränkung des Rechtsschutzbeauftragten (RSB); Informationsverbundsystem nach § 53a Abs. 5a SPG; verdeckte Ermittlung durch Vertrauenspersonen; Internetanalyse; in eventu zusätzlich - durch Aufhebung der Novellierungsanordnungen – das Weiterbestehen der „Information verfassungsmäßiger Einrichtungen" in § 93a SPG, falls der VfGH zur Ansicht gelangt, das bei vollständiger Aufhebung des PStSG die Aufgabe der „Information verfassungsmäßiger Einrichtungen" durch die Sicherheitsbehörden im SPG wiederherzustellen ist, damit keine (in die Verfassungssphäre reichende) Lücke entsteht und das Antragsbegehren nur deshalb abzuweisen wäre; Beseitigung untrennbar verbundener Normen)

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 1., 6., 24. und 29. näher bestimmte Wortfolgen;

(Zusammengefasst:
Eventualbegehren für den Fall, dass der VfGH den primären Antrag für überschießend hält; weitgehend wie das primäre Antragsbegehren zu 1.: Aufhebung PStSG; im SPG: Aufhebung Akteneinsichtsbeschränkung des RSB; Beibehaltung der Aufhebung der „erweiterten Gefahrenerforschung" im SPG; in eventu zusätzlich wie zum 1. Antrag durch Aufhebung der Novellierungsanordnungen das Weiterbestehen der „Information verfassungsmäßiger Einrichtungen" in § 93a SPG; Beseitigung untrennbar verbundener Normen; im Vergleich zu 1. unangefochten bleiben nach diesem Eventualbegehren: Informationsverbundsystem nach § 53a Abs.5a SPG; verdeckte Ermittlung durch Vertrauenspersonen; Internetanalyse;)

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 1, zur Gänze;**

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

(Zusammengefasst:
Eventualbegehren für den Fall, dass der VfGH die vorhergehenden Anträge zu 1. und 2. für überschießend hält, insbesondere weil die „erweiterte Gefahrenerforschung" nach diesen Anträgen ersatzlos entfallen würde; Aufhebung PStSG; im SPG: Aufhebung Akteneinsichtsbeschränkung RSB; Aufhebung von Novellierungsanordnungen mit den Ergebnissen: Weiterbestehen der „Information verfassungsmäßiger Einrichtungen" in § 93a SPG; Weiterbestehen der „erweiterten Gefahrenerforschung" im SPG; Beseitigung untrennbar verbundener Normen;

das Eventualbegehren zu 3. erscheint auf den ersten Blick weiter als die Anträge zu 1. und 2., weil es einer Anfechtung der positiven Novellierungsanordnungen zum SPG bedarf, um die – mit dem PStSG einhergehende – Aufhebung der „erweiterten Gefahrenerforschung" nach dem alten § 21 Abs.3 SPG rückgängig zu machen.)

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;

(Zusammengefasst:
Eventualbegehren für den Fall, dass der VfGH zur Ansicht gelangt, dass durch die Aufhebung des PStSG der verfassungskonforme Zustand hergestellt wird, ohne dass es einer Anfechtung von Bestimmungen aus der begleitenden SPG Novellierung bedarf; Beseitigung untrennbar verbundener Normen)

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**;

(Zusammengefasst:
Eventualbegehren für den Fall, dass der VfGH zur Ansicht gelangt, dass der verfassungskonforme Zustand nur durch Aufhebung des PStSG und der gesamten begleitenden SPG Novellierung hergestellt wird; Bestimmungen, die durch die Novelle verdrängt wurden, treten wieder in Kraft).

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 (§ 6 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 die 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 § 162 StPO."**;

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. 5a in der Fassung BGBl. I Nr. 5/2016 auch im Informationsverbundsystem geführt**";

alle wegen Verletzung des Rechtsstaatsprinzips, des § 1 DSG 2000 sowie der Artikel 8, 10 und 13 EMRK sowie Art 7 B-VG.

3 Ausführungen zur Antragslegitimation und Zulässigkeit

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 26.02.2016 im Bundesgesetzblatt, Teil I, als Nr. 5/2016 kundgemacht.

Gemäß Art 140 Abs.1 Z 2 B-VG erkennt der Verfassungsgerichtshof über die Verfassungswidrigkeit von Bundesgesetzen (auch) auf Antrag eines Drittels der Mitglieder des Nationalrates.

Ein Drittel der Mitglieder des Nationalrates ist nach dieser Verfassungsbestimmung antragslegitimiert, die Überprüfung eines Bundesgesetzes auf seine Verfassungskonformität durch den Verfassungsgerichtshof zu verlangen.

Der gegenständliche Antrag ist von sämtlichen 24 Nationalratsabgeordneten der Partei „Die Grünen“ sowie von den 38 Nationalratsabgeordneten der „Freiheitlichen Partei Österreichs“ unterzeichnet. Gemeinsam haben sohin 62 Mitglieder des Nationalrates diesen Antrag unterschrieben.

Der österreichische Nationalrat hat 183 Abgeordnete. Das von Artikel 140 Abs. 1 Z 2 B-VG geforderte Quorum ergibt sohin eine Antragslegitimation von zumindest 61 Mitgliedern des Nationalrates.

Das angefochtene Bundesgesetz tritt zwar erst am 01.07.2016 in Kraft. Nach der der Bestimmung von Art 140 Abs. 1 Z 2 B-VG immanenten Logik soll einer qualifizierten Minderheit des Nationalrates die Möglichkeit zukommen, die Überprüfung eines Bundesgesetzes auf seine Verfassungskonformität durch den Verfassungsgerichtshof zu verlangen. Dabei muss irrelevant sein, ob das Gesetz bereits in Kraft ist.

Der Antrag ist sohin zulässig.

4 Vorbemerkung

Die antragstellenden Abgeordneten sind besorgt über das Desinteresse der Regierungsparteien an den von den Oppositionsparteien und verschiedensten Organisationen der Zivilgesellschaft vorgebrachten verfassungsrechtlichen Bedenken gegen das „Polizeiliche Staatsschutzgesetz". Dieses Gesetz, das polizeistaatliche Tendenzen aufweist, wurde in übertriebener Hektik – in direkter Reaktion auf die schrecklichen Anschläge von Paris im November 2015 – am 27. Jänner 2016 im Nationalrat gegen die Stimmen der Oppositionsparteien beschlossen. Die Abgeordneten des Freiheitlichen Parlamentsklubs und des Grünen Klubs im Parlament sehen sich verpflichtet, in einem gemeinsamen Antrag die rechtsstaatlichen und grundrechtlichen Bedenken dem hohen Verfassungsgerichtshof zur Klärung vorzulegen.

Schon Hans Kelsen sah es klar:

> „Und die Geschichte zeigt, dass die demokratische Staatsgewalt nicht weniger zur Expansion neigt als die autokratische".[1]

Österreich befindet sich legistisch im Übergang weg von einer Strafrechtgesetzgebung hin zu einer „Bekämpfungsgesetzgebung", die Terroristen, Mitglieder der internationalen organisierten Kriminalität, Extremisten und Radikale aller Schattierungen schon im Vorfeld erkennen und ausschalten soll. Da diese Gefahrenabwehr in den Vordergrund der Sicherheits- und Justizpolitik rückt, wurde im Strafrecht die Strafbarkeit in vielen Bereichen bereits weit in das „Vorfeld" des eigentlich bekämpften strafbaren Verhaltens verlagert. Im Polizeirecht wiederum soll eine umfassende Überwachung möglichst Vieler – im polizeilichen Optimum wohl der gesamten Bevölkerung – ganz allgemein Sicherheit und im Besonderen den Schutz des Staates gewährleisten.

Am 08.04.2014 hob der EuGH die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung (VDS-RL), zur Gänze auf, weil die verdachtsunabhängige und anlasslose Überwachung der gesamten Bevölkerung gegen EU-Grundrechte verstieß. Der EuGH erkennt in seiner Urteilsbegründung zwar ausdrücklich an, dass nach Art 6 der Europäischen Grundrechtecharta jeder Mensch nicht nur das Recht auf Freiheit, sondern auch auf Sicherheit hat[2]. Allerdings führt der Gerichtshof weder in dieser noch einer anderen Entscheidung weiter aus, welchen substantiellen Gehalt das individuell garantierte „Recht auf Sicherheit" nach Art 6 EU Grundrechte-Charta hat.

Der österreichische Verfassungsgerichtshof (VfGH) folgte in seinem Erkenntnis vom 27.06.2014 dem EuGH in Sachen Vorratsdatenspeicherung und hob auch die innerstaatliche Umsetzung der VDS-RL als verfassungswidrig auf. In seiner Urteilsbegründung[3] fand der VfGH zum Spannungsfeld Sicherheit und Freiheit klare Worte:

---

[1] *Kelsen*, Vom Wesen und Wert der Demokratie, 2. Auflage (1929), Seite 11.

[2] Urteil des EuGH In den verbundenen Rechtssachen C-293/12 und C-594/12, RN 42.

[3] unter Verweis auf *Berka*, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT, 2012, Band I/1, 22

> „Ausgangspunkt der Beurteilung der Verhältnismäßigkeit der Vorratsdatenspeicherung ist die Einsicht, dass das Grundrecht auf Datenschutz in einer demokratischen Gesellschaft – in der hier bedeutsamen Schutzrichtung – auf die Ermöglichung und Sicherung vertraulicher Kommunikation zwischen den Menschen gerichtet ist. Der Einzelne und seine freie Persönlichkeitsentfaltung sind nicht nur auf die öffentliche, sondern auch auf die vertrauliche Kommunikation in der Gemeinschaft angewiesen; **die Freiheit als Anspruch des Individuums und als Zustand einer Gesellschaft** wird bestimmt von der Qualität der Informationsbeziehungen (….).“[4]

Natürlich anerkennen die Antragsteller/innen, dass sowohl das Individuum als auch die Gemeinschaft unter bestimmten Umständen einen Anspruch darauf hat, durch staatliche Organe vor spezifischen Bedrohungen geschützt zu werden. Dieser Anspruch erwächst in der Form von positiven Schutz- und Gewährleistungspflichten im Hinblick auf alle garantierten Grundrechte, etwas das Recht auf Leben[5], das Verbot der Folter, das Recht auf Meinungsfreiheit, das Recht auf Privatsphäre und viele mehr. Daher ist es letztlich ein Ausfluss dieser staatlichen Schutzpflichten, dass ein System der Strafverfolgung und der Sicherheitspolizei zur Prävention sowie zur Aufklärung von Straftaten eingerichtet wird.

Insofern ist die tägliche Arbeit der Strafverfolgungs- und Sicherheitsbehörden eben nicht nur als Eingriff in Grundrechte, sondern zugleich als stetiger (proaktiver und reaktiver) Schutz von Grundrechten zu verstehen. Die Herausforderung für das System ist dabei, die Balance nicht zu verlieren und rechtsstaatliche Grundprinzipien einzuhalten. Grundrechtseingriffe müssen immer in einem angemessenen Verhältnis zu den legitimen Zwecken stehen. Das Rechtsstaatsprinzip und der Grundsatz der Verhältnismäßigkeit dürfen nicht zur leeren Formel verkommen. Der Gesetzgeber muss abstrakt vorzeichnen, wo die Pole einer Abwägungsentscheidung liegen und nach welchen Kriterien diese konkretisiert werden soll. Das System muss strukturelle Schutzvorkehrungen vorsehen, damit die Verhältnismäßigkeit auch im Einzelfall möglichst gewahrt bleibt.

Das PStSG gewährt den „Staatschutzbehörden“ (in Kombination mit den Bestimmungen des SPG) umfassende Eingriffsbefugnisse, die im Regelfall ohne Differenzierung zur Verfügung stehen, sobald die Zuständigkeit dieser Behörden begründet ist. Mit anderen Worten entspricht die Abwägungsgrenze für tiefgehende Befugnisse zur verdeckten Überwachung und Ermittlung weitestgehend der Zuständigkeitsgrenze. Effektive Rechtsschutzmöglichkeiten für die Betroffenen fehlen fast völlig.

Gibt es aber keinen effektiven Rechtsschutz gegen Grundrechtseingriffe von hoher Intensität, können Ermittlungen auf Rechtsgrundlage des PStSG (und des SPG) gleichzeitig unkontrollierbar – wie bei einem Stein, den man ins Wasser wirft – immer weitere Kreise ziehen, ist die Rechtsstaatlichkeit und der Rechtsstaat am Ende. Dann wird aus dem Rechtsstaat ein „Feindrechtsstaat“, ein Polizeistaat – nicht von heute auf morgen, aber heimlich, leise und nachhaltig.

---

[4] VfGH 27.6.2014, G 47/2012-49 u.a., Rz 167

[5] Urteil des EGMR vom 31.5.2007 im Fall Kontrová gg. die Slowakei (NL 2007, 133).

5 Gesetze und verwendete Abkürzungen

Dieser Antrag nimmt Bezug auf Bestimmungen nachstehender Gesetze:

PStSG: Polizeiliches Staatschutzgesetz, BGBl. I Nr. 5/2016

SPG: Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei, Stammfassung BGBl. Nr. 566/1991 in der Fassung von BGBl. I Nr. 5/2016

StPO: Strafprozessordnung 1975, Stammfassung BGBl. Nr. 631/1975 in der Fassung BGBl. I Nr. 26/2016

StGB: Strafgesetzbuch, Stammfassung BGBl. Nr. 60/1974 in der Fassung BGBl. I Nr. 154/2015

DSG 2000: Bundesgesetz über den Schutz personenbezogener Daten, Stammfassung BGBl. I 165/1999 in der Fassung von BGBl. I Nr. 83/2013

EMRK: Europäische Menschenrechtskonvention, Stammfassung BGBl. Nr. 210/1958 in der Fassung von BGBl. III Nr. 47/2010

BVT: Bundesamt für Verfassungsschutz und Terrorismusbekämpfung

6 Darlegung der Bedenken

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,

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 deutschen nationalen Umsetzung der Vorratsdatenspeicherung 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.[6] Damit beschreibt das dt. Bundesverfassungsgericht im Prinzip die Notwendigkeit einer Art „Überwachungs-Gesamtrechnung“[7].

§ 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.

---

[6] BVerfG, 1 BvR 256/08 u.a. vom 2.3.2010 (FN 64), Rz 218.

[7] In diesem Sinne ist das AKVorrat-Projekt „HEAT“ (Handlungskatalog zur Evaluierung der Anti-Terror Gesetze in Österreich) zu sehen, welches zur Hälfte von der Internet Privatstiftung Austria (IPA) im Rahmen der „NetIdee“-Förderung finanziert wird und in diesem Zusammenhang Ende 2014 auch den „Privacy Award“ gewonnen hat. Das Ergebnis des Projekts ist eine Handlungsanleitung, gewissermaßen ein „Pflichtenheft“ zur Evaluierung bestehender wie auch neu vorgeschlagener Gesetze, die Überwachungsbefugnisse mit dem Ziel der Bekämpfung organisierter Kriminalität oder von Terrorismus normieren. Das Projekt HEAT wird im Sommer 2016 fertig gestellt, das Endprodukt wird einen Vorschlag für die Objekte einer notwendigen Evaluierung im Sinne der „Überwachungsgesamtrechnung“, Vorschläge zu den Methoden, Zielsetzungen, Handlungsalternativen der Politik und vor allem Vorschläge für die Kriterien enthalten, nach denen eine Evaluierung vorzunehmen ist. Gefolgt wird dabei im Wesentlichen den Vorgaben des Bundeskanzleramts für alle legistischen Projekte in ‚Österreichisches Handbuch „Bessere Rechtsetzung“, Bundeskanzleramt (Hrsg.), *Hable, Kunnert, Pürgy*, Wien 2008‘. Die „wirkungsorientierte Folgenabschätzung“ zum PStSG ist zweifellos nicht auf Basis der systematischen Vorgaben des Bundeskanzleramts entstanden.

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[8] 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."[9]

Schon kurz zuvor hat der EGMR in der Rechtssache Roman Zakharov v. Russland[10] 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."[11]

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.[12] 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.

---

[8] EGMR Szabó und Vissy v. Ungarn, Urteil 12.1.2016, Bsw. Nr. 37138/14.

[9] EGMR Szabó und Vissy v. Ungarn, Rn 57.

[10] EGMR Roman Zakharov v. Russland, Urteil (große Kammer) 4.12.2015, Bsw. Nr. 47143/06.

[11] EGMR Roman Zakharov v. Russland, Rn 260.

[12] EGMR Association for European Integration and Human Rights und Ekimdzhiev v. Bulgarien, Urteil 28.06.2007, Bsw. Nr. 62540/00, Rn 76, mit weiteren Rechtsprechungshinweisen.

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 betroffenen Personenkreises und das schwache Kontroll- und Rechtsschutzsystem entsteht daraus eine latent drohende 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 selbst 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[13] erkannt, dass bereits eine einschüchternde Wirkung einen Eingriff in das Grundrecht bewirken kann. Der Eingriff in die Meinungs- und Informationsfreiheit 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.

---

[13] EGMR, Rotaru v. Rumänien, Urteil 4.5.2000, Bsw. Nr. 28341/95.

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 Gegentyp, 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.[14] Im Hinblick auf das Missbrauchsrisiko, dass 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.[15]

---

[14] EGMR Association for European Integration and Human Rights und Ekimdzhiev v. Bulgarien, Urteil 28.06.2007, Bsw. Nr. 62540/00, Rn 74-75, mit weiteren Rechtsprechungshinweisen.

[15] Ibid.

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.[16] 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“.[17]

Das Gebot des effektiven Rechtsschutzes blieb die zentrale Konstante in der Rechtsstaatsjudikatur des VfGH[18].

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

---

[16] VfSlg 1804/1949. Der VfGH vertrat die Ansicht, dass das AVG in der Wahrung des Parteiengehörs „*in verfahrensrechtlicher Beziehung eine der wichtigsten Sicherungen des rechtsstaatlichen Prinzips*“ erblicke.

[17] VfSlg 2455/1952.

[18] Vgl. *Hiesel*, Die Rechtsstaatsjudikatur des Verfassungsgerichtshofes, ÖJZ 1999,522 (Heft 14-15).

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 Überblick sogleich) auf 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[19] 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. Ähnlich einem ins Wasser geworfenen Stein kann das PStSG Kreise ziehen, die sich später kaum kontrollieren lassen.

Die Organisationseinheiten nach § 1 Abs. 3 PStSG, im Folgenden als „Staatschutzorgane" 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 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.

---

19 Verein gegen Tierfabriken.

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 dermaßen viele, nämlich sämtliche tragenden Bestimmungen des PStSG als verfassungswidrig wegen Verletzung des Rechtsstaatsprinzips, dass 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 Wortfolge 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 wiederhergestellt werden durch Aufhebung des gesamten PStSG wegen Verfassungswidrigkeit schon seines Konzeptes bzw. 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 – ähnlich wie einem Stein, der ins Wasser geworfen wird und dort immer weitere Kreise zieht – 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.)"[20]

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).

[20] VfGH 29.09.1988, G 72/88, G 102/88, u.a., VfSlg 11.829.

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 um die Ausgestaltung seiner Befugnisse, seiner Organisation und seiner Ausstattung.

Die Geltendmachung von Rechtsschutzmängeln ist im abstrakten Normenkontrollverfahren vor dem Verfassungsgerichtshof eine besondere Herausforderung, wenn es darum geht, den Sitz der Verfassungswidrigkeit zu bestimmen. Typischerweise ist im Zusammenhang mit Rechtsschutz- und Kontrollaufgaben eine mangelhafte Norm für den Grundrechtsschutz noch immer 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 weiter 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 beantragten – 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:

§ 91d Abs.1 letzter Satz SPG idF BGBl. I Nr. 97/2014: „Dies gilt jedoch nicht für Auskünfte und Unterlagen über die Identität von Personen oder über Quellen, deren Bekannt werden die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde, und für Abschriften (Ablichtungen), wenn das Bekannt werden der Information die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde".

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".

„**§ 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**."

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 praktisch 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 Konteneinschau 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) dar, das nicht nur die Vollziehung sondern auch den Gesetzgeber bindet.

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 Handlungen 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[21] 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. 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 vom 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.

---

[21] Die nach § 91a SPG geforderten Quoren sind formaler Natur und begründen damit kein materielles verfassungsgesetzlich gewährleistetes Recht.

Daran ändert auch weder der Umstand etwas, 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. 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 „Rechtsschutzsenat" (§ 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 allem 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 immer Glauben zu schenken und die tatsächlich vorgelegten Meldungen 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 Antragssteller/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.[22]

Diese Bindung des Gesetzgebers an das Sachlichkeitsgebot gilt auch für die Bestimmungen zu den Befugnissen des Rechtsschutzbeauftragten gemäß PStSG und der 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[23] 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.

---

[22] Vgl. dazu z.B. VfSlg 10.492, 13.178, 17.143.

[23] entgegen den grundsätzlichen Vorgaben des VfGH bereits in VfSlg 11.196/1986.

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. Die Verletzungen des aus **Art 18 B-VG** abgeleiteten Rechtsstaatsprinzips durch die angefochtenen Normen ist augenfällig.

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.[24]

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

---

[24] Vgl. zu dieser Problematik und ihrer Grundrechtsrelevanz insb. VfGH 27.6.2014, G 47/2012-49 u.a., Rz 167.

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.

7 Zur Anfechtung einzelner Normen („Besonderer Teil“)

7.1 Mangelnde Bestimmtheit im Einzelnen

Der Verfassungsgerichtshof hat das Problem der Normenklarheit mehrfach eindeutig und durchaus pointiert zum Ausdruck gebracht (zB VfGH vom 4.12.2001, VfSlg 16.381):

> „Im Erkenntnis VfSlg. 3130/1956 hat der Verfassungsgerichtshof aus dem rechtsstaatlichen Gedanken der Publizität des Gesetzesinhaltes die Schlussfolgerung gezogen, dass der Gesetzgeber der breiten Öffentlichkeit den Inhalt seines Gesetzesbeschlusses in klarer und erschöpfender Weise zur Kenntnis bringen muss, da anderenfalls der Normunterworfene nicht die Möglichkeit hat, sich der Norm gemäß zu verhalten. Diesem Erfordernis entspricht weder eine Vorschrift, zu deren Sinnermittlung qualifizierte juristische Befähigung und Erfahrung sowie geradezu archivarischer Fleiß vonnöten ist (vgl. VfSlg. 3130/1956), noch eine solche zu deren Verständnis subtile verfassungsrechtliche Kenntnisse, außerordentliche methodische Fähigkeiten und eine gewisse Lust zum Lösen von Denksport-Aufgaben erforderlich ist (VfSlg. 12420/1990[25])“.

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)

„§ 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;“

Verbundene Normen: § 10 Abs. 1 Z 1; § 11 Abs. 1; § 12 Abs. 7;

Die „Erweiterte Gefahrenerforschung“ hat nicht erst mit dem PStSG Eingang in die Rechtsordnung gefunden, sondern war schon bisher in § 21 Abs.3 SPG normiert, der mit der Einführung des PStSG zugleich aufgehoben wird (siehe BGBl. I Nr. 5/2016, Artikel 2, Ziffer. 6). Die hier vorgebrachten verfassungsrechtlichen Bedenken beziehen sich also schon auf die geltende Rechtslage vor Inkrafttreten des PStSG. Für den Fall einer Gesamtaufhebung des PStSG wird daher bewusst die mit dem Beschluss des PStSG einhergehende Aufhebung aller Bestimmungen zur „Erweiterten Gefahrenerforschung“ im SPG nicht angefochten. Die in diesem Antrag argumentierte Verfassungswidrigkeit wäre nämlich nicht beseitigt, wenn die alte ähnliche Bestimmung des 21 Abs. 3 SPG wieder in Kraft treten würde.

[25] Anmerkung der Verfasser: sog. „Denksport-Erkenntnis“ des VfGH vom 29.06.1990.

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 ihre Ideen, Erkenntnisse, Kategorien und Wertvorstellungen, somit ihrer „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 zweckdienlichen 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, in dem er durch den synonymen griechischen Begriff mit der gleichen Bedeutung ersetzt wird, ist ein reiner Etikettenschwindel, der die Kritik geradezu verhöhnt.

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 Formulierungen 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 völlig 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, aber dadurch wird nicht automatisch die Organisation selbst 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)

„der vorbeugende Schutz vor verfassungsgefährdenden Angriffen durch eine Person, sofern ein begründeter Gefahrenverdacht für einen solchen Angriff besteht (§ 22 Abs.2 SPG);"

Verbundene Normen: § 10 Abs.1 Z 2; § 11 Abs.1; § 12 Abs.7;

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.[26]

Nach dem Gesetzeswortlaut beginnt der Einsatzbereich, wenn ein begründeter Gefahrenverdacht für einen verfassungsgefährdenden 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.

---

26 Vgl. *Heißl*, PStSG Polizeiliches Staatsschutzgesetz, Erweiterte Gefahrenerforschung § 6, Rn 16 ff, Manz 2016, 35 f.

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)

„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."

Bei dieser Bestimmung fehlt die Einschränkung eines **begründeten** Gefahrenverdachts, es bedarf also offensichtlich keiner konkreten Bedrohungssituation mehr (ganz abgesehen von einer konkreten Rechtsgutbeeinträchtigung).[27] 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.

---

27 *Heißl*, aaO, Rn 30, 38.

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

(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).

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" Verweisungstechnik 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 zuständige wäre. Durch die Formulierung der „in § 278c 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 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, das tatsächlich die öffentliche Sicherheit in einer verfassungsgefährdenden Weise dadurch 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 subsummiert 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 StBG 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[28] 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 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 bestimmte Länder 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.

[28] Das ist nach § 283 Abs. 1 Z 1 StGB eine „Kirche oder Religionsgesellschaft oder eine andere nach den vorhandenen oder fehlenden Kriterien der Rasse, der Hautfarbe, der Sprache, der Religion oder Weltanschauung, der Staatsangehörigkeit, der Abstammung oder nationalen oder ethnischen Herkunft, des Geschlechts, einer körperlichen oder geistigen Behinderung, des Alters oder der sexuellen Ausrichtung definierte Gruppe von Personen oder (…) ein Mitglied einer solchen Gruppe".

Auch bei den „Cybercrime“ Strafatbeständen 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, für den Bereich der erweiterten Gefahrenerforschung, ist die Ausdehnung der Ermittlungsbefugnisse nach dem PStSG zu solchen Sachverhalten 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, existiert zu § 6 Abs. 2 Z 5 PStSG nicht. Demgegenüber besteht kein effektives Kontroll- und Rechtsschutzsystem, das einer willkürlichen Rechtsanwendung systematisch entgegenstehen könnte.

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 fällt.

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)

„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."

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 gestellt werden.

Ein besonderes Gefährdungspotential für die Demokratie besteht vor allem 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 „rechtswidrige 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)

„§ 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."

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**"[29] erlaubt. Das heißt im 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.

---

29 Im ersten zur Begutachtung ausgesendeten Ministerialentwurf zum PStSG lautete diese Zweckbestimmung, damals noch als § 11 PStSG: „zum Zweck der Bewertung der Wahrscheinlichkeit einer Gefährdung sowie zum Erkennen von Zusammenhängen und Strukturen mittels operativer oder strategischer Analyse". Inwiefern die geänderte und nun normierte Formulierung einen substanziellen Unterschied bewirkt, ist fragwürdig.

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[30] 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 hochspezialisierte Suchmaschinen-tools, die speziell auf nachrichtendienstliche und/oder polizeiliche Ermittlungsfragen 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.

---

[30] ZB auch der damals verbreitetste Dienst, gewissermaßen als Pionier, die Suchmaschine „Altavista".

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 deutlich potenziert.

Logisch definieren lässt sich die Rasterfahndung als Schnittmengenbildung nach Merkmalen von Daten aus verschiedenen Quellen. Typischerweise besteht dabei Vollzugriff auf die jeweiligen Datenbanken und 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.[31] 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)

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**

[31] EGMR Urteil Segerstedt-Wiberg u.a. v. Schweden, Nr. 62332/00, 06.06.2006, § 72.

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.

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“[32] 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 höchsten 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:

[32] Ein „IMSI-Catcher“ ist ein technisches Gerät, das gegenüber dem Mobiltelefon als Sender auftritt und durch sein stärkeres Signal den echten Sender überlagert. Gleichzeitig gibt sich der IMSI-Catcher gegenüber dem Sender als Endgerät aus. Damit wird der IMSI-Catcher zum Relais, über das die gesamte Kommunikation läuft und diese daher mithören/mitschneiden kann. Es handelt sich um eine klassische sog. „Man in the Middle“ Attacke. Zusätzlich vermag der IMSI Catcher durch Vermessung der Signalvektoren, mit einer relativ hohen Genauigkeit von einigen Metern den Standort der Endeinrichtung zu bestimmen. Rechtlich zulässig ist der Einsatz des IMSI-Catchers nur im Hinblick auf die zuletzt genannte Funktion.

§ 11 PStSG – Besondere Bestimmungen für die Ermittlungen	**§ 54 SPG – Besondere Bestimmungen für die Ermittlung**
§ 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 (…) *3. Einsatz von Bild- und Tonaufzeichnungsgeräten (§ 54 Abs. 4 SPG); dieser darf verdeckt erfolgen, wenn die Erfüllung der Aufgabe ansonsten aussichtslos wäre;*	*§ 54 (4) Die Ermittlung 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* 1. *mit Tonaufzeichnungsgeräten, um nichtöffentliche und nicht in Anwesenheit eines Ermittelnden erfolgende Äußerungen aufzuzeichnen;* 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 fällt auf, dass die StPO ausdrücklich auch die technischen Mittel zur Bild- und Ton*übertragung* 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 Mobilteilnehmerkennung (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 einen 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[33], 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.

---

33 OGH 26.7.2005, 11 Os 57/05Z = JBl 2006, 130; OGH 6.12.1995, 13 Os 161/95 = JBl 1997, 260; OGH 17.6.1998, 13 Os 68/98 = EvBl 1998/191; wichtig: VwGH 27.5.2009, GZ 2007/05/0280; *Reindl*, Telefonüberwachung zweimal neu?, ÖJZ 2002, 69; dies, Die nachträgliche Offenlegung der Vermittlungsdaten im Fernmeldeverkehr („Rufdatenrückerfassung"), JBl 1999, 791; dies, WK-StPO Vor §§ 149a – c RZ, 9 (Stand: Jänner 2005); *Einzinger et al*, Wer ist 217.204.27.214?, MR 2005, 113; *Funk et al.*, Zur Registrierung von Ferngesprächsdaten durch den Dienstgeber, RdA 1984, 285; *Schmölzer*, Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr, JBl 1997, 211 (214).

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 Kommunikationspartner abgeleitet werden, sondern gleichsam Profile der Betroffenen erstellt werden, aus denen wiederum auf Kommunikationsinhalte geschlossen werden kann: So weist zum Bespiel 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[34], 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**".

[34] VfGH G 47/2012-49 u.a. Rz 168.

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[35] 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.

---

[35] Gemäß § 3 DSVO gibt es u.a. Ausnahmen bei Fällen von „Gefahr im Verzug" sowie für Notrufträger, eine generelle Ausnahme für eine ganze Behörde oder einen bestimmten Aufgabenbereich existiert jedoch nicht.

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.

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.

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. Möglichkeiten, wie z.B. ohne technische Kenntnisse über Facebook-Gesichtserkennungsdienste mit einem Referenzbild zu einer Person diese im Netz wiederfinden zu können, kämen aus damaliger Sicht für sich genommen bereits der Eingriffsintensität einer „Rasterfahndung“ gleich.

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.[36] 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. Beispielhaft genannt seien hier Sail LabsTechnology, Wien (http://www.arax.at/venture_capital/unternehmen_a_z_/sail_labs/), Recorded Future, Boston (https://www.recordedfuture.com/blog/), BLAB, Seattle (http://www.blabpredicts.com/), Brandwatch GmbH, Berlin (https://www.brandwatch.com/de/) oder Echosec (https://www.echosec.net/). Außerdem wird an diesem Thema auch mit öffentlichen Mitteln geforscht, wie etwa das von der EU geförderte Forschungsprojekt VIRTUOSO zeigt (http://www.virtuoso.eu/).

---

[36] EGMR Rotaru v. Rumänien, Urteil 04.05.2000, 28341/95, Rn 43.

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

§ 12 Abs. 3 PStSG
„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."

§ 13 Abs. 1 PStSG
„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.“

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[37] 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:

[37] AB 988 BlgNR XXV. GP, 8 f.

„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 besondere 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. Im 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:

> 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.**"

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 detaillierter 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, welches 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.[38]

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.[39] 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.

---

38 Vgl. EGMR 9.6.1998, Teixeira de Castro gg. Portugal, EuGRZ 1999, 660; ÖJZ 1999, 434 (eingehend dazu *Fuchs*, Verdeckte Ermittler – anonyme Zeugen, ÖJZ 2001, 495 [496 ff.] sowie EGMR 5.2.2008, Ramanauskas gg. Litauen, NL 2008, 21 und 4.11.2010, Bannikova gg. Russland.

39 EGMR 5.2.2008, Ramanauskas gg. Litauen, NL 2008, 21 und 4.11.2010, Bannikova gg. Russland (Z 48); *Grabenwarter/Pabel*, EMRK[5] § 24 Rz 63.

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 allem 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.[40]

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.

---

40 13 Os 153/03; 15 Os 63/04; *Kirchbacher*, WK-StPO § 252 Rz 66 f; EGMR 23.4.1997, Van Mechelen und andere gg. die Niederlande, NL 1997, 91; kritisch: *Schwaighofer*, Der Unmittelbarkeitsgrundsatz beim Zeugenbeweis und seine Ausnahmen, ÖJZ 1996, 124 (134) mit Berufung auf (die mittlerweile überholte Entscheidung) 14 Os 40/95.

7.9 § 4 (Das BVT als Zentralstelle)

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.

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.[41] 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.[42]

---

[41] Vgl zB die Ausführungen des Leiters des BVT, Peter Gridling in einer Podiumsdiskussion, Video abrufbar unter https://www.youtube.com/watch?v=ROMR0ZV5vZk, insbesondere ab Minute 2:01:40.

[42] Vgl die Ausführungen des EuGH in C-362/14 (Safe Harbor), Rn 90 und die dort zitierte Analyse der EU-Kommission zu Safe Harbor anlässlich der Veröffentlichungen durch Edward Snwoden. Einen Beleg für die Zusammenarbeit des HNaA mit der NSA findet man unter http://www.profil.at/home/hna-heeresnachrichtenamt-was-us-geheimdienste-362038 (15.6.2016).

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[43] zur Stärkung der Netzwerk- und Informationssicherheit, deren Inkrafttreten für August 2016 erwartet wird.

---

[43] Ratsdokument Nr. 5581/16 vom 21. April 2016.

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[44]-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.

[44] Informations- und Kommunikationstechnologie.

8. ANTRÄGE

Die Antragsteller stellen durch ihren bevollmächtigten Vertreter gemäß Art 140 Abs.1 Z 2 B-VG und §§ 62 ff VfGG die

ANTRÄGE,

der Verfassungsgerichtshof möge als verfassungswidrig aufheben

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. die Wortfolge „**oder im Auftrag der Sicherheitsbehörde durch andere Personen (Vertrauenspersonen), die ihren Auftrag weder offen legen noch erkennen lassen,"**
- in Ziffer 16. den letzten Satz „**§ 54a gilt für verdeckte Ermittlungen durch Vertrauenspersonen nicht."**;
- in Ziffer 24. den Satz „**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."** sowie im letzten Satz die Wortfolge „**, die Zusammensetzung des Rechtsschutzsenates (§ 14 Abs. 3 PStSG) sowie dessen Entscheidungsfindung"**;
- in Ziffer 30. in Absatz 8 die Wortfolge „**sowie unter den Voraussetzungen des § 53a Abs. 5a in der Fassung BGBl. I Nr. 5/2016 auch im Informationsverbundsystem geführt"**;

in eventu zusätzlich

- in Ziffer 1. die Wortfolge **„und es entfällt der Eintrag „§ 93a Information verfassungsmäßiger Einrichtungen""**;
- in Ziffer 6. die Wortfolge **„sowie 93a samt Überschrift"**;
- in Ziffer 29. in Absatz 39 die Wortfolge **„und 93a samt Überschrift"**;

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 Ziffer 24. den Satz **„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."** sowie im letzten Satz die Wortfolge „**, die Zusammensetzung des Rechtsschutzsenates (§ 14 Abs. 3 PStSG) sowie dessen Entscheidungsfindung"**;

in eventu zusätzlich

- in Ziffer 1. die Wortfolge **„und es entfällt der Eintrag „§ 93a Information verfassungsmäßiger Einrichtungen""**;
- in Ziffer 6. die Wortfolge **„sowie 93a samt Überschrift"**;
- in Ziffer 29. in Absatz 39 die Wortfolge **„und 93a samt Überschrift"**;

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 1, **zur Gänze;**
Artikel 2, Ziffer 6., 8., 14., und 27. **zur Gänze**;

- in Ziffer 1. die Wortfolge **„und es entfällt der Eintrag „§ 93a Information verfassungsmäßiger Einrichtungen""**;
- in Ziffer 24. den Satz **„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."** sowie im letzten Satz die Wortfolge „**, die Zusammensetzung des Rechtsschutzsenates (§ 14 Abs. 3 PStSG) sowie dessen Entscheidungsfindung"**;
- in Ziffer 29. In Absatz 39 die Wortfolge **„und 93a samt Überschrift"**;

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. den Satz **„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."** sowie im letzten Satz die Wortfolge „**, die Zusammensetzung des Rechtsschutzsenates (§ 14 Abs. 3 PStSG) sowie dessen Entscheidungsfindung"**;

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 Bundesgesetz 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 (§ 6 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. die 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 § 162 StPO.“**;

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. in Absatz 8 die Wortfolge „**sowie unter den Voraussetzungen des § 53a Abs. 5a in der Fassung BGBl. I Nr. 5/2016 auch im Informationsverbundsystem geführt**“;

alle wegen Verletzung des Rechtsstaatsprinzips, des § 1 DSG 2000 sowie der Artikel 8, 10 und 13 EMRK sowie Art 7 B-VG.

Wien, am 27. Juni 2016 für die Antragsteller/innen