Neue Rechtsgrundlage für den Staatsschutz (Polizeiliches Staatsschutzgesetz - PStSG) und Neuerungen im SPG

Ass.-Prof. Mag. Dr. Farsam Salimi

I. Zum Polizeilichen StaatsschutzG

1. Allgemeines

Am 31.3.2015 wurde ein Entwurf für ein neues **Polizeiliches Staatschutzgesetz (PStSG)** vorgelegt, das die Rechtsgrundlage für die Tätigkeit des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung (BVT) sowie der Landesämter Verfassungsschutz (LV) bilden soll.[1] Die wichtigsten Inhalte dieses Gesetzesvorschlages werden im Folgenden zusammengefasst.

Derzeit gilt für das BVT und die LV – wie für alle Sicherheitsbehörden – das Sicherheitspolizeigesetz als Rechtsgrundlage ihrer Tätigkeit. Besondere Bedeutung für den Staatsschutz hat § 21 Abs 3 SPG, der die Aufgabe der „erweiterten Gefahrenerforschung" normiert. Durch das vorgeschlagene Gesetz sollen die Aufgaben und Befugnisse des Staatsschutzes nur noch dem BVT und den LV zukommen, gleichzeitig werden die Aufgaben und Befugnisse neu gefasst und zum Teil erweitert.

Dabei soll der Staatsschutz nicht etwa aus der Organisation des Bundesministeriums für Inneres herausgelöst werden, sondern **weiter Teilorganisation der Generaldirektion für die öffentliche Sicherheit** bleiben.[2] Auftraggeber für die Verwendung personenbezogener Daten iSd § 4 Z 4 DSG bleibt grundsätzlich in Hinblick auf das BVT der Bundesminister für Inneres, für die LV die Landespolizeidirektion (vgl § 1 Abs 3 PStG). **§ 1 Abs 2 PStSG** definiert den **Umfang des „polizeilichen Staatsschutzes".** Dieser umfasst den Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit sowie von Vertretern ausländischer Staaten, internationaler Organisationen und anderer Völkerrechtssubjekte nach Maßgabe völkerrechtlicher Verpflichtungen, kritischer Infrastruktur und der Bevölkerung vor terroristisch, weltanschaulich oder religiös motivierter Kriminalität, vor Gefährdungen durch Spionage, durch nachrichtendienstliche Tätigkeit und durch Proliferation sowie die Wahrnehmung zentraler Funktionen der internationalen Zusammenarbeit in diesen Bereichen.

2. Organisation und Zentralstellenfunktionen

§ 2 PStSG regelt die **Organisation** des Bundesamts und der LV. Der Direktor des BVT muss besondere Kenntnisse auf dem Gebiet des polizeilichen Staatsschutzes aufweisen, Jurist sein und mindestens fünf Jahre in einem Beruf tätig gewesen sein, für den ein Rechtswissenschaftsstudium Voraussetzung ist (§ 2 Abs 1 PStG). Die spezielle Ausbildung der sonstigen Bediensteten des BVT und der LV ist in § 2 Abs 3 PStG geregelt; § 2 Abs 5 PStG bestimmt, dass die Bediensteten Sicherheitsüberprüfungen nach § 55 SPG unterzogen werden müssen.

[1] http://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00110/index.shtml.
[2] Erläut 110/ME 25.GP 2.

§ 4 PStSG regelt die **Zentralstellenfunktionen** des BVT. Vergleichbar mit der organisatorischen Vorschrift des § 4 Abs 2 BKA-G besagt § 4 PStSG, dass das BVT für den Bundesminister für Inneres als „Operative Koordinierungsstelle" für Angriffe auf Computersysteme verfassungsmäßiger Einrichtungen und kritischer Infrastrukturen (§ 4 Z 1 PStSG) sowie als Meldestelle für Fälle von nationalsozialistischer Wiederbetätigung (§ 4 Z 2 PStSG) fungiert. Weiters ist das Bundesamt zuständig für Sicherheitsüberprüfungen nach § 55 SPG (§ 4 Z 3 PStSG), die Gebäudesicherheit der Zentralstellen des BMI (§ 4 Z 4 PStSG) sowie die internationale Zusammenarbeit auf dem Gebiet des polizeilichen Staatsschutzes (§ 4 Z 5 PStSG).

§ 5 PStSG enthält eine **Generalklausel**, wonach das Sicherheitspolizeigesetz auch nach Inkrafttreten des PStSG für den Staatschutz anwendbar bleibt, soweit das PStSG keine besonderen Regelungen bereithält. Diese „Auffangfunktion" des SPG ist Konsequenz des Verbleibs des Staatsschutzes innerhalb der Sicherheitsbehördenstruktur. Damit können sich BVT und LV etwa in Bezug auf die Abwehr gefährlicher Angriffe weiterhin auf die Aufgaben und Befugnisse im SPG stützen.[3]

3. Erweiterte Gefahrenerforschung und sonstige Aufgaben

§ 6 PStSG enthält die zentralen Aufgaben des Staatsschutzes. Diesem obliegt nunmehr die „**Erweiterte Gefahrenerforschung und der Schutz vor verfassungsgefährdenden Angriffen**". **§ 6 Abs 1 Z 1 PStSG** definiert die erweiterte **Gefahrenerforschung bei Gruppierungen**, wobei diese Bestimmung wortgleich dem geltenden § 21 Abs 3 Z 2 SPG entspricht. § 6 Abs 1 Z 2 PStSG betrifft die erweiterte **Gefahrenerforschung bei Einzelpersonen** nach dem geltenden § 21 Abs 3 Z 1 SPG. Nach geltendem Recht ist eine erweiterte Gefahrenerforschung in Bezug auf Einzelpersonen nur zulässig, wenn sich diese Person öffentlich oder in schriftlicher oder elektronischer Kommunikation für Gewalt ausgesprochen oder sich Mittel und Kenntnisse verschafft hat, die sie in die Lage versetzen, Anschläge zu verüben, und zusätzlich damit zu rechnen ist, dass sie eine mit schwerer Gefahr für die öffentliche Sicherheit verbundene weltanschaulich oder religiös motivierte Gewalt herbeiführt. Nach der vorgeschlagenen Bestimmung fällt die Voraussetzung eines bestimmten Vorverhaltens der Person weg. Es reichen demnach künftig – anders als nach der geltenden Rechtslage – zu Recht auch entsprechende Aussagen gegenüber einem Strafverfolgungsorgan, wenn diese einen verfassungsgefährdenden Angriff wahrscheinlich erscheinen lassen.[4] Entscheidend bleibt aber die Prognose: Es muss **wahrscheinlich** sein, dass die Zielperson einen verfassungsgefährdenden Angriff begehen wird. Wahrscheinlich ist ein Angriff dann, wenn aufgrund hinreichender Anhaltspunkte anzunehmen ist, die Person werde einen verfassungsgefährdenden Angriff begehen. Die bloße Möglichkeit oder Nichtausschließbarkeit reicht nicht aus, der bevorstehende Angriff muss aber auch nicht gewiss sein.[5] Eine weitere Neuerung gegenüber der jetzigen Rechtslage besteht darin, dass der wahrscheinliche Angriff nicht unbedingt eine weltanschaulich oder religiös motivierte Gewalttat sein muss (vgl § 21 Abs 1 Z 1 SPG); vielmehr kommt nach dem Entwurf jeder verfassungsgefährdende Angriff in Frage.

§ 6 Abs 1 Z 3 PStSG enthält die spezielle Aufgabe des Schutzes vor verfassungsgefährdenden Angriffen aufgrund von **Informationen von Dienststellen inländischer Behörden oder ausländischer**

[3] Erläut 110/ME 25.GP 3.
[4] Erläut 110/ME 25.GP 3.
[5] Erläut 110/ME 25.GP 4.

Sicherheitsbehörden zu Personen, die verdächtig sind, im Ausland verfassungsgefährdende Angriffe gesetzt zu haben. Damit sollen insb nachrichtendienstlichen Informationen über gefährliche Personen ausreichend Rechnung getragen werden. Die daran anknüpfenden Befugnisse beschränken sich auf §§ 10 und 11 PStSG. Die besonderen Datenermittlungsbefugnisse des § 12 PStG sind zur Erfüllung dieser Aufgabe nicht anwendbar.

§ 6 Abs 2 PStSG definiert den **verfassungsgefährdenden Angriff**. Dazu werden konkrete Straftatbestände des StGB taxativ aufgezählt. Die Strafrechtsakzessorietät des Polizeirechts wird dadurch konsequent weiter betrieben und durch einen konkreten Straftatenkatalog im Bereich der erweiterten Gefahrenerforschung und des Schutzes vor verfassungsgefährdenden Angriffen von Einzelpersonen gegenüber der geltenden Rechtslage noch ausgebaut. Ein verfassungsgefährdender Angriff ist nach dem ME die Bedrohung von Rechtsgütern durch terrorismusbezogene Tatbestände (§ 6 Abs 2 Z 1: §§ §§ 278b, 278c bis 278f sowie § 165 Abs 3 StGB), weltanschaulich oder religiös motivierte Delikte mit extremistischem Hintergrund (§ 6 Abs 2 Z 2: §§ 279, 280, 282, 283 StGB oder die in § 278c StGB genannten strafbaren Handlungen), bestimmte Delikte gegen den öffentlichen Frieden sowie Staatsschutz- und Spionagedelikte (§ 6 Abs 2 Z 3: §§ 274, 284, 285 StGB, 14. – 16. Abschnitt des StGB, Verbotsgesetz), bestimmte Delikte in Zusammenhang mit Proliferation und Störungen der Beziehungen zum Ausland (§ 6 Abs 2 Z 4: §§ 175, 177a, 177b StGB, §§ 79 bis 82 AußenwirtschaftsG, § 7 KMG; §§ 124, 316, 319 und 320 StGB) sowie Cybercrime-Delikte, die sich gegen verfassungsmäßige Einrichtungen sowie kritische Infrastruktur richten (§ 6 Abs 2 Z 5: §§ 118a, 119, 119a, 126a, 126b, 126c StGB). Dabei ist – wie derzeit beim gefährlichen Angriff iSd § 16 SPG – zwar tatbestandmäßiges und rechtswidriges, nicht jedoch schuldhaftes Verhalten vorausgesetzt.

§ 7 PStSG beinhaltet eine der kriminalpolizeilichen Beratung in § 25 SPG vergleichbare Regelung über **staatsschutzrelevante Beratung** durch Öffentlichkeitsarbeit und Beratung von juristischen und natürlichen Personen. Zu denken ist etwa an Aufklärung über modi operandi bei Cyberangriffen sowie mögliche Gefahren durch Wirtschafts- und Industriespionage. [6]

§ 8 PStSG enthält die bisher in § 93a SPG geregelte Aufgabe der **Information verfassungsmäßiger Einrichtungen.** Dazu obliegen dem BVT und den LV die Analyse und Beurteilung staatsschutzrelevanter Bedrohungslagen. Diese können sich auch aus verfassungsgefährdenden Entwicklungen im Ausland ergeben. Bei solchen Bedrohungen hat die Bundesministerin für Inneres die in Abs 2 genannten verfassungsmäßigen Einrichtungen wie den Bundespräsidenten, die Präsidenten des Nationalrats sowie die Mitglieder der Bundesregierung zu unterrichten. Die Information der Landeshauptleute obliegt gem § 8 Abs 3 PStSG dem Landespolizeidirektor.

4. Befugnisse

Die **§§ 9 ff PStSG** normieren die zentralen Befugnisse des Staatschutzes. **§ 9 PStSG** regelt die **Aufgabenbezogenheit**: Personenbezogene Daten dürfen vom BVT und den LV gem den §§ 10 ff PStSG nur verwendet werden, wenn dies zur Erfüllung ihrer Aufgaben notwendig ist. Als Aufgaben kommen die §§ 6 bis 8 PStSG in Frage. Dabei soll nach den Materialien durch den Verweis auf das

[6] Erläut 110/ME 25.GP 4.

SPG in § 5 PStSG auch § 51 SPG mitzulesen sein, sodass die Wahrung der **Verhältnismäßigkeit** bei Datenverwendungen auch für den Staatsschutz zwingend ist.[7]

§ 10 PStSG enthält eine **allgemeine Datenermittlungsbefugnis**, vergleichbar § 53 Abs 1 SPG. Diese allgemeine Ermächtigung wird durch die folgenden §§ 11 und 12 PStSG begrenzt, die besondere Datenverwendungsbefugnisse und besondere Voraussetzungen für diese enthalten. Die Abs 2 bis 4 des § 10 PStSG sind § 53 Abs 2, 3 und 5 SPG nachgebildet. § 10 Abs 5 PStSG entspricht weitgehend § 53 Abs 4 SPG: Demnach ist es dem Staatsschutz erlaubt, zur Erfüllung seiner Aufgaben nach Abs 1 personenbezogene Daten aus allen anderen verfügbaren Quellen, insb durch Zugriff auf im Internet öffentlich zugängliche Daten, zu ermitteln und weiterzuverarbeiten. Öffentlich zugängliche Daten sind nach den Materialien solche, die einem nicht im Vorhinein beschränkten Personenkreis im Internet zugänglich sind.[8] Darunter fallen etwa Daten in offenen Blogs, Foren, Newsgroups, aber auch solche in Foren und sozialen Netzwerken, deren Zugang lediglich eine Anmeldung durch Zulegen eines „Nicknames" erfordert. [9] Dabei soll aber dem Organ nicht erlaubt werden, aktiv Informationen zu ermitteln. Eine solche „verdeckte Ermittlung" wäre nur unter den Voraussetzungen des § 12 PStSG möglich.[10]

§ 11 PStSG regelt die **Datenanwendungen**, die vom BVT und den LV im Informationsverbund geführt werden und der operativen oder strategischen Analyse dienen. § 11 Abs 1 PStSG definiert die Datenkategorien, die verarbeitet werden dürfen (Z 1 und 2 zu den Betroffenen von Aufgaben nach § 6 Abs 1 Z 1 bis 3 bzw Verdächtigen eines verfassungsgefährdenden Angriffs, Z 3 die Daten von Kontakt- und Begleitpersonen, Z 4 die Daten zu Informanten und sonstigen Auskunftspersonen). § 11 Abs 2 PStSG enthält Löschungspflichten für die nach Abs 1 verarbeiteten Daten, wobei alle Daten spätestens nach fünf Jahren zu löschen sind. § 11 Abs 3 PStSG regelt, dass die Daten schon vor ihrer Verarbeitung auf ihre Erheblichkeit und Richtigkeit hin zu überprüfen und während der Dauer der Verarbeitung aktuell zu halten sind. Erweisen sich Daten als unrichtig, sind diese idR richtigzustellen oder zu löschen. Abs 4 bestimmt, dass jede Abfrage und Übermittlung personenbezogener Daten aus diesen Datenanwendungen zu protokollieren ist, wobei die Protokolldaten drei Jahre aufzubewahren sind. Damit werden in den Abs 3 und 4 allgemeine datenschutzrechtliche Grundsätze speziell für die staatsschutzrelevanten Analysedateien festgeschrieben.

Die **besonderen Ermittlungsmaßnahmen** des Staatsschutzes sind in **§ 12 PStG** geregelt. Nach § 12 Abs 1 PStSG ist zur erweiterten Gefahrenerforschung (§ 6 Abs 1 Z 1 PStSG) und zum Schutz vor wahrscheinlichen verfassungsgefährdenden Angriffen (§ 6 Abs 1 Z 2 PStSG) die Ermittlung personenbezogener Daten durch folgende Maßnahmen zulässig:

1. Observation, inkl Einsatz technischer Mittel (§ 54 Abs 2 und Abs 2a SPG);
2. Verdeckte Ermittlung (§ 54 Abs 3 SPG);
3. Einsatz von Bild- und Tonaufzeichnungsgeräten; auch verdeckt, falls die Aufgabe ansonsten aussichtlos wäre (§ 54 Abs 4 SPG);
4. Einsatz von Kennzeichnungserkennungsgeräten (§ 54 Abs 4b SPG); dabei soll kein Abgleich mit dem KFZ-Register erfolgen, sondern lediglich ein Abgleich mit KFZ-Kennzeichen aus Datenanwendungen nach § 11 Abs 1 Z 1 lit l PStSG.

[7] Erläut 110/ME 25.GP 5.
[8] Erläut 110/ME 25.GP 5.
[9] Erläut 110/ME 25.GP 6.
[10] Erläut 110/ME 25.GP 6.

5. Auskünfte zu Stammdaten, IP-Adressen und Name und Anschrift zu dynamischen IP-Adressen sowie Standorten von Personen, die von einer Aufgabe nach § 6 Abs 1 Z 1 und 2 PStSG betroffen sind, sowie zu deren Kontakt- oder Begleitpersonen bei Betreibern öffentlicher Telekommunikationsdienste und sonstigen Diensteanbietern (vgl § 53 Abs 3a und b SPG);
6. Auskünfte von Beförderungsunternehmen (Fluggesellschaften, Reisebüros, Mietwagenfirmen) [11] und
7. Auskünfte zu sonstigen, über Z 5 hinausgehenden Verkehrsdaten, Zugangsdaten und Standortdaten für einen beschränkten Zeitraum. Damit wird eine § 134 Z 2 StPO vergleichbare Befugnis eigens für den Staatsschutz geschaffen, wobei die rechtliche Kontrolle für den Staatschutz – der bisherigen Systematik des Polizeirechts entsprechend – durch den Rechtsschutzbeauftragen beim BMI erfolgt.

§ 13 PStSG regelt die **Vertrauenspersonenevidenz**. Die Regelung ist weitgehend § 54b SPG nachgebildet. Durch die Änderung des § 54 Abs 3 SPG (siehe dazu Seite 7), soll auch im Bereich des SPG der **Einsatz von Vertrauenspersonen** ermöglicht werden. Durch den allgemeinen Verweis in § 12 Abs 1 PStSG auf § 54 Abs 3 SPG wird es dem Entwurf nach auch dem Staatsschutz möglich sein, verdeckte Ermittlungen nicht nur durch eigene Ermittler durchzuführen, sondern auch Vertrauenspersonen aus dem jeweiligen Milieu einzusetzen.

Richtigstellungs- und Löschungsverpflichtungen in Bezug auf unrichtige oder entgegen den Bestimmungen des PStSG ermittelte Daten sind in **§ 14 Abs 1 PStSG** geregelt, ebenso die Löschungsverpflichtung in Bezug auf Daten, die nicht mehr benötigt werden, es sei denn, es bestünde eine spezielle Regelung, etwa in Bezug auf die nach § 11 PStSG verarbeiteten Daten. § 14 Abs 2 PStSG regelt die derzeit in § 63 Abs 1b SPG normierten Löschungspflichten neu. Daten, die zur Erfüllung der Aufgaben der erweiterten Gefahrenerforschung sowie des Schutzes vor verfassungsgefährdenden Angriffen ermittelt wurden, können demnach auch nach Ablauf der Zeit, für die die Ermächtigung durch den RSB erteilt wurde, aufbewahrt werden, wenn aufgrund bestimmter Tatsachen erwartet werden kann, dass die betroffene Person neuerlich Anlass zu einer entsprechenden Aufgabe geben wird. Nach regelmäßigen Überprüfungen (alle 6 Monate) sowie Ermächtigungen zur Weiterverarbeitung durch den Rechtsschutzbeauftragen (zwei Jahre nach Ablauf der Ermächtigung für die Datenermittlung, dann jeweils jährlich) müssen die Daten aber jedenfalls nach Ablauf von sechs Jahren endgültig gelöscht werden.

5. Rechtsschutz

Der **besondere Rechtschutz** im Bereich des Staatsschutzes obliegt – wie bisher nach dem SPG – dem unabhängigen **Rechtsschutzbeauftragen beim BMI (§ 15 Abs 1 PStSG**). Stellt sich eine Aufgabe nach § 6 Abs 1 Z 1 oder 2 PStSG oder sollen Befugnisse nach § 12 oder § 10 Abs 4 PStSG in Anspruch genommen werden, dann ist vorab die Ermächtigung des Rechtsschutzbeauftragen einzuholen. Die Ermächtigung darf höchstens für sechs Monate erteilt werden, wobei (auch mehrere) Verlängerungen zulässig sind. Dieser Rechtsschutz entspricht dem jetzigen Stand bezogen auf die derzeit verfügbaren Befugnisse nach dem SPG. Obwohl dies für die besonderen Ermittlungsnahmen im SPG derzeit nicht zwingend vorgeschrieben wird, erteilt der Rechtsschutzbeauftrage auch nach geltender Rechtslage seine Ermächtigungen generell nur für einen Zeitraum von höchstens sechs

[11] Erläut 110/ME 25.GP 7.

Monaten, wobei Verlängerungsanträge zulässig sind. Die in **§ 16 PStSG** geregelten **Rechte und Pflichten des Rechtsschutzbeauftragen** entsprechen jenen in § 91 d SPG.

Ergänzt wird der kommissarische Rechtsschutz durch eine **Verpflichtung zur Information Betroffener** in **§ 17 PStSG**. Nimmt der Rechtsschutzbeauftrage eine rechtswidrige Verwendung personenbezogener Daten wahr, hat er den Betroffenen zu informieren oder Beschwerde an die Datenschutzbehörde zu erheben und so die Rechte des Betroffenen stellvertretend wahrzunehmen, falls dies nicht möglich ist (§ 17 Abs 1 PStSG). Nach Ablauf der Zeit, für die die Ermächtigung erteilt wurde, ist der Betroffene grundsätzlich vom BVT und LV über Grund, Dauer und Rechtsgrundlage der gegen ihn gerichteten Maßnahme zu informieren (§ 17 Abs 2 PStSG), worüber dem Rechtsschutzbeauftragen Bericht zu erstatten ist. § 17 Abs 3 PStSG regelt jene Fälle, in denen diese Information des Betroffenen aufgeschoben werden oder unterbleiben kann.

§ 18 PStSG normiert zum einen die **Verpflichtung des BVT** zur jährlichen Erstellung eines **Berichts** an die Öffentlichkeit (Abs 1), zum anderen eine **halbjährliche Berichtspflicht der Bundesministerin für Inneres** an den ständigen Unterausschuss des Innenausschusses (Abs 2) und in Abs 3 die Verpflichtung der Bundesministerin für Inneres, den jährlich zu verfassenden **Tätigkeitsbericht des Rechtsschutzbeauftragen** dem genannten **Unterausschuss zugänglich** zu machen.

II. Zum Sicherheitspolizeigesetz

Neben Anpassungen, die sich aufgrund des Herauslösens der erweiterten Gefahrenerforschung in § 21 Abs 3 aus dem SPG ergeben, enthält der Ministerialentwurf andere, nicht unmittelbar im Zusammenhang mit dem PStSG stehende Änderungen. Die wichtigsten Reformvorhaben werden in der Folge kurz zusammengefasst.

Zum einen soll durch Schaffung eines **§ 13a Abs 3 SPG** eine Rechtsgrundlage für den **offenen Einsatz von Bild- und Tonaufzeichnungsgeräten**, etwa sog „body worn cameras“, geschaffen werden. Diese dienen dem Zweck der Dokumentation von Amtshandlungen, wodurch die Einordnung in § 13a SPG verständlich wird. Solche Geräte dürfen aber nicht beim regulären Streifendienst zum Einsatz kommen, sondern nur soweit der Einsatz von Befehls- und Zwangsgewalt ausgeübt wird. Der Einsatz soll für alle Beteiligten eindeutig erkennbar sein.[12]

Durch Einfügung eines **§ 21 Abs 2a SPG** wird normiert, dass den Sicherheitsbehörden auch die **Abwehr und Beendigung von gefährlichen Angriffen an Bord österreichischer Zivilluftfahrzeuge** obliegt, soweit sich ihre Organe auf Ersuchen des Luftfahrzeughalters oder zur Erfüllung ihrer Aufgaben an Bord befinden und kein bindendes Völkerrecht dagegensteht.

Bei der **Standortfeststellung** in **§ 54 Abs 3b SPG** wird der Kreis der Personen, deren Standort gepeilt werden kann, erweitert. Neben der gefährdeten Person und ihrer Begleitperson soll nun auch der **Gefährder** gepeilt werden dürfen, etwa eine Person, die eine Bombendrohung geäußert hat.[13]

[12] Erläut 110/ME 25.GP 11.
[13] Erläut 110/ME 25.GP 12.

§ 54 Abs 3 SPG idF ME sieht allgemein den **Einsatz von Vertrauenspersonen** auch im Bereich des Sicherheitspolizeigesetzes vor. Die Bestimmungen im PStSG knüpfen an diese allgemeine Erweiterung der verdeckten Ermittlung im polizeilichen Bereich an.

Durch eine Änderung in **§ 54 Abs 5 SPG** sollen **Bild- und Tonaufzeichnungsgeräte** auch in sachlichem, zeitlichem und örtlichem Zusammenhang mit einer Zusammenkunft zahlreicher Menschen zum Einsatz kommen können. Durch diese Erweiterung dürften auch die Daten von Personen aufgezeichnet werden, die sich von der Zusammenkunft im Rahmen von Aufsplitterungen entfernt haben.[14] Die Aufzeichnungen dürfen nach dem ME auch zur Verfolgung von Verwaltungsübertretungen verwendet werden.

Der ME schlägt **in § 75 Abs 1a SPG** eine eigene Rechtsgrundlage für die **Verarbeitung von Spuren** vor, die auf Grundlage der StPO ermittelt wurden. Zweck dieser Verarbeitung ist die Zuordnung dieser Spuren zu einer Person, wobei nur solche Spuren erfasst sind, die auch Gegenstand einer erkennungsdienstlichen Maßnahme nach § 64 Abs 2 SPG sein können, insb Fingerabdrücke, DNA-Profile oder Abbildungen.[15]

Änderungen in **§ 75 Abs 2 SPG** sollen es ermöglichen, dass die nach Abs 1 und Abs 1a verarbeiteten Daten miteinander verglichen werden dürfen. Daneben werden nach dem ME Abfragen und Übermittlungen von Daten nach Abs 1 und Abs 1a im Dienst der Strafrechtspflege, der Sicherheitspolizei und anderer Aufgaben der Sicherheitsverwaltung zulässig sein, wenn die jeweiligen Materiengesetze dies erlauben. § 80 Abs 1a SPG enthält eine Konkretisierung des Auskunftsrechts nach § 26 DSG in Bezug auf die nach § 75 Abs 1a SPG idf ME verarbeiteten Daten.

[14] Erläut 110/ME 25.GP 12.
[15] Erläut 110/ME 25.GP 13.