Verein Arbeitskreis Vorratsdaten Österreich (AKVorrat.at),
ZVR: 140062668
Kirchberggasse 7/5
1070 Wien
info@akvorrat.at

Wien, 14. April 2015

Betreff: Stellungnahme des Arbeitskreis Vorratsdaten im Begutachtungsverfahren zum Entwurf des BM.I für ein Polizeiliches Staatsschutzgesetz – PStSG und Änderungen im SPG.

Für den AKVorrat: Ing. Dr. Christof Tschohl, RA Mag. Ewald Scheucher, Rolf-Dieter Kargl, LL.B. (WU)

Der AKVorrat nimmt zu dem Begutachtungsentwurf wie folgt Stellung:

Bundesgesetz, mit dem das Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz – PStSG) erlassen wird

I. Einleitung – Grundsatzkritik

Mit dem vorgeschlagenen PStSG kommen wir endgültig im „Feindrechtsstaat“ an.

Mit der „organisierten (internationalen) Kriminalität“, den Terroristen, den Extremisten, den Radikalen aller Schattierungen sind dem „freie Westen“ und damit auch dem kleinen Österreich offensichtlich so viele „Feinde“ erwachsen, dass deren – behauptete oder tatsächliche – Gefährlichkeit von der Politik und den staatlichen und supranationalen Sicherheitsapparaten nur mehr durch eine ständig gesteigerte Intensität von Grundrechtseingriffen, durch eine massive „Sicherheitsgesetzgebung“ begegnet werden kann. Natürlich nur, um „Sicherheit“ zu gewährleisten.

Angesichts dieser – behaupteten oder tatsächlichen – Gefahren für „unser Gemeinwesen“, die von „unseren Feinden“ ausgehen, müssen effizienten Ermittlungen und eine erfolgreiche Strafverfolgung offensichtlich oberste Priorität erhalten, was immer auch die Folgen für unser Gemeinwesen sein mögen. Wir befinden uns offensichtlich im Übergang weg von einer „Strafrechtgesetzgebung“, die inkriminiertes Verhalten sanktioniert, hin zu einer „Bekämpfungsgesetzgebung“, die „unsere Feinde“ schon im Vorfeld erkennen und ausschalten soll.

Da die Gefahrenabwehr in den Vordergrund der Sicherheits- und Justizpolitik rückt, musste ja bereits die Strafbarkeit soweit wie möglich in das „Vorfeld“ des eigentlich bekämpften strafbaren Verhaltens verlagert werden. Hier muss(te) regelmäßig das Argument herhalten, „unsere Feinde“ hielten sich weder an staatliche noch moralische Gesetze und seien daher immer einen Schritt voraus. Nach den vorliegenden Entwürfen sollen die Verfassungsschützer von Bund und Ländern zur Kompensation dieses Problems nun über all die rechtsstaatlichen „Hindernisse“ der Strafprozessordnung und (teilweise) des Sicherheitspolizeigesetzes erhaben werden, allein schon um die Wahrscheinlichkeit zu bewerten, ob ein „verfassungsgefährdender Angriff“ drohen könnte. Wie weit dieser – durch einen Straftatenkatalog definierte – Begriff geht und warum diese Definition in Bezug auf die Zielsetzung überschießend ist, wird unten im „besonderen Teil“ dieser Stellungnahme im Detail dargestellt.

Am 08.04.2014 hob Gerichtshof der EU (EuGH) die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung (VDS-RL), zur Gänze auf, weil sie gegen die EU Grundrechte verstieß. Am 27.06.2014 folgte ihm darin der österreichische Verfassungsgerichtshof (VfGH) und hob auch die innerstaatliche Umsetzung der VDS-RL als verfassungswidrig auf. Der EuGH erkennt in seiner Urteilsbegründung auch ausdrücklich an, „dass nach Art. 6 der Charta jeder Mensch nicht nur das Recht auf Freiheit, sondern auch auf Sicherheit hat“[1]. 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. Auch Art. 5 der Europäischen Menschenrechtskonvention garantiert im ersten Satz wortgleich: „Jede Person hat das Recht auf Freiheit und Sicherheit“. Die ausdrückliche Erwähnung des Rechts auf Sicherheit in den Freiheitsgewährleistungen ist eher als Katalysator für die Einhaltung der Gesetzmäßigkeit bei Freiheitsentziehungen zu verstehen. Der Verfassungsgesetzgeber des „Bundesverfassungsgesetzes zum Schutz der persönlichen Freiheit“ (PersFrG) hat den Begriff unreflektiert aus der Konvention

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

übernommen.[2] Nach herrschender Ansicht kommt ihm nach keiner der Grundrechtsgarantien eine eigenständige Bedeutung zu, das Schutzgut der „persönlichen Freiheit" wird dadurch nicht erweitert.[3] Der Europäische Gerichtshof für Menschenrechte (EGMR) leitet daraus in einer seiner bislang einzigen ausdrücklichen Entscheidung zum „Recht auf Sicherheit" einen gewissen Schutz vor staatlichen Maßnahmen außerhalb des Hoheitsgebietes des handelnden Konventionsstaates ab[4].

Nichts desto trotz ist anzuerkennen, 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. Das bedeutet, dass der Staat für Bedrohungen und Verletzungen der grundrechtlich garantierten Rechtsgüter, die an sich nicht dem Staat zurechenbar sind, dann trotzdem haftet, wenn er keinen angemessenen Schutz gegen Bedrohungen durch „Dritte" geboten hat. Daher ist es letztlich ein Ausfluss dieser staatlichen Schutzpflichten – Hand in Hand mit der Begründung eines grundsätzlichen staatlichen Gewaltmonopols – 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 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, Grundrechtseingriffe müssen in einem angemessenen Verhältnis zu den legitimen Zwecken stehen. Dieser Grundsatz der Verhältnismäßigkeit darf aber nicht zur leeren Formel verkommen. Der Gesetzgeber muss schon 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 gewährt bleibt. Der vorliegende Entwurf gewährt jedoch den „Staatschutzbehörden" umfassende Eingriffsbefugnisse, die ohne Differenzierung zur Verfügung stehen, sobald die Zuständigkeit dieser Behörden begründet ist. Mit anderen Worten verläuft die Abwägungsgrenze für tiefgehende Befugnisse zur verdeckten Überwachung und Ermittlung parallel zur Zuständigkeitsgrenze. Damit wird auch bei den Personen, die für diese Behörden arbeiten, sehr wahrscheinlich ein Selbstverständnis wachsen, wonach es keine Grenzen geben darf, sobald sie sich einer Angelegenheit im Wirkungsbereich annehmen.

Im Zusammenhang mit geheimer Überwachung und elektronischer (Kommunikations-) Datenverarbeitung hat der Verfassungsgerichtshof im VDS Urteil auf den Punkt gebracht, worum es geht: *„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*

[2] Vgl zur Ergänzung der Worte „und Sicherheit", die in der Regierungsvorlage zum PersFrG noch nicht enthalten waren, *Laurer*, Verfassungsänderungen 1988 (1989) 28 f.
[3] *Berka*, Grundrechte, Rz 400 f; *Kopetzki*, in Korinek/Holoubek (Hrsg), Art 1 PersFrG, Rz 17; zur Straßburger Judikatur bis 1996 vgl *Peukert*, in *Frohwein/Peukert*, EMRK², Art 5, Rz 4 f; vgl aus der jüngeren Rsp EGMR 1.6.2004, *Altun*, 24.561/94.
[4] Im Urteil *Öcalan* sah der EGMR das Recht auf Sicherheit durch die Verhaftung *Öcalans* durch türkische Organe in Kenia (ohne dessen Einverständnis) berührt. Vgl *Grabenwarter*, EMRK³, 161, Rz 3.
[5] Urteil des EGMR vom 31.5.2007 im Fall Kontrová gg. die Slowakei (NL 2007, 133).

Informationsbeziehungen (vgl. Berka, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT, 2012, Band I/1, 22). „

Aber Politik und Gesetzgeber haben nichts verstanden.

Ermittler, „Staatschützer“ brauchen Informationen, sie brauchen Erkenntnisse und immer mehr Daten, um Verdächtige aus der schützenswerten Masse der harmlosen Bürgerinnen und Bürger präventiv „herausfiltern“ zu können. Dieses Paradigma und ein geradezu blindes Vertrauen in dessen Erfolg bestimmt die Debatte und wird jedenfalls auf Regierungsebene nicht mehr reflektiert.

Im „Vorblatt“ zum Entwurf des PStSG wird als erstes Ziel definiert:
„ – der Schutz der im Staatsgebiet lebenden Menschen sowie der verfassungsmäßigen Grundordnung“.

Die „im Staatsgebiet lebenden Menschen“ wurden nicht gefragt, ob „sie“ als Preis für ein Mehr an – behaupteter oder tatsächlicher – Sicherheit bezahlte Spitzel in ihrem Umfeld zu akzeptieren bereit sind. Die Menschen wurden auch nicht gefragt, ob sie mit einem Inlandsgeheimdienst einverstanden sind, der gegenüber seiner einzigen Kontrollinstanz – dem Rechtsschutzbeauftragten des BM.I – selbst aussuchen darf, inwieweit deren Akteneinsicht „die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde“ und daher abzulehnen ist (§ 16 Abs. 1 PStSG). Wenn dieser Staat, dieses Gemeinwesen, aber „den im Staatsgebiet lebenden Menschen“ gehört, dann muss einem Gesetz mit derartig weitgehenden Ermächtigungen, insbesondere auch für den Einsatz bezahlter Spitzel, eine gesellschaftliche Debatte vorausgehen – mit offenem Ergebnis.

Und was bedeutet in Österreich „Schutz der verfassungsmäßigen Grundordnung“? Die Republik Österreich, die – lässt man die Nazizeit außer Betracht – nächstes Jahr ihren 100. Geburtstag feiert, war bisher nicht in der Lage, einen eigenen Grundrechtekatalog vorzulegen – im Sinne eines Bekenntnisses: „Das sind wir, das ist Österreich“. Das österreichische B-VG 1920 idF 1929 ist letztlich eine „Spielregelverfassung“, sie legt fest, wie der Staat aufgebaut ist und zu funktionieren hat. Sie repräsentiert kein Menschenbild, kein Wertesystem. Einige Grundrechte stammen noch aus der Monarchie vor allem von 1862 und 1867, dann natürlich die Europäische Menschenrechtskonvention (EMRK), die Grundrechtecharta der EU, verstreute Verfassungsbestimmungen in verschiedenen Gesetzen (zB § 1 Datenschutzgesetzt 2000), aber ein eigenständiger Österreichischer Grundrechtekatalog existiert nicht. Anstrengungen in diese Richtung im Rahmen des „Österreich Konvent“ für eine große Verfassungsreform wurden politisch in der Folge niemals aufgegriffen.

Dem könnte man entgegenhalten: Aber „Österreich ist eine demokratische Republik. Ihr Recht geht vom Volk aus.“ (Art 1 B-VG). Tatsächlich findet derzeit aber in unserer Gesellschaft ein „von oben“ initiierter und gelenkter schleichender Paradigmenwechsel statt, und die Regierung, das Parlament, die „Staatsschützer“ – unsere von uns bezahlten Angestellten – haben nicht bloß vergessen zu fragen, ob wir bereit sind, unsere Freiheit ihrer Staatssicherheit zu opfern. Aber vielleicht ist das unsere eigene Schuld und Alexis de Tocqueville (1805-1859) hatte recht: "*Es ist wirklich schwer einzusehen, wie Menschen, die der Gewohnheit, sich selbst zu regieren, vollständig entsagt haben, imstande sein könnten, diejenigen gut auszuwählen, die sie regieren sollen.*"

Die Folgen dieser geplanten Gesetzgebung im Interesse der „Staatschützer“ sind für den Fall ihrer Realisierung derzeit noch unabsehbar, klar ist aber, dass sie auf Dauer verheerend sein werden. In gesellschaftskritischen Gruppierungen, Menschenrechtsorganisationen, politischen Gruppierungen jenseits des politischen „mainstream“ wird das Misstrauen ein steter Gast werden, in der Gesellschaft wird sich ein Gefühl wie in der untergegangenen DDR ausbreiten.

Massiver Widerstand im Sinne eines Einforderns des gesellschaftlichen Diskurses rund um die Einschränkung gesellschaftlicher Grundrechte kann uns vielleicht nicht vor potentiellen Terroranschlägen retten, aber wir können damit jenes Gut erhalten, auf welches es jeder Terroranschlag abgesehen hat, unser demokratisches Gemeinwesen. Zu spät ist es noch nicht. „*Es ist selten, dass eine Freiheit irgendwelcher Art mit einem Schlage verloren geht*“. (David Hume)

II. Wirkungsorientierte Folgenabschätzung

Auf den ersten Blick erscheint es erfreulich, dass dem Gesetzesvorschlag eine „wirkungsorientierte Folgenabschätzung“ (WFA) zugrunde liegt. Bei Betrachtung des Inhalts der WFA zeigt sich jedoch, 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 lassen. Die Notwendigkeit der Änderungen bzw. Neuerungen wird postuliert aber nicht begründet. An dieser Stelle sei daran erinnert, dass der europäische Gerichtshof (EuGH) ebenso wie der österreichische Verfassungsgerichtshof (VfGH) in den Verhandlungen zur Aufhebung der Vorratsdatenspeicherung (VDS) durch die Fragen der Richterinnen und Richter besonders hervorgehoben haben, dass den rechtspolitischen Entscheidungen zur rechtlichen Ausführung der VDS kein objektiviertes Datenmaterial zugrunde gelegt worden sei und dass auch die Evaluierung keine Einschätzung des Nutzens im Hinblick auf die vorgegebenen Ziele der Bekämpfung von Terrorismus und schwerer (organisierter) Kriminalität zulasse. Aus den Grundrechten, insbesondere der Europäischen Menschenrechtskonvention, die den wichtigsten Teil unseres Grundrechtekatalogs ausmacht, 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 pervertiert diesen liberalen Abwehrcharakter unserer Grundrechte ins Gegenteil und verdächtigt alle, die eine Sphäre ohne staatlichen Einblick als verfassungsrechtlich geschützten Grundzustand reklamieren.

Das deutsche Bundesverfassungsgericht hat in dessen Urteil zur Aufhebung der deutschen nationalen Umsetzung der Vorratsdatenspeicherung den Gedanken ausgeführt, dass eine staatliche Überwachungsmaßnahme bzw. deren Verhältnismäßigkeit nur beurteilt werden kann, wenn man diese in Zusammenschau mit anderen, bereits bestehenden Befugnissen betrachtet. Durch die

Summe aller Eingriffe könne sich ergeben, dass der Spielraum des Gesetzgebers zur Normierung neuer Befugnisse enger wird. Damit beschreibt das dt. Bundesverfassungsgericht im Prinzip die Notwendigkeit einer „Überwachungs-Gesamtrechnung". In eben diesem Geiste steht das AKVorrat Projekt HEAT (Handlungskatalog zur Evaluierung der Anti-Terror Gesetze in Österreich), 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 Herbst 2015 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 *Leitlinien zur Folgenabschätzung*, Europäische Kommission, SEK(2009) 92, ergänzt durch die Vorgaben des Bundeskanzleramts für alle legistischen Projekte als ‚Österreichisches Handbuch „Bessere Rechtsetzung", Bundeskanzleramt (Hrsg.), *Hable, Kunnert, Pürgy,* Wien 2008'. Die dort praxisbezogen und einfach beschriebene Systematik und deren Kriterien sollten schon längst die Standardprozedur für jedes konkrete legistische Vorhaben sein, insbesondere wenn dieses mit Schwerwiegenden und breit gestreuten Grundrechtseingriffen verbunden ist. Die vorliegende „wirkungsorientierte Folgenabschätzung" ist ohne jeden Zweifel nicht auf Basis der systematischen Vorgaben von EU Kommission und Bundeskanzleramt entstanden.

Mit gutem Willen kann man freilich das gegenständliche Begutachtungsverfahren als Initialzündung für einen vorbildlichen Stakeholder-Prozess und eine sachliche öffentliche Debatte sehen. Falls diese Intention dem Begutachtungsverfahren zugrunde liegen sollte, ist der vorliegende Entwurf keine optimale Basis für eine aufgeklärte sachliche Debatte in und mit der Zivilgesellschaft, weil dieser vor allem im Hinblick auf Normenklarheit, Transparenz und Verständlichkeit an schweren Mängeln leidet. So ist beispielsweise der zentrale Begriff des „verfassungsgefährdenden Angriffs" durch eine komplizierte Aufzählung in § 6 PStSG mit unzähligen Verweisen auf Straftatbestände des StGB definiert. Die verwiesenen Normen enthalten teilweise ihrerseits weitere Verweise auf weitere Straftatbestände (zB § 278c StGB mit einer weiteren umfassenden Liste von Straftatbeständen). Dazu kommt, dass eine Kumulation von Befugnissen nach den verschiedenen Regelungen in Strafprozessordnung (StPO), Sicherheitspolizeigesetz (SPG) und Polizeilichem Staatsschutzsgesetz (PStSG) mit überlappenden Anwendungsbereichen vorliegt. Hieraus einen Überblick zu schaffen, der umfassend zeigt, welche Befugnisse zu welchen Straftatbeständen nach welchen Rechtsgrundlagen unter welchen Voraussetzungen zur Verfügung stehen, hat sich im Zuge der Ausarbeitung dieser Stellungnahme als echte „Denksportaufgabe" herausgestellt. Das Team des AKVorrat hat dennoch – oder gerade deshalb – die Mühe auf sich genommen und eine tabellarische Aufstellung (ein „Mapping") ausgearbeitet, mit der die verschiedenen Dimensionen, Unterschiede und Zusammenhänge von Befugnissen und Straftatbeständen im Überblick dargestellt werden. Außerdem haben wir im vorgeschlagenen Text zu § 6 PStSG zu den §§-Verweisen auf die StGB Tatbestände zumindest die Überschriften der jeweiligen Delikte ergänzt, damit man ein erstes Bild davon bekommt, was ein „verfassungsgefährdender Angriff" überhaupt sein soll. Die nachfolgenden Tabellen zeigen jeweils den gesamten Deliktskatalog, der in Summe den „verfassungsgefährdenden Angriff" definiert, und bezieht die einzelnen Delikte auf bestimmte Ermittlungsbefugnisse in den verschiedenen und weitgehend überlappenden Regimen der Strafprozessordnung (StPO), des Sicherheitspolizeigesetzes (SPG) und des Polizeilichen Staatsschutzgesetzes (PStSG). Die Felder der so entstehenden Matrix werden durch Farbcodierung mit einer dritten, semantischen Ebene angereichert, die darüber Auskunft gibt, welche Organe in welcher Funktion unter welchen

Genehmigungsvoraussetzungen zu den verschiedenen Ermittlungsbefugnissen ermächtigt werden. Dadurch entsteht eine Visualisierung von Gemeinsamkeiten und Unterschieden. So fällt etwa sofort auf, dass im Rahmen eines konkreten Strafverfahrens eine Standortdatenermittlung durch Mobiltelefonortung nur eingeschränkt zulässig ist. Mit dieser Visualisierung will der AKVorrat einen nützlichen Beitrag zu einer sachlichen Debatte im Dialog mit der Zivilgesellschaft leisten, insofern als dadurch jene Transparenz befördert wird, die eigentlich dem vorgeschlagenen Gesetz selbst inhärent sein sollte.

Zusammenfassend darf an dieser Stelle vorweggenommen werden, dass der AKVorrat das gesamte vorgeschlagene „Reformpaket“ zur Terrorismusbekämpfung in Österreich sowohl in Hinblick auf dessen Substanz als auch im Hinblick auf dessen systematische Ausarbeitung ablehnt. Soweit in der Folge im „besonderen Teil“ im Einzelnen konkrete Kritik geübt wird, soll daraus nicht abgeleitet werden, dass sich der AKVorrat damit grundsätzlich mit dem Gesetzesvorschlag in der vorliegenden Form „abgefunden“ hat und nur noch um die Details verhandelt. Die spezielle Kritik an unzähligen Stellen des Entwurfs soll vielmehr verdeutlichen, dass das vorgeschlagene Gesetz punktuell und mehr noch als Ganzes Grundrechte verletzen würde und darüber hinaus wegen Unbestimmtheit (Art 18 B-VG) verfassungswidrig wäre.

Der AKVorrat verschließt sich jedoch nicht einem ergebnisoffenen sachlichen Austausch im Rahmen eines (definierten) Stakeholderprozesses zur Findung einer angemessenen Balance von Sicherheit und Freiheit. Grundsätzlich erscheint es dabei richtig, allenfalls notwendige Kompetenzen zur Prävention und Aufklärung „verfassungsgefährdender Angriffe“ aus dem allgemeinen Regime des Sicherheitspolizeigesetzes herauszulösen und eine spezialisierte Behörde damit zu betrauen, anstatt die Kompetenzen über den gesamten Polizeiapparat zu streuen. Welche Kompetenzen aber im Hinblick auf welche Gefährdungslagen bestehen sollen, wie die abstrakte und konkrete Wahrung der Verhältnismäßigkeit aussieht und wie schließlich ein effektiver Rechtsschutz gestaltet werden soll, muss aber auf Basis einer umfassenden Folgenabschätzung und in transparenter Weise erfolgen.

III. Mapping der Delikte zum „verfassungsgefährdenden Angriff“ (§ 6 PStSG) mit Ermittlungsbefugnissen nach StPO, SPG und PStSG

Legende / Farbcodierung:

- unzulässig… keine Rechtsgrundlage oder ausdrücklich verboten
- nur StA + Gericht… Polizei wird im Dienste der Strafjustiz (Kriminalpolizei) aufgrund einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft tätig
- nur StA… Polizei wird im Dienste der Strafjustiz (Kriminalpolizei) aufgrund einer Anordnung der Staatsanwaltschaft tätig
- BVT/LVT… "Staatsschutzorgane" werden auf Basis der (gegenüber der Polizei ausschließlichen) Befugnisse nach dem PStSG tätig
- Polizei + BVT

Tabelle *Delikte/Befugnisse I*

Norm	Bezeichnung	Strafdrohung	"Kleine Rasterfahndung" Datenabgleich § 141 Abs 2 StPO (Abgleich nur Daten von Sicherheits- und Strafverfolgungsbehörden)	"Große Rasterfahndung" Datenabgleich § 141 Abs 3 StPO (Abgleich auch mit privaten/gewerblichen Datenbanken)	Datenabgleich öffentliche Quellen/ Internet (OSINT) § 10 Abs 5 PStSG (?Abgrenzung § 141 (2) StPO?)	Datenabgleich öffentliche Quellen/ Internet (OSINT) § 53 Abs 4 SPG (?Abgrenzung § 141 (2) StPO?)	IP-Adressen (Zugangsdaten) § 76a Abs 2 StPO	IP-Adressen (Zugangsdaten) § 53 Abs 3a SPG	IP-Adressen (Zugangsdaten) § 12 Abs 1 Z 7 PStSG
75	Mord	bis lebenslang							
75	Mord iZ Terror	bis lebenslang							
84	schwere Körperverletzung	bis 3 Jahre							
84	schwere	bis 4,5 Jahre							

	Körperverletzung iZ Terror								
85	Körperverletzung mit schweren Dauerfolgen	bis 5 Jahre							
85	Körperverletzung mit schweren Dauerfolgen iZ Terror	bis 7,5 Jahre							
86	Körperverletzung mit tödlichem Ausgang	bis 10 Jahre							
86	Körperverletzung mit tödlichem Ausgang iZ Terror	bis 15 Jahre							
87	Absichtliche schwere Körperverletzung	bis 5 Jahre							
87	Absichtliche schwere Körperverletzung iZ Terror	bis 7,5 Jahre							
102	Erpresserische Entführung	bis 20 Jahre							
102	Erpresserische Entführung iZ Terror	bis 20 Jahre							
106	schwere Nötigung	bis 5 Jahre							
106	schwere Nötigung iZ Terror	bis 7,5 Jahre							
107 Abs 2	qualifizierte gefährliche Drohung	bis 3 Jahre							
107 Abs 2	qualifizierte	bis 4,5 Jahre							

	gefährliche Drohung iZ Terror								
118a	Widerrechtlicher Zugriff auf ein Computersystem	bis 6 Monate							
118a (3)	Widerrechtlicher Zugriff auf ein Computersystem iZ OK (Kriminelle Vereinigung)	bis 3 Jahre							
119	Verletzung des Telekommunikationsgeheimnisses	bis 6 Monate							
119a	Missbräuchliches Abfangen von Daten	bis 6 Monate							
124	Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses zugunsten des Auslands	bis 3 Jahre							
126	schwere Sachbeschädigung	bis 2 Jahre							
126	schwere Sachbeschädigung iZ Terror	bis 3,5 Jahre							
126a	Datenbeschädigung	bis 6 Monate							
126a (2)	Datenbeschädigung iZ OK (Kriminelle Vereinigung)	bis 5 Jahre							
126a iVm	Datenbeschädigu	bis 9 Monate							

278c	ng iZ OK/Terror								
126b	Störung der Funktionsfähigkeit eines Computersystems	bis 6 Monate							
126b (2)	Störung der Funktionsfähigkeit eines Computersystems iZ OK	bis 5 Jahre							
126c	Missbrauch von Computerprogrammen oder Zugangsdaten	bis 6 Monate							
165 Abs 3	Geldwäscherei iZ OK/Terror	bis 3 Jahre							
169	Brandstifung	bis 10 Jahre							
169	Brandstifung iZ Terror	bis 15 Jahre							
171	Vorsätzliche Gefährdung durch Kernenergie oder ionisierende Strahlen	bis 10 Jahre							
171	Vorsätzliche Gefährdung durch Kernenergie oder ionisierende Strahlen iZ Terror	bis 15 Jahre							
173	Vorsätzliche Gefährdung durch Sprengmittel	bis 10 Jahre							

173	Vorsätzliche Gefährdung durch Sprengmittel iZ Terror	bis 15 Jahre							
175	Vorbereitung eines Verbrechens durch Kernenergie, ionisierende Strahlen oder Sprengmittel	bis 5 Jahre							
175	Vorbereitung eines Verbrechens durch Kernenergie, ionisierende Strahlen oder Sprengmittel iZ Terror	bis 7,5 Jahre							
176	Vorsätzliche Gemeingefährdung	bis 10 Jahre							
176	Vorsätzliche Gemeingefährdung iZ Terror	bis 15 Jahre							
177a	Herstellung und Verbreitung von Massenvernichtungswaffen	bis 10 Jahre							
177a	Herstellung und Verbreitung von Massenvernichtungswaffen iZ	bis 15 Jahre							

	Terror								
177b	Unerlaubter Umgang mit Kernmaterial, radioaktiven Stoffen oder Strahleneinrichtungen	bis 3 Jahre							
177b	Unerlaubter Umgang mit Kernmaterial, radioaktiven Stoffen oder Strahleneinrichtungen iZ Terror	bis 4,5 Jahre							
178	Vorsätzliche Gefährdung von Menschen durch übertragbare Krankheiten	bis 3 Jahre							
178	Vorsätzliche Gefährdung von Menschen durch übertragbare Krankheiten iZ Terror	bis 4,5 Jahre							
180	vorsätzliche Beeinträchtigung der Umwelt	bis 3 Jahre							
180	vorsätzliche Beeinträchtigung der Umwelt iZ Terror	bis 4,5 Jahre							
185	Luftpiraterie	bis 10 Jahre							
185	Luftpiraterie iZ Terror	bis 15 Jahre							

186	vorsätzliche Gefährdung der Sicherheit der Luftfahrt	bis 10 Jahre							
186	vorsätzliche Gefährdung der Sicherheit der Luftfahrt iZ Terror	bis 15 Jahre							
242	Hochverrat	bis 20 Jahre							
244	Vorbereitung eines Hochverrats	bis 10 Jahre							
246	Staatsfeindliche Verbindungen	bis 5 Jahre							
248	Herabwürdigung des Staates und seiner Symbole	bis 1 Jahr							
249	Gewalt und gefährliche Drohung gegen den Bundespräsidenten	bis 10 Jahre							
250	Nötigung eines verfassungsmäßigen Vertretungskörpers, einer Regierung, des Verfassungsgerichtshofs, des Verwaltungsgerichtshofs oder des Obersten Gerichtshofs	bis 10 Jahre							

251	Nötigung von Mitgliedern eines verfassungsmäßigen Vertretungskörpers, einer Regierung, des Verfassungsgerichtshofs, des Verwaltungsgerichtshofs oder des Obersten Gerichtshofs oder des Präsidenten des Rechnungshofs oder des Leiters eines Landesrechnungshofs	bis 5 Jahre							
252	Verrat von Staatsgeheimnissen	bis 10 Jahre							
253	Preisgabe von Staatsgeheimnissen	bis 3 Jahre							
254	Ausspähung von Staatsgeheimnissen	bis 5 Jahre							
256	Geheimer Nachrichtendienst zum Nachteil Österreichs	bis 3 Jahre							
257	Begünstigung feindlicher Streitkräfte	bis 10 Jahre							

258	Landesverräterische Fälschung und Vernichtung von Beweisen	bis 5 Jahre							
274	Landfriedensbruch	bis 2 Jahre							
278 b	Terroristische Vereinigung	bis 15 Jahre							
278 d	Terrorismusfinanzierung	bis 10 Jahre							
278 e	Ausbildung für terroristische Zwecke	bis 10 Jahre							
278 f	Anleitung zur Begehung einer terroristischen Straftat	bis 2 Jahre							
279	Bewaffnete Verbindungen	bis 3 Jahre							
280	Ansammeln von Kampfmitteln	bis 3 Jahre							
282	Aufforderung zu mit Srafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen	bis 2 Jahre							
282a	Aufforderung zu terroristischen Straftaten und Gutheißung terroristischer Straftaten	bis 2 Jahre							
282a	Aufforderung zu terroristischen	bis 3,5 Jahre							

	Straftaten und Gutheißung terroristischer Straftaten iZ Terror								
283	Verhetzung	bis 2 Jahre							
284	Sprengung einer Versammlung	bis 1 Jahr							
285	Verhinderung oder Störung einer Versammlung	bis 6 Monate							
316	Hochverräterische Angriffe gegen einen fremden Staat	bis 5 Jahre							
319	Militärischer Nachrichtendienst für einen fremden Staat	bis 2 Jahre							
320	Verbotene Unterstützung von Parteien bewaffneter Konflikte	bis 5 Jahre							
Verbotsgesetz	Zusammengefasst	Grunddelikte bis 20 Jahre							
7 KMG		bis 3 Jahre							
7 KMG	iZ Terror	bis 4,5 Jahre							
79-82 AußWG	Zusammengefasst	Grunddelikte bis 5 Jahre							
50 WaffenG	Gerichtlich strafbare Handlungen	bis 1 Jahr							
50 WaffenG	Gerichtlich strafbare	bis 1,5 Jahre							

	Handlungen iZ Terror											

Fortsetzung: Tabelle *Delikte/Befugnisse II*

Norm	Bezeichnung	Strafdrohung	Verkehrsdatenauskunft § 135 Abs 2 Z 3 StPO	historische Standortdatenauskunft § 135 Abs 2 Z 3 StPO	gegenwärtige Standortdatenauskunft § 135 Abs 2 Z 3 StPO (Stille SMS- strittig)	Inhaltsüberwachung § 135 Abs 3 Z 3 StPO	gegenwärtige Standortauskunft § 53 Abs 3b SPG (IMSI-Catcher)		Auskünfte "Dienst der Informationsgesellschaft (§ 18 ECG)	Optische & akustische Überwachung von Personen § 136 Abs 1 Z 3 StPO	Optische & akustische Überwachung von Personen § 12 (1) (3) PStSG (ohne Ermittler)	Optische & akustische Überwachung von Personen § 54 (4) SPG (ohne Ermittler)
							Gefährder	Gefährdeter				
75	Mord	bis lebenslang										
75	Mord iZ Terror	bis lebenslang										
84	schwere Körperverletzung	bis 3 Jahre										
84	schwere	bis 4,5										

	Körperverletzung iZ Terror	Jahre											
85	Körperverletzung mit schweren Dauerfolgen	bis 5 Jahre											
85	Körperverletzung mit schweren Dauerfolgen iZ Terror	bis 7,5 Jahre											
86	Körperverletzung mit tödlichem Ausgang	bis 10 Jahre											
86	Körperverletzung mit tödlichem Ausgang iZ Terror	bis 15 Jahre											
87	Absichtliche schwere Körperverletzung	bis 5 Jahre											
87	Absichtliche schwere Körperverletzung iZ Terror	bis 7,5 Jahre											
102	Erpresserische Entführung	bis 20 Jahre											
102	Erpresserische Entführung iZ Terror	bis 20 Jahre											

106	schwere Nötigung	bis 5 Jahre											
106	schwere Nötigung iZ Terror	bis 7,5 Jahre											
107 Abs 2	qualifizierte gefährliche Drohung	bis 3 Jahre											
107 Abs 2	qualifizierte gefährliche Drohung iZ Terror	bis 4,5 Jahre											
118a	Widerrechtlicher Zugriff auf ein Computersystem	bis 6 Monate											
118a (3)	Widerrechtlicher Zugriff auf ein Computersystem iZ OK (Kriminelle Vereinigung)	bis 3 Jahre											
119	Verletzung des Telekommunikationsgeheimnisses	bis 6 Monate											
119a	Missbräuchliches Abfangen von Daten	bis 6 Monate											
124	Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses zugunsten des	bis 3 Jahre											

	Auslands												
126	schwere Sachbeschädigung	bis 2 Jahre											
126	schwere Sachbeschädigung iZ Terror	bis 3,5 Jahre											
126a	Datenbeschädigung	bis 6 Monate											
126a (2)	Datenbeschädigung iZ OK (Kriminelle Vereinigung)	bis 5 Jahre											
126a iVm 278c	Datenbeschädigung iZ OK/Terror	bis 9 Monate											
126b	Störung der Funktionsfähigkeit eines Computersystems	bis 6 Monate											
126b (2)	Störung der Funktionsfähigkeit eines Computersystems iZ OK	bis 5 Jahre											
126c	Missbrauch von Computerprogrammen oder Zugangsdaten	bis 6 Monate											

165 Abs 3	Geldwäscherei iZ OK/Terror	bis 3 Jahre											
169	Brandstifung	bis 10 Jahre											
169	Brandstifung iZ Terror	bis 15 Jahre											
171	Vorsätzliche Gefährdung durch Kernenergie oder ionisierende Strahlen	bis 10 Jahre											
171	Vorsätzliche Gefährdung durch Kernenergie oder ionisierende Strahlen iZ Terror	bis 15 Jahre											
173	Vorsätzliche Gefährdung durch Sprengmittel	bis 10 Jahre											
173	Vorsätzliche Gefährdung durch Sprengmittel iZ Terror	bis 15 Jahre											
175	Vorbereitung eines Verbrechens durch Kernenergie, ionisierende Strahlen oder Sprengmittel	bis 5 Jahre											

175	Vorbereitung eines Verbrechens durch Kernenergie, ionisierende Strahlen oder Sprengmittel iZ Terror	bis 7,5 Jahre											
176	Vorsätzliche Gemeingefährdung	bis 10 Jahre											
176	Vorsätzliche Gemeingefährdung iZ Terror	bis 15 Jahre											
177a	Herstellung und Verbreitung von Massenvernichtung swaffen	bis 10 Jahre											
177a	Herstellung und Verbreitung von Massenvernichtung swaffen iZ Terror	bis 15 Jahre											
177b	Unerlaubter Umgang mit Kernmaterial, radioaktiven Stoffen oder Strahleneinrichtung en	bis 3 Jahre											
177b	Unerlaubter Umgang mit Kernmaterial,	bis 4,5 Jahre											

	radioaktiven Stoffen oder Strahleneinrichtungen iZ Terror											
178	Vorsätzliche Gefährdung von Menschen durch übertragbare Krankheiten	bis 3 Jahre										
178	Vorsätzliche Gefährdung von Menschen durch übertragbare Krankheiten iZ Terror	bis 4,5 Jahre										
180	vorsätzliche Beeinträchtigung der Umwelt	bis 3 Jahre										
180	vorsätzliche Beeinträchtigung der Umwelt iZ Terror	bis 4,5 Jahre										
185	Luftpiraterie	bis 10 Jahre										
185	Luftpiraterie iZ Terror	bis 15 Jahre										
186	vorsätzliche Gefährdung der Sicherheit der	bis 10 Jahre										

	Luftfahrt												
186	vorsätzliche Gefährdung der Sicherheit der Luftfahrt iZ Terror	bis 15 Jahre											
242	Hochverrat	bis 20 Jahre											
244	Vorbereitung eines Hochverrats	bis 10 Jahre											
246	Staatsfeindliche Verbindungen	bis 5 Jahre											
248	Herabwürdigung des Staates und seiner Symbole	bis 1 Jahr											
249	Gewalt und gefährliche Drohung gegen den Bundespräsidenten	bis 10 Jahre											
250	Nötigung eines verfassungsmäßigen Vertretungskörpers, einer Regierung, des Verfassungsgerichtshofs, des Verwaltungsgerichtshofs oder des Obersten	bis 10 Jahre											

	Gerichtshofs											
251	Nötigung von Mitgliedern eines verfassungsmäßigen Vertretungskörpers, einer Regierung, des Verfassungsgerichtshofs, des Verwaltungsgerichtshofs oder des Obersten Gerichtshofs oder des Präsidenten des Rechnungshofs oder des Leiters eines Landesrechnungshofs	bis 5 Jahre										
252	Verrat von Staatsgeheimnissen	bis 10 Jahre										
253	Preisgabe von Staatsgeheimnissen	bis 3 Jahre										
254	Ausspähung von Staatsgeheimnissen	bis 5 Jahre										
256	Geheimer Nachrichtendienst zum Nachteil	bis 3 Jahre										

	Österreichs												
257	Begünstigung feindlicher Streitkräfte	bis 10 Jahre											
258	Landesverräterische Fälschung und Vernichtung von Beweisen	bis 5 Jahre											
274	Landfriedensbruch	bis 2 Jahre											
278 b	Terroristische Vereinigung	bis 15 Jahre											
278 d	Terrorismusfinanzierung	bis 10 Jahre											
278 e	Ausbildung für terroristische Zwecke	bis 10 Jahre											
278 f	Anleitung zur Begehung einer terroristischen Straftat	bis 2 Jahre											
279	Bewaffnete Verbindungen	bis 3 Jahre											
280	Ansammeln von Kampfmitteln	bis 3 Jahre											
282	Aufforderung zu mit Srafe bedrohten	bis 2 Jahre											

	Handlungen und Gutheißung mit Strafe bedrohter Handlungen												
282a	Aufforderung zu terroristischen Straftaten und Gutheißung terroristischer Straftaten	bis 2 Jahre											
282a	Aufforderung zu terroristischen Straftaten und Gutheißung terroristischer Straftaten iZ Terror	bis 3,5 Jahre											
283	Verhetzung	bis 2 Jahre											
284	Sprengung einer Versammlung	bis 1 Jahr											
285	Verhinderung oder Störung einer Versammlung	bis 6 Monate											
316	Hochverräterische Angriffe gegen einen fremden Staat	bis 5 Jahre											
319	Militärischer Nachrichtendienst	bis 2 Jahre											

	für einen fremden Staat												
320	Verbotene Unterstützung von Parteien bewaffneter Konflikte	bis 5 Jahre											
Verbotsgesetz	Zusammengefasst	Grunddelikte bis 20 Jahre											
7 KMG		bis 3 Jahre											
7 KMG	iZ Terror	bis 4,5 Jahre											
79-82 AußWG	Zusammengefasst	Grunddelikte bis 5 Jahre											
50 Waffen G	Gerichtlich strafbare Handlungen	bis 1 Jahr											
50 Waffen G	Gerichtlich strafbare Handlungen iZ Terror	bis 1,5 Jahre											

IV. Zu den einzelnen Bestimmungen

§ 1: Anwendungsbereich; Polizeilicher Staatsschutz

„(1) Dieses Bundesgesetz regelt den polizeilichen Staatsschutz in Ausübung der Sicherheitspolizei.

(2) Der polizeiliche Staatsschutz dient dem Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit sowie von Vertretern ausländischer Staaten, internationaler Organisationen und anderer Völkerrechtssubjekte nach Maßgabe völkerrechtlicher Verpflichtungen, kritischer Infrastruktur und der Bevölkerung vor terroristisch, weltanschaulich oder religiös motivierter Kriminalität, vor Gefährdungen durch Spionage, durch nachrichtendienstliche Tätigkeit und durch Proliferation sowie der Wahrnehmung zentraler Funktionen der internationalen Zusammenarbeit in diesen Bereichen. Hiezu bestehen als Organisationseinheit der Generaldirektion für die öffentliche Sicherheit das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (Bundesamt) und als Organisationseinheit der Landespolizeidirektion in jedem Bundesland ein Landesamt Verfassungsschutz (Landesamt).

(3) Das Bundesamt wird bei Vollziehung dieses Bundesgesetzes für den Bundesminister für Inneres, das Landesamt für die Landespolizeidirektion tätig. Der Bundesminister für Inneres kann bestimmte Angelegenheiten nach Abs. 2 dem Bundesamt vorbehalten.“

Kommentar:

Die Terminologie der Ziel- und Aufgabendefinition wirkt schon wie der Titel des Gesetzes etwas befremdlich: Warum ist vom „Staatsschutz“ die Rede – warum nicht (mehr) vom „Verfassungsschutz“? Offenbar wird der Staat hier ausschließlich institutionell verstanden, was zB § 1 (2) PStSG erkennen lässt: „Der polizeiliche Staatsschutz dient dem Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit (…)“. Verfassungsmäßige Einrichtungen sind nach dem Modell des Entwurfs also solche, die auch eine „Handlungsfähigkeit“ haben, die zu schützen ist. Handlungsfähig können Organisationen, Körperschaften und Institutionen sein, letztlich jede Art juristischer Personen des öffentlichen Rechts. Allerdings haben nicht alle „verfassungsmäßigen Einrichtungen“ eine Handlungsfähigkeit in diesem Sinn. So gehören etwa die Demokratie an sich sowie die verfassungsgesetzlich gewährleisteten Grundrechte ebenso zu den „verfassungsmäßigen Einrichtungen“. Der „Staat“ besteht nicht nur aus dem Apparat der Institutionen, die im Namen des Staates handeln können. Nach der „Reinen Rechtslehre“ von Hans Kelsen, des geistigen Vaters der österreichischen Bundesverfassung (B-VG) ist der Staat normativ gesehen gleichzusetzen mit der gesamten Rechtsordnung, daher insbesondere der Verfassung an deren Spitze. Dazu gehören auch die Grundrechte der Menschen sowie die Prinzipien der Verfassung, etwa das Prinzip der Gewaltenteilung, das liberale Prinzip aus dem Konzept der liberalen Grundrechte oder das demokratische Prinzip. Das dem Entwurf zugrunde liegende Staatsverständnis zeigt, dass der Sicherheitsgedanke völlig überwiegt und der Freiheitsgedanke neuerlich nur am Rande und eher als Lippenbekenntnis eine Rolle spielt.

Der Staat sind letztlich alle Bürgerinnen und Bürger, die im Staatsgebiet leben und durch deren Produktivität und Steuerleistung (das heißt auch über den Fiskalfaktor „Konsum“) die staatlichen Institutionen überhaupt erst geschaffen werden können. Diese Institutionen dienen den Menschen

und sind nicht Selbstzweck. Die Menschen, die den Staat also erst legitimieren, haben garantierte Freiheiten – deren Achtung ebenso Aufgabe einer umfassenden Sicherheitspolitik zu sein hat.

§ 2: Organisation

„(1) Dem Bundesamt steht ein Direktor vor. Dem Direktor kommt die Funktion des Informationssicherheitsbeauftragten nach dem Informationssicherheitsgesetz zu.

(2) Zum Direktor kann nur ernannt werden, wer besondere Kenntnisse auf dem Gebiet des polizeilichen Staatsschutzes aufweist und mindestens fünf Jahre in einem Beruf tätig gewesen ist, in dem der Abschluss des Studiums der Rechtswissenschaften Berufsvoraussetzung ist.

(3) Sonstige Bedienstete des Bundesamtes und der Landesämter haben innerhalb von zwei Jahren nach Dienstbeginn eine spezielle Ausbildung für Verfassungsschutz und Terrorismusbekämpfung zu absolvieren, deren näherer Inhalt durch Verordnung des Bundesministers für Inneres festzusetzen ist.

(4) Sofern es sich bei den Bediensteten nicht bereits um Organe des öffentlichen Sicherheitsdienstes handelt, kann der Generaldirektor für die öffentliche Sicherheit sie nach Absolvierung der Ausbildung (Abs. 3) zur Ausübung von Befehls- und Zwangsgewalt ermächtigen.

(5) Vor Beginn der Tätigkeit muss sich jeder Bedienstete einer Sicherheitsüberprüfung (§ 55 Sicherheitspolizeigesetz - SPG, BGBl. Nr. 566/1991) für den Zugang zu geheimer Information unterziehen. Strebt der Bedienstete eine Leitungsfunktion an, muss er sich einer Sicherheitsüberprüfung für den Zugang zu streng geheimer Information unterziehen. Die Sicherheitsüberprüfungen sind nach drei Jahren zu wiederholen. Bei Vorliegen von Anhaltspunkten, wonach ein Bediensteter nicht mehr vertrauenswürdig sein könnte, ist die Sicherheitsüberprüfung vor Ablauf dieser Frist zu wiederholen."

Kommentar:

In der Organisatorischen Ausgestaltung erscheint interessant, dass zu den Landesämtern zwar Regelungen im Hinblick auf das sonstige Personal normiert werden, anders als beim Bundesamt aber keine Regelungen getroffen werden, wie die Leitung der Landesämter organisiert sein soll. § 1 PStSG normiert zwar den Weisungszug zur jeweiligen Landespolizeidirektion und stellt klar, dass die Landesämter eigene Organisationseinheit sind. Allerdings lässt sich daraus nicht ableiten, wie die Organisation innerhalb dieser Einheiten gestaltet sein soll. Die Frage ist, ob hier möglicherweise ein Problem der Kompetenzverteilung zwischen Bund und Ländern vorliegen könnte. In diesem Falle wäre aber wohl auch § 2 Abs. 3 PStSG ein Problem, wo auch für Bedienstete der Landesämter die Ausbildung grundsätzlich geregelt wird. Von einem Problem der Kompetenzverteilung, die eine umfassende organisatorische Regelung auch der Landesämter durch Bundesgesetz verbieten, ist nicht auszugehen, zumal Art 78a B-VG klarstellt, dass die Landespolizeidirektionen nachgeordnete Behörden des Bundesministers für Inneres sind. Dann ist aber jedenfalls nicht einzusehen, warum nicht zumindest rudimentäre organisatorische Bestimmungen auch für die Landesämter normiert werden.

§ 3: Geschäftsordnung des Bundesamtes

„ Der Direktor hat im Einvernehmen mit dem Generaldirektor für die öffentliche Sicherheit

festzulegen, wem die Genehmigung von Entscheidungen für den Bundesminister für Inneres im Rahmen der Geschäftseinteilung zukommt, in welchen Fällen ihm die Genehmigung vorbehalten ist und wem diese im Fall der Verhinderung obliegt (Geschäftsordnung).“

Kommentar:

Hier ist schon wie zu § 2 zu fragen, weshalb nur das Bundesamt eine Geschäftsordnung haben soll, die Landesämter hingegen nicht. Die Festlegung von Regelungen im Sinne des § 3 PStSG ist schließlich insbesondere aus rechtsstaatlichen Erwägungen wichtig – immerhin geht es darum, auch im Weisungszusammenhang zu den Landesämtern letztlich die politische und rechtliche Verantwortung des Bundesministers bzw. der Bundesministerin für Inneres zu wahren.

§ 4: Bundesamt als Zentralstelle

„ Das Bundesamt erfüllt für den Bundesminister für Inneres folgende zentrale Funktionen:
1. Operative Koordinierungsstelle für jede Form von Angriffen auf Computersysteme 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 Strafgesetzbuch (StGB), BGBl. Nr. 60/1974;
2. Meldestelle für jede Form der Betätigung im nationalsozialistischen Sinn nach dem Verbotsgesetz, StGBl. Nr. 13/1945 (Meldestelle NS-Wiederbetätigung);
3. die Durchführung von Sicherheitsüberprüfungen (§ 55 SPG);
4. die Organisation der Gebäudesicherheit der Zentralstellen des Bundesministeriums für Inneres;
5. die internationale Zusammenarbeit auf dem Gebiet des Staatsschutzes; davon unberührt bleibt die Zusammenarbeit der Landesämter mit benachbarten regionalen Sicherheitsdienststellen.“

Kommentar:

Der grundsätzliche Anknüpfungspunkt für die (nach den Erläuterungen exklusiven) Zuständigkeiten des BVT ist der Schutz der „verfassungsmäßigen Einrichtungen“. Angesichts der tiefgreifenden Kompetenzen für Grundrechtseingriffe gilt daher – über das allgemeine Bestimmtheitsgebot des Art 18 B-VG hinaus – ein strenger Maßstab für die **Bestimmtheit und Klarheit der Normen**, auf deren Basis auch ein Eingriff in Grundrechte unbescholtener Bürger legitim sein soll. **Unbestimmte Rechtsbegriffe** sind mit dieser Anforderung nur schwer vereinbar, daher wäre eine Definition des Begriffs der „**verfassungsmäßigen Einrichtungen**“ dringend geboten. § 4 Z 1 PStSG erweckt mit dem in Klammern gesetzten Verweis auf § 22 Abs. 1 Z 2 SPG zunächst den Eindruck, die Legaldefinition des Begriffes würde sich eben dort finden. Vergebens, denn § 22 Abs. 1 Z 2 SPG lautet:
„Den Sicherheitsbehörden obliegt der besondere Schutz

1. (…)
2. der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit;“

Dieser Verweis ist ein Zirkelschluss und es ist äußerst fragwürdig, welchen normativen Gehalt ein Rechtsanwender diesem Verweis auf das SPG abgewinnen soll.

Gemäß der Einleitung in den Erläuterungen zum Entwurf seien „im zweiten Hauptstück jene Aufgaben taxativ genannt, die ausschließlich diesen Behörden zukommen“. Der Verweis auf § 22 Abs. 1 Z 2 SPG zeigt, dass diese Aussage falsch ist. Diese Bestimmung weist die Aufgabe des besonderen Schutzes „der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit“ den Sicherheitsbehörden (§ 4 SPG) zu. Im Gegensatz zu anderen Bestimmungen des SPG, die nach dem Entwurf aufgehoben werden sollen, weil sie künftig in das Regime des PStSG und damit die ausschließliche Zuständigkeit der „Staatsschutzbehörden“ überführt werden sollen, bleibt diese Aufgabe weiterhin im SPG verankert. Dadurch wird aber das Ziel, diese Aufgaben ausschließlich den „Staatsschutzbehörden“ zu übertragen, jedenfalls verfehlt. Außerdem zeigt der Deliktskatalog des § 6

PStSG mit den Verweisen auf das Strafgesetzbuch, dass dort viele Straftatbestände darunter fallen, deren Vorbeugung mit Sicherheit gleichzeitig in den Schutz der „normalen" Sicherheitspolizei nach den Regeln des SPG fallen – beispielsweise werden die mit dem Verweis auf § 278c StGB einbezogenen Delikte Mord; Körperverletzung; erpresserische Entführung; schwere Nötigung; gefährliche Drohung; schwere Sachbeschädigung; Datenbeschädigung zum „verfassungsgefährdenden Angriff", wenn sie weltanschaulich oder religiös motiviert sind. ZB könne man auch die Überzeugung eines Täters, dass ihm aufgrund seiner Lebensgeschichte nach „den Gesetzen des Karma" mehr zustünde, als die Gesellschaft ihm gibt, als „weltanschauliches" oder gar „religiöses" Motiv für die Verwirklichung einer strafbaren Handlung qualifizieren. Dabei ist praktisch schwer vorstellbar, dass die Sicherheitspolizei in so einem Fall alle Präventionsmaßnahmen sogleich an die „Staatsschutzorgane" abtritt, weil deren ausschließliche Zuständigkeit begründet sein soll. Formal besteht durch die Akzessorietät des „gefährlichen Angriffs" in § 16 SPG zu allen offizial-Vorsatzdelikten des StGB jedenfalls weiterhin die Zuständigkeit der Sicherheitspolizei zur Gefahrenabwehr auch zu jenen Delikten, welche gleichzeitig die Zuständigkeit nach dem PStSG begründen. Lediglich die „erweiterte Gefahrenerforschung" wird zur ausschließlichen Kompetenz der „Staatsschutzorgane".

Fragen im Hinblick auf die Normenklarheit wirft auch der Begriff der „kritischen Infrastrukturen" auf, der im Entwurf mehrmals verwendet wird. Die erstmalige Verwendung dieses Begriffs beinhaltet in Klammern einen Verweis auf (§ 22 Abs. 1 Z 6 SPG), wo sich eine Definition befindet:

„von Einrichtungen, Anlagen, Systemen oder Teilen davon, die eine wesentliche Bedeutung für die Aufrechterhaltung der öffentlichen Sicherheit, die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie, die Verhütung oder Bekämpfung von Katastrophen, den öffentlichen Gesundheitsdienst, die öffentliche Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern oder den öffentlichen Verkehr haben (kritische Infrastrukturen)".

Unklar ist nun, ob durch den Verweis in Klammern auf die Legaldefinition des Begriffs nach § 22 Abs. 1 Z 6 SPG diese Definition auch für das PStSG verbindlich sein soll. Auch die Erläuterungen bieten hier keinen weiteren Hinweis. Allerdings ist davon auszugehen, dass die Definition des § 22 Abs. 1 Z 6 SPG als verbindliche Definition zu verstehen ist, zumal der im Rahmen des aktuelle vorliegenden Begutachtungsentwurfs für ein „Strafrechtsänderungsgesetz 2015"[6] einen Vorschlag enthält, wonach in § 74 Abs. 1 Z 11 Strafgesetzbuch (StGB) der Begriff „kritische Infrastruktur" wortgleich definiert ist. Eine eindeutige Klarstellung im PStSG, dass dies so gemeint ist, wäre jedoch wünschenswert.

§ 5: Anwendbarkeit des Sicherheitspolizeigesetzes

„Soweit in diesem Bundesgesetz nicht Besonderes bestimmt ist, gilt das Sicherheitspolizeigesetz."

Kommentar:

Die Erläuterungen weisen darauf hin, dass sowohl das Bundesamt als auch die Landesämter für Verfassungsschutz nach wie vor Sicherheitsbehörden sind, denen auch die Aufgaben und Befugnisse nach dem SPG zukommen, soweit das PStSG keine besonderen Regelungen normiert. So soll etwa die Aufgabe der Gefahrenabwehr und die damit einhergehenden Befugnisse, die in diesem Bundesgesetz nicht geregelt werden, wie bisher auf Grundlage des SPG erfolgen.

Daraus folgt, dass die Staatsschutzbehörden bei der Erfüllung ihrer Aufgaben in manchen Fällen auf die erweiterten Befugnisse nach dem PStSG zurückgreifen können und in anderen Fällen an die

[6] https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Begut&Dokumentnummer=BEGUT_COO_2026_100_2_1079520.

engeren Grenzen von Sicherheitspolizeigesetz (SPG) und Strafprozessordnung (StPO) gebunden sind. Diese Doppelgleisigkeit kann vor allem dann zu Schwierigkeiten führen, wenn ein Dritter gegenüber den Behörden Auskunftspflichten zu erfüllen hat, die in allen Rechtsgrundlagen vorgesehen sind, aber jeweils unterschiedliche Rechtsschutzvoraussetzungen verlangen. Wenn beispielsweise das BVT Auskünfte über Verkehrsdaten von einem Dienstanbieter nach dem Telekommunikationsgesetz (TKG) begehrt, kann diese Anfrage entweder im Dienste der Strafjustiz nach den Regeln der StPO erfolgen, oder nach der viel großzügigeren Regelung des § 12 Abs. 1 Z 7 PStSG. Im ersten Fall ist eine gerichtlich bewilligte Anordnung der Staatsanwaltschaft beim Anbieter nach TKG vorzulegen, im zweiten Fall hat die „Staatsschutzbehörde“ nur im Innenverhältnis eine Ermächtigung des Rechtsschutzbeauftragten einzuholen, welche dem Anbieter jedoch nicht vorgelegt werden muss – eine sogenannte „Betreiberanordnung“ wie sie § 138 Abs. 3 StPO verlangt ist in SPG und PStSG nicht vorgesehen. Welches Regelwerk richtigerweise anzuwenden wäre, könnte ein Anbieter aber nur beurteilen, wenn er über nähere Informationen zum konkreten, die Anfrage auslösenden Verdacht verfügt. Die „Staatsschutzbehörden“ werden aber in aller Regel keine weiteren Informationen weitergeben, weil ansonsten ja die Staatssicherheit gefährdet sein könnte. Letztlich wird ein Anbieter im Sinne des TKG also bei Verkehrsdatenauskünften insbesondere durch das BVT in der Praxis generell hinnehmen müssen, wenn keine – nach § 138 Abs. 3 StPO ansonsten ausnahmslos geforderten – gerichtlichen Bewilligungen vorgelegt werden.

Die Doppelgleisigkeiten der Aufgabenerfüllung nach SPG/StPO sowie nach PStSG sind ein strukturelles Problem, das eine Dynamik mit großem Missbrauchspotential birgt. Die „Staatsschutzbehörden“ werden nämlich im Kernbereich Ihrer Tätigkeiten überwiegend mit einem Selbstverständnis ausgestattet werden, wonach sie kaum Grenzen der Befugnisse oder „Behinderungen“ durch effektive Rechtsschutzvorkehrungen (wie eine gerichtliche Bewilligung) erfahren. Wenn diese Behörden aber – wie offenbar ausdrücklich vorgesehen – doch auch im Regime von StPO/SPG handeln, sollen sie plötzlich in der Lage sein, dieses Selbstverständnis abzulegen und sich an dieselben Regeln zu halten, wie alle nicht „privilegierten“ Sicherheitsbehörden. Dazu kommt, dass im Zusammenhang mit den nach § 6 PStSG normierten Aufgaben einige Abgrenzungsschwierigkeiten zum Anwendungsbereich von SPG und StPO bestehen, die eine klare Trennung kaum zulassen – dazu jedoch sogleich.

§ 6: Erweiterte Gefahrenerforschung und Schutz vor verfassungsgefährdenden Angriffen

„(1) Dem Bundesamt und den Landesämtern 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 weltanschaulich oder religiös motivierter Gewalt kommt;
2. der vorbeugende Schutz vor wahrscheinlichen verfassungsgefährdenden Angriffen durch eine Person;
3. der Schutz vor verfassungsgefährdenden Angriffen aufgrund von Informationen von Dienststellen inländischer Behörden oder ausländischer Sicherheitsbehörden (§ 2 Abs. 3 Polizeikooperationsgesetz – PolKG, BGBl. I Nr. 104/1997) zu Personen, die im Verdacht stehen, im Ausland einen Sachverhalt verwirklicht zu haben, der einem verfassungsgefährdenden Angriff entspricht.

(2) Ein verfassungsgefährdender Angriff ist die Bedrohung von Rechtsgütern
1. durch die rechtswidrige Verwirklichung des Tatbestandes einer nach §§ 278b (Terroristische Vereinigung), 278c bis 278f (Terroristische Straftaten; Terrorismusfinanzierung; Ausbildung für terroristische Zwecke; Anleitung zur Begehung einer terroristischen Straftat)

oder, soweit es der Verfügungsmacht einer terroristischen Vereinigung unterliegende Vermögensbestandteile betrifft, nach § 165 Abs. 3 StGB (Geldwäscherei) strafbaren Handlung;

2. durch die weltanschaulich oder religiös motivierte rechtswidrige Verwirklichung des Tatbestandes einer nach §§ 279 (Bewaffnete Verbindungen), 280 (Ansammeln von Kampfmitteln), 282 (Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen), 283 (Verhetzung) oder in § 278c StGB genannten strafbaren Handlung (Mord; Körperverletzung; erpresserische Entführung; schwere Nötigung; gefährliche Drohung; schwere Sachbeschädigung; Datenbeschädigung; vorsätzliche Gemeingefährdungsdelikte; vorsätzliche Beeinträchtigung der Umwelt; Luftpiraterie; vorsätzliche Gefährdung der Sicherheit der Luftfahrt; Aufforderung zu terroristischen Straftaten und Gutheißung terroristischer Straftaten; § 50 Waffengesetz; § 7 Kriegsmaterialgesetz);

3. durch die rechtswidrige Verwirklichung des Tatbestandes einer nach §§ 274 (Landfriedensbruch), 284 (Sprengung einer Versammlung) und 285 StGB (Verhinderung oder Störung einer Versammlung), nach dem vierzehnten bis sechzehnten Abschnitt des StGB (Hochverrat, Vorbereitung eines Hochverrats, Staatsfeindliche Verbindungen, Herabwürdigung des Staates und seiner Symbole, Gewalt und gefährliche Drohung gegen den Bundespräsidenten; Nötigung eines verfassungsmäßigen Vertretungskörpers, einer Regierung, des Verfassungsgerichtshofs, des Verwaltungsgerichtshofs oder des Obersten Gerichtshofs; Nötigung von Mitgliedern eines verfassungsmäßigen Vertretungskörpers, einer Regierung, des Verfassungsgerichtshofs, des Verwaltungsgerichtshofs oder des Obersten Gerichtshofs oder des Präsidenten des Rechnungshofs oder des Leiters eines Landesrechnungshofs; Verrat von Staatsgeheimnissen; Preisgabe von Staatsgeheimnissen; Ausspähung von Staatsgeheimnissen; Geheimer Nachrichtendienst zum Nachteil Österreichs; Begünstigung feindlicher Streitkräfte; Landesverräterische Fälschung und Vernichtung von Beweisen) oder nach dem Verbotsgesetz strafbaren Handlung;

4. durch die rechtswidrige Verwirklichung des Tatbestandes einer nach §§ 175 (Vorbereitung eines Verbrechens durch Kernenergie, ionisierende Strahlen oder Sprengmittel), 177a (Herstellung und Verbreitung von Massenvernichtungswaffen), 177b StGB (Unerlaubter Umgang mit Kernmaterial, radioaktiven Stoffen oder Strahleneinrichtungen), §§ 79 bis 82 Außenwirtschaftsgesetz 2011 (AußWG 2011), BGBl. I Nr. 112/2011, § 7 Kriegsmaterialgesetz (KMG), BGBl. Nr. 540/1977, sowie nach §§ 124 (Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses zugunsten des Auslands), 316 (Hochverräterische Angriffe gegen einen fremden Staat), 319 (Militärischer Nachrichtendienst für einen fremden Staat) und 320 StGB (Verbotene Unterstützung von Parteien bewaffneter Konflikte) strafbaren Handlung;

5. durch die rechtswidrige Verwirklichung des Tatbestandes einer nach §§ 118a (Widerrechtlicher Zugriff auf ein Computersystem), 119 (Verletzung des Telekommunikationsgeheimnisses), 119a (Missbräuchliches Abfangen von Daten), 126a (Datenbeschädigung), 126b (Störung der Funktionsfähigkeit eines Computersystems) und 126c StGB (Missbrauch von Computerprogrammen oder Zugangsdaten) strafbaren Handlung gegen verfassungsmäßige Einrichtungen und ihre Handlungsfähigkeit (§ 22 Abs. 1 Z 2 SPG) sowie kritische Infrastrukturen (§ 22 Abs. 1 Z 6 SPG).“

Kommentar:

Der vorgeschlagene § 6 PStSG enthält die wesentlichen Definitionen der Aufgaben sowie des damit verbundenen Begriffes des „verfassungsgefährdenden Angriffs“. Diese Norm ist für die den gesamten Gesetzesvorschlag von zentraler Bedeutung, weil der die Kompetenzgrenzen und Handlungsspielräume der „Staatschutzorgane“ bestimmt. Die folgende Analyse betrachtet die

Regelungen vor allem unter zwei Aspekten: Einerseits geht es um die Frage der Bestimmtheit bzw. Klarheit für alle Rechtsadressaten[7], andererseits lässt sich erst durch eine genauere Analyse der – durch das materielle Strafrecht determinierten – Kompetenzreichweite in einem ersten Ansatz beurteilen, wie es um die Verhältnismäßigkeit der Mittel in Bezug auf die konkreten Zwecke zumindest abstrakt bestellt ist.

Vorbemerkung zur Normenklarheit:

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[8])“.

Im Folgenden wird gezeigt, warum die zentralen Bestimmungen des § 6 PStSG in mehrfacher Hinsicht und konkret große Bedenken im Hinblick auf die Verständlichkeit und Transparenz des gesamten Entwurfs mit sich bringt. Darüber hinaus werden jeweils auch die Aspekte der Verhältnismäßigkeit analysiert.

Ad Absatz 1 (erweiterte Gefahrenerforschung):

Die Erläuterungen zu § 6 PStSG führen aus, dass sich die erweiterte Gefahrenerforschung im Hinblick auf Gruppierungen – die nach dem Entwurf vollständig aus dem SPG in das PStSG überführt werden sollen – in der Praxis bewährt habe. Der an Staatssicherheit interessierte Staatsbürger vermisst an dieser Stelle dann aber jeglichen Hinweis auf Nachweise, Berichte oder Statistiken, auf welche die Annahme der Bewährung des Instruments in der Praxis gestützt wird. Außerdem dräng sich die Frage auf, warum zur Erfüllung des Aufgabenbereichs „erweiterte Gefahrenerforschung von Gruppierungen“ die Notwendigkeit für erweiterte Befugnisse nach den Vorschlägen des 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.
In der Sache betrifft die Kritik an der „erweiterten Gefahrenerforschung“ als solche schon die geltende Rechtslage, also den

Gemäß Ziffer 2 obliegen dem Bundesamt und den Landesämtern *„der vorbeugende Schutz vor wahrscheinlichen verfassungsgefährdenden Angriffen durch eine Person“.* Der – jedenfalls vom BM.I intendierte – Bedeutungsgehalt dieser Bestimmung erschließt sich erst durch die begleitende Lektüre der Erläuterungen zu § 6 des Entwurfs: *„Mit dem vorliegenden Entwurf soll die bisherige Aufgabe der erweiterten Gefahrenerforschung bei Einzelpersonen im vorbeugenden Schutz von Rechtsgütern angesiedelt werden, eingeschränkt auf wahrscheinliche Angriffe, die verfassungsgefährdend sind.“* Demnach soll diese Bestimmung als (modifizierter) Ersatz für die derzeitige Regelung zur „erweiterten Gefahrenerforschung“ in Bezug auf Einzelpersonen nach § 21 Abs. 3 Z 1 SPG dienen.

[7] Dieser Begriff wird hier als (bessere) Alternative synonym zum geläufigen Begriff der „Rechtsunterworfenen“ verwendet.

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

Ohne die erläuternden Ausführungen würden die Verfasser dieser Stellungnahme auch als erfahrene Juristen nicht auf die Idee kommen, dass *„der vorbeugende Schutz vor wahrscheinlichen verfassungsgefährdenden Angriffen durch eine Person“* gleichzusetzen ist mit „der Beobachtung einer Person“ iSd § 21 Abs. 3 Z 1 SPG. Offenbar geht der Entwurf davon aus, dass *„der vorbeugende*[9] *Schutz vor wahrscheinlichen verfassungsgefährdenden Angriffen“* automatisch rechtfertigt, die Personen, von denen der „wahrscheinliche Angriff“ mutmaßlich ausgeht systematisch zu beobachten. Wenn diese Annahme richtig wäre, würde sich aber die Frage stellen, warum dann notwendig ist, die Beobachtung von Personengruppen, von denen mutmaßlich eine gleichartige Gefahr ausgeht, ausdrücklich in § 6 Abs. 1 Z 1 PStSG zu normieren.

Außerdem ist das Kriterium eines „wahrscheinlichen“ verfassungsgefährdenden Angriffs zu hinterfragen. Nach den Erläuterungen muss „ein begründeter Gefahrenverdacht bestehen, dass der Betroffene einen verfassungsgefährdenden Angriff in absehbarer Zeit begehen werde. Wahrscheinlich bedeutet dabei mehr als die bloße Möglichkeit oder Nichtausschließbarkeit eines Angriffes, aber weniger als mit Gewissheit zu erwarten (vgl. Hauer/Keplinger, SPG[4], § 22 Anm 10.1)“. Im Gegensatz zur Abwehr einer konkreten Gefahr bietet die Anknüpfung an einen „wahrscheinlichen“ Angriff wesentlich mehr Spielraum. Noch weiter abstrahiert von einer konkreten Gefahr werden die Befugnisse der „Staatsschutzorgane“ dadurch, dass einige der wesentlichen Delikte im Aufgabenbereich schon die Verlagerung der Strafbarkeit in den Vorbereitungsbereich verlagern wollen. In diesem Sinn ist die Mitgliedschaft zu einer kriminellen Organisation (§ 278a) oder zu einer terroristischen Organisation (§ 278b) unabhängig davon strafbar, ob der Täter darüber hinaus an einer konkreten Rechtsgutverletzung schuldhaft mitgewirkt hat oder nicht. Dabei werden die Befugnisse nicht erst bei einer bestimmten Wahrscheinlichkeit ausgelöst, sondern stehen gemäß § 11 PStSG schon „zum Zweck der Bewertung der Wahrscheinlichkeit“ zur Verfügung (vgl. dazu auch den Kommentar zu § 11 unten).

Die Dimension des mit diesem unbestimmten Begriff verbundenen Problems lässt sich erst in Zusammenschau mit den konkreten Straftatbeständen, die in Absatz 2 den **„verfassungsgefährdenden Angriff“** definieren, beurteilen. Dies soll anhand eines (zur Beurteilung des Absatz 2 vorweggenommenen **Beispiels** anschaulich gemacht werden:

Gemäß § 6 Abs. 2 Z 3 PStSG stellt auch die **„Verhinderung oder Störung einer Versammlung“** im Sinne des **§ 285 StGB** einen verfassungsgefährdenden Angriff dar. Der Straftatbestand des § 285 StGB lautet folgendermaßen:

*„**Verhinderung oder Störung einer Versammlung***
***§ 285.** Wer eine nicht verbotene Versammlung dadurch verhindert oder erheblich stört, daß er*

1. *den Versammlungsraum unzugänglich macht,*
2. *eine zur Teilnahme berechtigte Person am Zutritt hindert oder ihr den Zutritt erschwert oder ihr die Teilnahme an der Versammlung durch schwere Belästigungen unmöglich macht oder erschwert,*
3. *in die Versammlung unbefugt eindringt oder*
4. *eine zur Leitung oder Aufrechterhaltung der Ordnung berufene Person verdrängt oder sich einer ihrer auf den Verlauf der Versammlung bezüglichen Anordnungen tätlich widersetzt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.“*

Als bekanntes Beispielszenario ist hier etwa an den „Wiener Akademikerball“ zu denken, der als Nachfolgeveranstaltung des „Wiener Korporations-Balls“ (auch Ball des Wiener Korporationsrings oder kurz WKR-Ball) gilt, der von 1952 bis 2012 jährlich von farbentragenden und mehrheitlich schlagenden Hochschulkorporationen ausgerichtet wurde. Diese Veranstaltung wird nach dem

[9] Tautologie: der Schutz vor einem in der Zukunft liegenden Angriff ist immer vorbeugend.

Impressum ihrer Internetseite (www.wiener-akademikerball.at) von Landesgruppe Wien der Freiheitlichen Partei Österreichs (FPÖ) organisiert, das heißt dem Ball kommt über den reinen Unterhaltungsfaktor hinaus eine politische Dimension zu, die sich auch in der alljährlichen polarisierten öffentlichen Auseinandersetzung mit dieser Veranstaltung zeigt. Der Ball könnte daher rechtlich durchaus als Versammlung qualifiziert werden, welche den Schutz des § 285 StGB genießt. Gleichzeitig ist hinreichend bekannt, dass diese Veranstaltung seit vielen Jahren massive politische Gegendemonstrationen mit sich ziehen, die sowohl von politisch links ausgerichteten Gruppen als auch von Einzelpersonen ohne Organisationshintergrund mitgetragen werden. Nach der Definition des § 6 Abs. 2 Z 3 PStSG in Verbindung mit § 285 StGB könnte eine Gegendemonstration – die schon per se beabsichtigt, die Ausrichtung der „Versammlung“ zumindest zu erschweren – daher naheliegend als „verfassungsgefährdender Angriff“ qualifiziert werden, der die erweiterten Befugnisse des „Staatsschutzorgane“ aktiviert.
Der Verdacht, dass eine bestimmte Person „wahrscheinlich“ an einem solchen „verfassungsgefährdender Angriff“ mitwirkt, könnte sich zB aus der Ermittlung personenbezogener Daten „aus allen anderen verfügbaren Quellen (…), insbesondere durch Zugriff etwa auf im Internet öffentlich zugängliche Daten“ ergeben. Wenn sich eine Person etwa in einem öffentlich zugänglichen Internetforum (zB zur online-Berichterstattung einer Tageszeitung) kritisch zu der genannten Veranstaltung äußert und möglicherweise im sozialen online-Netzwerk dieser Person (zB Facebook) öffentlich erkennbar Personen befinden, die (amtsbekannt) an früheren Demonstrationen gegen diese Veranstaltung teilgenommen haben, ist die geforderte Wahrscheinlichkeit wohl gegeben. Die Konsequenz daraus wäre, dass die Person im Beispiel zulässigerweise einer systematischen Beobachtung durch das BVT ausgesetzt wäre.

Ad Absatz 2 (Definition des „verfassungsgefährdenden Angriffs“):

Die Ausweitung der Befugnisse der „Staatsschutzorgane“ zur Erfüllung der Aufgaben der inneren Sicherheit steht „in einem Spannungsverhältnis“ zum „verfassungsmäßig garantierten Schutz des Individuums“, wie schon in den Erläuterungen zum Entwurf im zweiten Absatz der Einleitung eingeräumt wird. Damit gehen – wie schon oben zu § 4 ausgeführt – besondere Anforderungen an die Bestimmtheit und Klarheit der Normen einher.

Das Transparenzproblem des vorliegenden Entwurfs besteht vor allem darin, dass schon die Legaldefinition des Aufgabenbereichs der „Staatsschutzorgane“ durch dynamische Verweise auf StGB Delikte erfolgt, wobei nicht einmal Überschriften genannt werden, um zumindest ein erstes Bild zu zeichnen. Dazu kommt das weitere Problem der verschachtelten Verweise, zB von § 6 PStSG auf § 278c StGB, der seinerseits aus einer komplexen Liste von Straftaten mit Veränderung der Strafdrohungen bei bestimmten Begehungsform besteht. Selbst für erfahrene Juristen ist es letztlich einigermaßen aufwendig, den substantiellen Bedeutungsgehalt der wichtigsten Normen zu erschließen. Die Technik der Verweise wird dabei von einer Reihe unbestimmter aber zentraler Rechtsbegriffe begleitet, zB in § 6 PStSG die „weltanschaulich motivierte“ Begehung von Straftaten oder die „schwere Gefahr“ für die öffentliche Sicherheit, bei der unklar bleibt, wie sich diese von einer nicht schweren Gefahr unterscheiden lassen soll.

Schließlich ist nicht nachvollziehbar, nach welchen Kriterien der Deliktskatalog zusammengestellt wurde, wenn man sich einige der Delikte betrachtet, die als „verfassungsgefährdender Angriff“ definiert werden – zB Verhinderung oder Störung einer Versammlung (§ 285 StGB) oder (gemäß § 6 Abs. 2 Z 2 PStSG iVm § 278c StFG) jede „weltaunschaulich oder religiös motivierte“ Gefährliche Drohung (§ 107 StGB) oder Körperverletzung (§ 84 StGB), um nur zwei konkrete Beispiele zu nennen. Das würde bedeuten, dass jede mit gefährlichen Drohungen verbundene Auseinandersetzung oder gar Rangelei mit Verletzungsfolgen im Wirtshaus einen „verfassungsgefährdenden Angriff“ darstellt, wenn sich der Streit ursprünglich etwa um eine Debatte zur Wehrpflicht oder zur Steuerreform

entzündet hat, weil hier mit großer Wahrscheinlichkeit verschiedene Weltanschauungsmodelle die Emotionalität und das „Eskalationspotential“ einer Debatte bestimmen.

§ 7: Polizeilich staatsschutzrelevante Beratung

„ (1) Dem Bundesamt und den Landesämtern obliegt zur Vorbeugung verfassungsgefährdender Angriffe, insbesondere auf dem Gebiet der Cybersicherheit, die Förderung der Bereitschaft und Fähigkeit des Einzelnen, sich über eine Bedrohung seiner Rechtsgüter Kenntnis zu verschaffen und Angriffen entsprechend vorzubeugen.

(2) Darüber hinaus obliegt es dem Bundesamt und den Landesämtern, Vorhaben, die der Vorbeugung verfassungsgefährdender Angriffe dienen, zu fördern.“

Kommentar:

Dem Bundesamt und den Landesämtern für Verfassungsschutz wird mit dem Verweis auf „Cybersicherheit“ in § 7 eine Aufgabe übertragen, deren Dimension äußerst weitreichend ist. Grundsätzlich sind Ansätze zu begrüßen, mit denen die Bewusstseinsbildung und die Fertigkeiten zu erhöhter „Cybersicherheit“ vor allem im Kontext mit dem Schutz kritischer Infrastruktur der Republik gefördert werden. Allerdings ist eine gewisse Vorsicht geboten, wenn die Behörden, die allenfalls dafür zuständig ist, Bürger und somit auch deren informationstechnische Systeme zu überwachen, gleichzeitig in Umfassender Weise für „Cybersicherheit“ zuständig sind. Das sind durchaus gegenläufige Interessen und hier könnten sich Interessenkonflikte ergeben, insbesondere im Hinblick auf Maßnahmen zum Schutz der Vertraulichkeit der Kommunikation der Bürger, zumal beispielsweise auch die Betreiber von Telekommunikations- und Internetzugangsdiensten als Teil der kritischen Infrastruktur gelten. In dieser Hinsicht ist daher problematisch, dass weder Absatz 1 noch Absatz 2 der Bestimmung erkennen lassen, ob damit auch allenfalls operative Befugnisse verbunden sein sollen und ob auf der anderen Seite möglicherweise Mitwirkungspflichten begründet werden sollen, die den „Staatsschutzorganen“ Zugriffe bis in den Kern der internen kritischen Infrastruktur betroffener Organisationen und Unternehmen gewähren könnten.

Schließlich enthalten weder der Normtext noch die Erläuterungen einen Hinweis auf das Verhältnis zu und die Kooperation mit den wichtigsten Stellen in diesem Aufgabengebiet, insbesondere der „C4“ Cybercrime-Spezialeinheit des Bundeskriminalamts oder dem „Computer Emergency Response Team“ der Republik (gov-CERT). Gerade was den (bi-direktionalen) Austausch von Informationen betrifft, wären in der praktischen Arbeit zur Cybersicherheit oft klare Rechtsgrundlagen höchst wünschenswert.

§ 8: Information verfassungsmäßiger Einrichtungen

„(1) Dem Bundesamt und den Landesämtern obliegen zur Information verfassungsmäßiger Einrichtungen die Analyse und Beurteilung von staatsschutzrelevanten Bedrohungslagen, die sich auch aus verfassungsgefährdenden Entwicklungen im Ausland ergeben können, sofern nicht der Vollziehungsbereich des Bundesministers für Landesverteidigung und Sport betroffen ist.

(2) Der Bundesminister für Inneres hat über staatsschutzrelevante Bedrohungen den Bundespräsidenten, die Präsidenten des Nationalrates, den Vorsitzenden und die stellvertretenden

Vorsitzenden des Bundesrates sowie die anderen Mitglieder der Bundesregierung zu unterrichten, soweit dies für die Wahrnehmung der gesetzlichen Aufgaben in deren Zuständigkeitsbereich oder für die Wahrung des Ansehens des Bundespräsidenten, des Nationalrates, des Bundesrates oder der Bundesregierung von Bedeutung ist.

(3) Der Landespolizeidirektor hat über staatsschutzrelevante Bedrohungen den Landeshauptmann und die Präsidenten des Landtages zu unterrichten, soweit dies für die Wahrnehmung der gesetzlichen Aufgaben in deren Zuständigkeitsbereich oder für die Wahrung des Ansehens des Landeshauptmannes, der Landesregierung oder des Landtages von Bedeutung ist."

§ 9: Aufgabenbezogenheit

„ Personenbezogene Daten dürfen vom Bundesamt und den Landesämtern gemäß diesem Hauptstück nur verwendet werden, soweit dies zur Erfüllung der ihnen übertragenen Aufgaben erforderlich ist. Ermächtigungen nach anderen Bundesgesetzen bleiben unberührt."

Kommentar:

Die Erforderlichkeit im Hinblick auf die gesetzlichen Aufgaben adressiert den – im Datenschutz zentralen – Zweckbindungsgrundsatz, der sich auch allgemein aus § 6 Datenschutzgesetz (DSG 2000) eindeutig ergibt. Darüber hinaus muss eine zulässige Datenverarbeitung aber auch notwendig (im Sinne des gelindesten Mittels) und vor allem Verhältnismäßig sein. Der Grundsatz der Verhältnismäßigkeit erfordert in jedem Einzelfall eine Prüfung, zwischen Mittel und Zweck noch eine angemessene Relation steht. Angesichts der tiefgehenden Eingriffsbefugnisse erscheint es erstaunlich, dass im gesamten Entwurf zum PStSG nur ein einziges Mal auf das Kriterium der Verhältnismäßigkeit (mit Verweis auf § 29 SPG) Bezug genommen wird, und zwar konkret im Zusammenhang mit Eingriffen in die Privatsphäre durch die Verwendung privater Videoaufzeichnungen gemäß § 10 Abs. 4 PStSG. Weil nur an dieser einzigen Stelle die Verhältnismäßigkeit erwähnt wird, entsteht der Eindruck, dass sie auch nur in diesem Zusammenhang beachtlich sei. Wenn die allgemeine Beachtung des Verhältnismäßigkeitsgrundsatzes selbstverständlich wäre, hätte sie der Gesetzgeber auch in § 29 SPG nicht normieren müssen.

§ 10: Ermittlungsdienst für Zwecke des polizeilichen Staatsschutzes

„ (1) Das Bundesamt und die Landesämter dürfen personenbezogene Daten ermitteln und weiterverarbeiten für
1. die erweiterte Gefahrenerforschung (§ 6 Abs. 1 Z 1);
2. den vorbeugenden Schutz vor wahrscheinlichen verfassungsgefährdenden Angriffen (§ 6 Abs. 1 Z 2);
3. den Schutz vor verfassungsgefährdenden Angriffen aufgrund von Informationen von Dienststellen inländischer Behörden oder ausländischer Sicherheitsbehörden (§ 6 Abs. 1 Z 3);
4. die Information verfassungsmäßiger Einrichtungen (§ 8).

(2) Das Bundesamt und die Landesämter dürfen Daten, die sie in Vollziehung von Bundes- oder Landesgesetzen verarbeitet haben, für die Zwecke des Abs. 1 ermitteln und weiterverarbeiten. Ein automationsunterstützter Datenabgleich im Sinne des § 141 Strafprozessordnung (StPO), BGBl. Nr. 631/1975, ist davon nicht umfasst. Bestehende Übermittlungsverbote bleiben unberührt.

(3) Das Bundesamt und die Landesämter 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) Das Bundesamt und die Landesämter 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 § 12 sind das Bundesamt und die Landesämter 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."

Kommentar:

Zu Absatz 1 (Zwecke der Datenverarbeitung):

Die Definition der Zwecke für eine rechtmäßige Datenverarbeitung der verschiedensten Kategorien personenbezogener Daten, darunter gemäß § 11 Abs. 1 PStSG ausdrücklich auch sensible Daten im Sinne des § 4 Z 2 Datenschutzgesetz (DSG 2000), ist praktisch mit der Definition der Aufgaben der „Staatsschutzorgane" gleichgesetzt. Diese Bestimmung ist gemeinsam mit der in § 11 Abs. 1 PStSG folgenden Zweckbindung zu lesen. Demzufolge ist die Verarbeitung der dort aufgelisteten personenbezogenen Daten zu Verdächtigen sowie zu Kontakt- und Begleitpersonen sowie zu Informanten und schließlich von tat- und fallbezogenen Informationen zum Zweck der **„Bewertung der Wahrscheinlichkeit** einer Gefährdung sowie zum Erkennen von Zusammenhängen und Strukturen **mittels operativer oder strategischer Analyse**" 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.

zu Absatz 2 bis 5 (Weiterverarbeitung der ermittelten Daten)

Zunächst wird in Absatz 2 die Befugnis zur Datenverarbeitung ausdrücklich einschränkend von der „Rasterfahndung" abgegrenzt (automationsunterstützter Datenabgleich im Sinne des § 141 Strafprozessordnung). 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 *„durch Zugriff etwa auf im Internet öffentlich zugängliche Daten"* kann nun durch Menschen erfolgen, die systematisch im Internet nach bestimmten Schlagworten „das Internet" 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 heutigen einfachen „Google-Suche" damals nicht einmal im Ansatz vorstellbar waren. Die ersten

Suchmaschinen damals[10] waren außerdem nicht nur viel weniger komplex, auch die Größenordnung der verfügbaren Datenmenge war um etliche 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 Person im Netz wiederzufinden, wäre das aus damaliger Sicht schon für sich eine „Superrasterfahndung" gewesen.

Nun ist aber anzunehmen, dass moderne Ermittlungstechnologien auch den österreichischen Verfassungsschützern zur Verfügung stehen sollen. Hierzu gibt es einen großen Markt privater Anbieter für Tools 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.

Nach dem Vorschlag des § 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 (vg. § 12 PStSG). All diese Daten dürfen dann – wohl auch in Verbindung mit den „im Internet" ermittelten Daten – gemeinsam weiterverarbeitet werden. Es drängt sich daher die Frage auf, 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 wir eigentlich nicht so genau wissen, 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 des AKVorrat 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.

§ 11: Datenanwendung

„ (1) Das Bundesamt und die Landesämter dürfen zum Zweck der Bewertung der

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

Wahrscheinlichkeit einer Gefährdung sowie zum Erkennen von Zusammenhängen und Strukturen mittels operativer oder strategischer Analyse
1. zu Betroffenen einer Aufgabe nach § 6 Abs. 1 Z 1 bis 3
a) Namen,
b) frühere Namen,
c) Aliasdaten,
d) Namen der Eltern,
e) Geschlecht,
f) Geburtsdatum und Ort,
g) Staatsangehörigkeit,
h) Wohnanschrift/Aufenthalt,
i) sonstige zur Personenbeschreibung erforderliche Daten,
j) Dokumentendaten,
k) Beruf und Qualifikation/Beschäftigung/Lebensverhältnisse,
l) sachbezogene Daten zu Kommunikations- und Verkehrsmittel sowie Waffen einschließlich Registrierungsnummer/Kennzeichen,
m) erkennungsdienstliche Daten und
n) Informationen über wirtschaftliche und finanzielle Verhältnisse einschließlich damit im Zusammenhang stehender Daten juristischer Personen,
2. zu Verdächtigen eines verfassungsgefährdenden Angriffs die Datenarten nach Z 1 a) bis n),
3. zu Kontakt- oder Begleitpersonen, die nicht nur zufällig mit Personen nach Z 1 oder Z 2 in Verbindung stehen und bei denen ausreichende Gründe für die Annahme bestehen, dass über sie Informationen zu diesen Personen beschafft werden können, die Datenarten nach Z 1 a) bis l) bis zur möglichst rasch vorzunehmenden Klärung der Beziehung zu diesen Personen, sowie
4. zu Informanten und sonstigen Auskunftspersonen die Datenarten nach Z 1 a) bis j),
sowie tat- und fallbezogene Informationen und Verwaltungsdaten verarbeiten, auch wenn es sich um besonders schutzwürdige Daten im Sinne des § 4 Z 2 Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999, handelt.

(2) Die Datenanwendung darf als Informationsverbundsystem zwischen dem Bundesamt und den Landesämtern geführt werden. Daten gemäß Abs. 1 Z 1, 2 und 4 sind längstens nach fünf Jahren, Daten gemäß Abs. 1 Z 3 bei Wegfall der ausreichenden Gründe für die Annahme nach dieser Ziffer, längstens aber nach fünf Jahren zu löschen. Bei mehreren Speicherungen nach derselben Ziffer bestimmt sich die Löschung nach dem Zeitpunkt der letzten Speicherung. Übermittlungen sind an Sicherheitsbehörden für Zwecke der Sicherheitspolizei und Strafrechtspflege, an Staatsanwaltschaften und ordentliche Gerichte für Zwecke der Strafrechtspflege, an Dienststellen inländischer Behörden, soweit dies eine wesentliche Voraussetzung zur Wahrnehmung einer ihr gesetzlich übertragenen Aufgabe ist, sowie an ausländische Sicherheitsbehörden entsprechend den Bestimmungen über die internationale polizeiliche Amtshilfe zulässig.

(3) Die Daten sind vor der Verarbeitung in der Datenanwendung auf ihre Erheblichkeit und Richtigkeit zu prüfen sowie während der Verarbeitung zu aktualisieren. Erweisen sich Daten als unrichtig, dann sind diese richtigzustellen oder zu löschen, es sei denn, die Weiterverarbeitung von Falschinformationen mit der Kennzeichnung „unrichtig“ ist zur Erfüllung des Zwecks (Abs. 1) erforderlich. Bei Einstellung von Ermittlungen oder Beendigung eines Verfahrens einer Staatsanwaltschaft oder eines Strafgerichtes sind die Daten durch Anmerkung der Einstellung oder Verfahrensbeendigung und des bekannt gewordenen Grundes zu aktualisieren.

(4) Jede Abfrage und Übermittlung personenbezogener Daten ist so zu protokollieren, dass eine Zuordnung der Abfrage oder Übermittlung zu einem bestimmten Organwalter möglich ist. Die Protokollaufzeichnungen sind drei Jahre aufzubewahren und danach zu löschen.“

Kommentar:

Zu Absatz 1 (Zweck der Datenverarbeitung):

Im Vergleich zur hier vorgeschlagenen Regelung verlang die entsprechende Befugnis nach dem Sicherheitspolizeigesetz (SPG) noch einen konkreten Zusammenhang mit einer bestimmten Gefahrensituation im Sinne eines gefährlichen Angriffs (§ 16 SPG), wenn also die Verwirklichung einer konkreten gerichtlich strafbaren Handlung (keine reinen Privatanklagedelikte) droht. Auch für die „Erweiterte Gefahrenerforschung nach § 21 Abs. 3 SPG ist die Voraussetzung, dass *„damit zu rechnen ist, dass es zu mit schwerer Gefahr für die öffentliche Sicherheit verbundener Kriminalität, insbesondere zu weltanschaulich oder religiös motivierter Gewalt kommt“.* Das bedeutet, die daran anknüpfenden Befugnisse zur (verdeckten) Ermittlung und Verarbeitung von personenbezogenen Daten erfordern als Voraussetzung, dass schon ein bestimmter und konkreter Verdacht besteht (Arg. „damit zu rechnen ist“ (…) „schwerer Gefahr“).

Im Gegensatz dazu reicht für die Aktivierung der Befugnisse nach dem PStSG schon aus, dass die Zielsetzung der Behörde darin besteht, die „Wahrscheinlichkeit einer Gefährdung“ (§ 11 Abs. 1 PStSG) beurteilen zu können. Mit anderen Worten: Wenn ein Risikoszenario im Hinblick auf einen „verfassungsgefährdenden Angriff“ (zB § 285 StGB: Verhinderung oder Störung einer Versammlung) durch die Organwalter abstrakt identifiziert wird, stehen alle (verdeckten und offenen) Ermittlungsbefugnisse zur Verfügung, um herauszufinden, wie wahrscheinlich die Realisierung dieses Risikos (zB die Verhinderung einer Versammlung durch eine Gegendemonstration) ist. Dieser Zusammenhang mit einer konkreten Gefährdungslage ist sehr weit, faktisch bedeutet das, dass der Entwurf von abstrakten Risikoszenarien durch die „Staatsschutzorgane“ selbst den Handlungsspielraum bestimmt.
Das daraus resultierende Problem soll mit einem weiteren Beispiel aus der Praxis (vgl. OGH vom 16.12.2010, 13Os130/10g und 13Os136/10i) veranschaulicht werden.

ORF Dokumentation „Am Schauplatz – am rechten Rand“:

Nach dem Sachverhalt bestand der Verdacht, ein Jugendlicher habe am 12. März 2010 in Wiener Neustadt im Zuge von Dreharbeiten für die vom ORF ausgestrahlte Fernsehreportage „Am Schauplatz - Am rechten Rand“ bei einer Wahlkampfveranstaltung der F***** vor laufender Kamera „Sieg Heil“ gerufen. Das Film- und Tonmaterial war daraufhin über Anordnung der Staatsanwaltschaft Wiener Neustadt – gegen den Willen der Redaktion zu diesem Beitrag – sichergestellt worden. Weitere Ermittlungen hätten auch gegen einen weiteren Jugendlichen den Verdacht ergeben, „vor laufender Kamera sowie anwesenden Mitgliedern des Produktionsteams und mehreren Bekannten die rechte Hand zum Hitlergruß erhoben und dazu ‚Sieg Heil’ oder ‚Heil Hitler’“ gerufen zu haben. Außergewöhnlich war in diesem Fall nun die Annahme der Ermittlungsbehörde, der leitende Redakteur dieser Dokumentation stehe im Verdacht, er habe „die ‚Protagonisten’ seines Beitrags“ „mehrfach - und zwar keineswegs beschränkt auf den 12. 3. 2010 - zu verbotsgesetzrelevanten Handlungen und Äußerungen vor laufender Kamera zu bestimmen versucht“.

Bemerkenswert an diesem Beispiel ist der – zunächst sogar gelungene – Versuch der Strafverfolgungsbehörden, das gemäß § 31 Mediengesetz absolut geschützte Redaktionsgeheimnis zu umgehen. Die Staatsanwaltschaft berief sich nämlich darauf, dass § 144 Abs 3 erster Satz StPO eine Durchbrechung dieses Geheimnisschutzes dann zulässt, wenn die durch § 31 MedienG geschützten Personen selbst als Beschuldigte 'der Tat dringend verdächtig' sind. Beim Oberlandesgericht Wien hielt diese Argumentation noch Stand und die an sich geschützten Redaktionsmaterialien mussten herausgegeben werden. Erst der Oberste Gerichtshof entschied im

Rahmen eines außerordentlichen Rechtsbehelfs[11], dass die Sicherstellung eine unzulässige Verletzung des Redaktionsgeheimnisses darstelle und dadurch die Meinungsfreiheit nach Artikel 10 EMRK verletzt wurde. Der OGH hob hervor, dass das Oberlandesgericht einen ***dringenden*** Tatverdacht gegen den Journalisten gar nicht angenommen hatte. Die gesellschaftliche Bedeutung des Redaktionsgeheimnisses hob der OGH in seiner Entscheidungsbegründung mit Nachweisen aus der Rechtsprechung hervor:
„Sicherstellung von einem Medium recherchierten Materials stellt einen Eingriff in das Grundrecht auf Freiheit der Meinungsäußerung nach Art 10 Abs 1 MRK dar, ist doch der Schutz der Vertraulichkeit journalistischer Quellen eine der Grundbedingungen der Pressefreiheit und bildet somit einen wesentlichen Bestandteil der konventionsrechtlichen Garantie. Ohne solchen Schutz könnten Quellen abgeschreckt werden, Medien dabei zu unterstützen, die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren („chilling effect"). Dies könnte zur Folge haben, dass die lebenswichtige öffentliche Funktion der Medien als „Wachhund" („public watchdog") beeinträchtigt und ihre Fähigkeit, präzise und verlässliche Informationen zu bieten, nachteilig berührt werden (EGMR 27. 3. 1996 [Große Kammer], Nr 17488/90, Goodwin gg Vereinigtes Königreich, ÖJZ 1996/28 [MRK]; 15. 12. 2009, Nr 821/03, Financial Times ua gg Vereinigtes Königreich, uva)."

Mit Blick auf dieses Beispiel wird das grundrechtliche Problem der Ermittlungsbefugnisse nach dem PStSG besser sichtbar. Praktisch könnte bei jeder Bild- oder Tonaufnahme, die einen Verstoß gegen das Verbotsgesetz dokumentiert, die Möglichkeit bestehen, dass jemand hinter der Kamera die sichtbaren Personen zu solchem Handeln angehalten hat und daher selbst als Bestimmungstäter (§ 12, 2. Fall StGB) oder zumindest als Beitragstäter (§ 12, 3. Fall StGB) in Verdacht steht, einen „verfassungsgefährdenden Angriff" (vgl. § 6 Abs. 2 Z 3 PStSG) begangen zu haben. Wenn es sich wie im ORF Beispiel um ein durch § 31 MedienG geschütztes Medium handelt, muss nach der zitierten Judikatur des OGH ein „dringender Verdacht" vorliegen. Dafür wäre laut OGH „darzulegen gewesen, welche bestimmten Tatsachen die hohe Wahrscheinlichkeit einer Sachverhaltsannahme des Inhalts rechtfertigen", der Redakteur habe die mutmaßlichen unmittelbaren Täter solcherart zu Äußerungen[12] veranlassen wollen, diese zur Erfüllung des Tatbestands nach § 3g Verbotsgesetz notwendige Eignung also nicht nur (wertend) erkannt, sondern sich auch damit abgefunden. Nur dann dürfen auf Basis von § 144 Abs. 3 StPO Ermittlungsmaßnahmen gesetzt werden, die auch das Redaktionsgeheimnis unterwandern – was insbesondere auch für verdeckte Ermittlungen und Eingriffe in das Kommunikationsgeheimnis gilt.

Diese nach der Judikatur strengen Voraussetzungen der StPO sollen den „Staatsschutzorganen" nach dem vorgeschlagenen PStSG nicht im Wege stehen. Vielmehr könnten die Befugnisse schon „zum Zweck der Bewertung der Wahrscheinlichkeit einer Gefährdung" (§ 11 PStSG) aktiviert werden. Effektive Rechtsschutzinstrumente – wie im Beispiel der „Erneuerungsantrag" nach § 363a StPO an den OGH – gibt es hier jedoch keine. Die Betroffenen werden vom Eingriff höchstwahrscheinlich (und nach den Vorschlägen rechtlich zulässig) nichts erfahren und wären darauf angewiesen, dass der Rechtsschutzbeauftragte den kommissarischen Rechtsschutz wahrnimmt – falls er davon erfährt. Zu den strukturellen Rechtsschutzproblemen im Detail weiter unten.

<u>zu Absatz 2 (Löschungsfrist):</u>

Die Ermittlungsbefugnisse nach dem PStSG sind in vielerlei Hinsicht zu weitgehend und unverhältnismäßig. Daher kann aus Sicht des AKVorrat auch nicht beurteilt werden, inwiefern 5 Jahre eine angemessene Aufbewahrungsfrist darstellen, zumal unseres Erachtens in vielen Fällen schon die Datenerhebungsbefugnis verfassungswidrig ist. Auffällig ist aber jedenfalls, dass gleichzeitig eine

[11] Einem sogenannten „Erneuerungsantrag" nach § 363a StPO, ein durch die Judikatur des OGH geschaffenes Instrument zur raschen Wahrnehmung von Grundrechtsverletzungen.

[12] Gemäß OGH nämlich solche mit der Eignung, (zumindest) eine der spezifischen Zielsetzungen der NSDAP zu neuem Leben zu erwecken oder zu propagieren (Lässig in WK2 VG § 3g Rz 4).

Diskrepanz zur Löschungsfrist für die Protokollierung der Datenverwendung durch bestimmte Organwalter besteht – solche Protokollaufzeichnungen sind nämlich gemäß § 11 Abs. 4 sowie gemäß § 59 Abs 2 SPG nach drei Jahren zu löschen.

§ 12: Besondere Bestimmungen für die Ermittlungen

„ (1) Zur erweiterten Gefahrenerforschung (§ 6 Abs. 1 Z 1) und zum vorbeugenden Schutz vor wahrscheinlichen verfassungsgefährdenden Angriffen (§ 6 Abs. 1 Z 2) ist die Ermittlung personenbezogener Daten unter den Voraussetzungen des § 15 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 zu Betroffenen nach § 11 Abs. 1 Z 1 lit. l verarbeitet werden;
5. Einholen von Auskünften nach §§ 53 Abs. 3a Z 1 bis 3 und 53 Abs. 3b SPG zu Betroffenen einer Aufgabe nach § 6 Abs. 1 Z 1 und Z 2 sowie zu deren Kontakt- oder Begleitpersonen (§ 11 Abs. 1 Z 3) von Betreibern öffentlicher Telekommunikationsdienste (§ 92 Abs. 3 Z 1 Telekommunikationsgesetz 2003 - TKG 2003, BGBl. I Nr. 70/2003) und sonstigen Diensteanbietern (§ 3 Z 2 E-Commerce-Gesetz - ECG, BGBl. I Nr. 152/2001), wenn die Erfüllung der Aufgabe durch Einsatz anderer Ermittlungsmaßnahmen aussichtslos wäre;
6. Einholen von Auskünften von Beförderungsunternehmen 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 Betroffenen einer Aufgabe nach § 6 Abs. 1 Z 1 und 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. Im Übrigen ist die Ermittlung 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.“

Kommentar:

Zu Absatz 1 (Besondere Ermittlungsbefugnisse):

Observation nach § 54 Abs. 2 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 der IMSI-Catcher adressiert, der ebenso zur Unterstützung von Observationen eingesetzt wird.

Die in § 12 Abs. 1 Z 2 PStSG vorgesehene verdeckte Ermittlung besteht sowohl nach § 53 Abs. 3 SPG als auch nach § 131 StPO. Auffällig ist, dass die Strafprozessordnung deutlich strenger ist, was die Zulässigkeitsvoraussetzungen betrifft. Nach der StPO muss die Maßnahme von der Staatsanwaltschaft höchsten für einen Zeitraum von 3 Monaten angeordnet werden. Dem gegenüber kann die Ermächtigung des Rechtsschutzbeauftragten für eine verdeckte Ermittlung nach dem PStSG jeweils für einen Zeitraum von 6 Monaten erteilt werden.

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

§ 12 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:

§ 12 PStSG – Besondere Bestimmungen für die Ermittlungen	**§ 54 SPG – Besondere Bestimmungen für die Ermittlung**
§ 12 (1) Zur erweiterten Gefahrenerforschung (§ 6 Abs. 1 Z 1) und zum vorbeugenden Schutz vor wahrscheinlichen verfassungsgefährdenden Angriffen (§ 6 Abs. 1 Z 2) ist die Ermittlung personenbezogener Daten unter den Voraussetzungen des § 15 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 (4) SPG ausdrücklich normierten Einschränkung aber in der Abgrenzung von der Befugnis nach § 136 Strafprozessordnung (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 § 12 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 (für den Fall, dass der Entwurf in der vorliegenden Fassung zum Gesetz würde) 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 § 12 Abs. 1 Z 3 PStSG besteht – zumal die StPO diese Befugnis an deutlich strengere Voraussetzungen und auch Rechtschutzvorkehrungen knüpft.

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 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. Mit § 12 Abs. 1 Z 7 PStSG wird mit dieser alten „Tradition", dass umfassende Eingriffe in das Kommunikationsgeheimnis mit Richtervorbehalt ausgestattet sind, gebrochen.

In der Rechtssprechung und Literatur ist die Meinung zunehmend verbreitet, dass auch Verkehrsdaten vom Schutz des Fernmeldegeheimnisses gemäß Art 10a StGG erfasst sind[13], 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.

[13] 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);

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

Dieses Verständnis des Schutzbereiches war in der Vergangenheit nicht unumstritten, ist jedoch unter Berücksichtigung des Schutzzwecks des Grundrechts die einzige im Ergebnis zufriedenstellende Interpretation: Verkehrsdaten erlauben regelmäßig Rückschlüsse auf den Inhalt von Nachrichten (z.B. hilfe@anonyme-alkoholiker.at als Adressat einer E-Mail, Anruf bei einem psychosozialen Beratungsdienst) und können – bis zu einem gewissen Grad, insbesondere vom Durchschnittsanwender – nicht „vermieden" oder verschleiert werden. Im Gegensatz dazu besteht beim „klassischen" Brief immer die Möglichkeit, Nachrichten nach außen hin anonym zu übermitteln, indem z.B. auf dem Briefumschlag kein Absender angegeben wird. Aus diesem Grund war eine völlige Gleichstellung der Verkehrsdaten mit den „äußeren Kommunikationsdaten" eines Briefes schon zum Zeitpunkt der Entstehung des Art. 10a 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 Beispiel regelmäßiger Kontakt zu Fachärzten für Onkologie auf eine Krebserkrankung hin, häufiger Kontakt zu bestimmten Uhrzeiten auf Freundschaften bzw. Arbeitskollegen usw.

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

Schließlich ist anzumerken, dass die Auskunftsbefugnisse im Hinblick auf Verkehrsdaten in der vorgeschlagenen Form auch formal unzulänglich sind, weil diese nicht einmal im Ansatz mit den einschlägigen Bestimmungen des Telekommunikationsgesetzes (TKG) akkordiert sind. § 99 Abs. 1 TKG normiert ausdrücklich, dass die Verwendung (= Verarbeitung und Übermittlung, § 4 DSG) von Verkehrsdaten nur zulässig ist, wenn diese im TKG selbst zumindest dem Grunde nach vorgesehen ist. Aus diesem Grund enthält die Aufzählung des § 99 Abs. 5 TKG dann auch die Verweise auf die einschlägigen Bestimmung von SPG und StPO. Diese Vorschrift dient nach den Erläuterungen zum TKG ausdrücklich der Transparenz gegenüber TKG-Anbietern und deren Kunden – ansonsten müsste ein Datensubjekt nämlich die gesamte Rechtsordnung kennen, um eine Vorstellung davon zu erhalten, wer nach welchen Rechtsgrundlagen Zugriff auf seine/ihre personenbezogenen Verbindungsdaten bekommen darf. Diese abschließende Aufzählung lässt sich auch nicht mit dem Argument umgehen, dass § 12 PStSG (dann) die jüngere/neuere Norm wäre (sog. „lex-posterior Regel"), weil § 99 TKG das Kommunikationsgeheimnis des § 93 TKG näher ausgestaltet und insofern jedenfalls die speziellere Norm darstellt (sog. „lex-specialis Regel"). Damit verbunden ist auch die Frage der organisatorischen und technischen Abwicklung von Auskünften über Kommunikationsdaten gem. § 12 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[14] 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. Hier ist auch anzumerken, dass ein Kernproblem des § 12 PStSG schon darin besteht, dass die nach § 15 PStSG einzuholende Ermächtigung des Rechtsschutzbauftragten einen rein internen Verwaltungsakt darstellt, bei dem ein zur Auskunft verpflichteter Anbieter nicht kontrollieren kann, ob er eingehalten wurde. Der Gesetzgeber der Strafprozessordnung hat erkannt, dass die Publizität des Rechtsschutzes gegenüber dem Anbieter eine enorm wichtige Funktion bei der Verhinderung von Missbrauch hat, weshalb § 138 Abs. 3 StPO ausdrücklich verlangt, die gerichtliche Bewilligung der sogenannten „Betreiberanordnung“ anzuschließen. Demgegenüber müsste sich ein verpflichteter Betreiber bei Auskunftsersuchen nach dem PStSG stets darauf verlassen, dass die Ermächtigung des RSB eingeholt wurde – eine (wenn auch gekürzte) Ausfertigung für den Betreiber ist nicht vorgesehen.

§ 13: Vertrauenspersonenevidenz

„ (1) Das Bundesamt ist ermächtigt, personenbezogene Daten von Menschen, die ihm Informationen zur Erfüllung der Aufgabe der erweiterten Gefahrenerforschung (§ 6 Abs. 1 Z 1), des vorbeugenden Schutzes vor wahrscheinlichen verfassungsgefährdenden Angriffen (§ 6 Abs. 1 Z 2), zur Abwehr gefährlicher Angriffe oder krimineller Verbindungen (§ 21 Abs. 1 SPG) gegen Zusage einer Belohnung weitergeben, zu verarbeiten. Soweit dies zur Verhinderung von Gefährdungen der Betroffenen und zur Bewertung der Vertrauenswürdigkeit der Informationen unbedingt erforderlich ist, dürfen auch sensible und strafrechtsbezogene Daten über die Betroffenen verarbeitet werden.

(2) Das Bundesamt darf sonstigen Sicherheitsbehörden über die in der Evidenz verarbeiteten personenbezogenen Daten nur Auskunft erteilen, wenn diese die Daten für die Abwehr gefährlicher Angriffe oder krimineller Verbindungen (§ 21 Abs. 1 SPG) oder zum vorbeugenden Schutz von Leben, Gesundheit oder Freiheit (§ 22 Abs. 2 SPG) der in Abs. 1 genannten Menschen benötigen. Eine Auskunftserteilung an andere Behörden ist unzulässig. Anzeigepflichten nach der StPO bleiben unberührt.

(3) Jede Verwendung der gemäß Abs. 1 verarbeiteten personenbezogenen Daten ist zu protokollieren. Die Daten sind spätestens zehn Jahre nach der letzten Information zu löschen.“

Kommentar:

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 hält. Allerdings mangelt es hierzu schon an formalen Begründungspflichten im Rahmen effektiver begleitender

[14] 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.

Sicherungsmechanismen zur Wahrung des Rechtsschutzes. Hierzu wäre nicht nur eine richterliche Kontrolle wünschenswert, notwendig wäre überdies ein detaillierter Katalog von Zulässigkeitsvoraussetzungen und Begründungspflichten. Solche „Saveguards" 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.[15]

Ein System staatlich bezahlter Spitzel birgt hier zunächst auch das Problem der Zurechnung zum Staat: Wenn V-Mann bezahlt wird, muss sich der Staat dessen Handlungen (zB 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.[16] In so einem Fall wird man den V-Mann regelmäßig als Zeugen benötigen. Allerdings gibt es keine Rechtsgrundlage, auf der ein Gericht das BM.I zwingen kann, die Identität eines V-Manns oder eines verdeckten Ermittlers offen zu legen. Auch wird ein solcher „Spitzel" häufig eine wichtige Rolle im Beweisverfahren in der Hauptverfahren 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 VE 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.[17]

Aus diesen Gründen sollten 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 Gesetzesentwurf und die Erläuterungen zeigen nicht einmal ansatzweise, dass die beschriebenen Herausforderungen bedacht und reflektiert wurden.

§ 14: Pflicht zur Richtigstellung und Löschung

[15] 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.

[16] 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.

[17] 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.

„(1) Wird festgestellt, dass unrichtige oder entgegen den Bestimmungen dieses Bundesgesetzes ermittelte Daten aufbewahrt werden, so ist unverzüglich eine Richtigstellung oder Löschung vorzunehmen. Desgleichen sind personenbezogene Daten zu löschen, sobald sie für die Erfüllung der Aufgabe, für die sie verwendet worden sind, nicht mehr benötigt werden, es sei denn, für ihre Löschung wäre eine besondere Regelung getroffen worden.

(2) In den Fällen des § 10 Abs. 1 Z 1 und 2 sind die Daten zu löschen, wenn sich nach Ablauf der Zeit, für die die Ermächtigung dazu erteilt wurde, keine Aufgabe für das Bundesamt und die Landesämter stellt. Die unverzügliche Löschung kann jedoch unterbleiben, wenn in Hinblick auf die Person oder Gruppierung aufgrund bestimmter Tatsachen erwartet werden kann, dass sie neuerlich Anlass zu einer Aufgabe nach § 6 Abs. 1 Z 1 oder 2 geben wird. Das Bundesamt und die Landesämter haben solche Daten, wenn sie sechs Monate unverändert geblieben sind, daraufhin zu prüfen, ob sie nicht gemäß Abs. 1 richtig zu stellen oder zu löschen sind. Wenn sich zwei Jahre nach Ablauf der Zeit, für die die Ermächtigung dazu erteilt wurde, keine Aufgabe für das Bundesamt und die Landesämter 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.“

§ 15: Rechtsschutzbeauftragter

„(1) Dem Rechtsschutzbeauftragten (§ 91a SPG) kommt der besondere Rechtsschutz bei den Aufgaben nach § 6 Abs. 1 Z 1 und Z 2 zu.

(2) Das Bundesamt und die Landesämter, denen sich eine Aufgabe gemäß § 6 Abs. 1 Z 1 und Z 2 stellt, haben vor der Durchführung der Aufgabe die Ermächtigung des Rechtsschutzbeauftragten im Wege des Bundesministers für Inneres einzuholen. Dasselbe gilt, wenn beabsichtigt ist, besondere Ermittlungsmaßnahmen nach § 12 zu setzen oder gemäß § 10 Abs. 4 ermittelte Daten weiterzuverarbeiten. Jede Einholung einer Ermächtigung ist entsprechend zu begründen. Eine Ermächtigung darf nur für die Dauer von höchstens sechs Monaten erteilt werden; Verlängerung ist zulässig.“

§ 16: Rechte und Pflichten des Rechtsschutzbeauftragten

„(1) Das Bundesamt und die Landesämter haben dem Rechtsschutzbeauftragten bei der Wahrnehmung seiner Aufgaben jederzeit Einblick in alle erforderlichen Unterlagen und Aufzeichnungen 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 und Unterlagen über die Identität von Personen oder über Quellen, deren Bekanntwerden die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde, und für Abschriften (Ablichtungen), wenn das Bekanntwerden der Information die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde.

(2) Dem Rechtsschutzbeauftragten ist jederzeit Gelegenheit zu geben, die Durchführung der in § 15 Abs. 2 genannten Maßnahmen zu überwachen und alle Räume zu betreten, in denen Aufnahmen oder sonstige Überwachungsergebnisse aufbewahrt werden. Darüber hinaus hat er im Rahmen seiner Aufgabenstellungen die Einhaltung der Pflicht zur Richtigstellung oder Löschung nach § 14 oder den besonderen Löschungsbestimmungen zu überwachen.

(3) Der Rechtsschutzbeauftragte erstattet dem Bundesminister für Inneres jährlich bis spätestens 31. März einen Bericht über seine Tätigkeit und Wahrnehmungen im Rahmen seiner Aufgabenerfüllung nach diesem Bundesgesetz.“

Kommentar:

§ 16 Abs. 1 zweiter Satz lässt die gesamte Rechtsschutzkonstruktion durch den RSB des BM.I wie ein Kartenhaus zusammenfallen. Demzufolge können die „Staatsschutzorgane" nämlich gegenüber ihrem (einzigen) Rechtsschutzorgan jederzeit den Umfang der Kontrolle beschränken, wenn sie behaupten, dass *„deren Bekanntwerden die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde"*. Abgesehen davon, dass diese unbestimmte Einschränkung ein Transparenzproblem ist (wann ist die Sicherheit von Menschen gefährdet), wird dadurch der RSB de facto entmachtet, weil er nicht unbedingt alle Unterlagen erhalten muss, die er zur Beurteilung der Verhältnismäßigkeit und Zulässigkeit der Mittel brauch würde. Damit wird der „Verfassungsschutz" zum echten Geheimdienst. Interessant ist jedenfalls die offenbar der Ausnahme zugrunde liegende Annahme, dass der Rechtsschutzbeauftragte des BM.I nicht vertrauenswürdig genug ist, um ihm volle Akteneinsicht zu geben.

Abgesehen davon, dass schon die Akteneinsicht des Rechtsschutzbeauftragten geradezu willkürlich beschränkt werden darf, hält der AKVorrat hier auch weiterhin die Grundsatzkritik an der Konzeption des Rechtsschutzes durch die konkrete Ausgestaltung des RSB aufrecht. Diskutierte werden sollte etwa die Frage, ob die für den gesamten Polizeibereich zentrale Kontrollfigur auch mit hinreichenden Unabhängigkeitsgarantien ausgestattet ist. Der Rechtsschutzbeauftragte (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. Weiters wird er von der Exekutive bestellt, nämlich vom Bundespräsidenten auf Vorschlag der Bundesregierung (§ 91a Abs 2 SPG), die Präsidenten des Nationalrats sowie der Höchstgerichte haben im Zuge der Bestellung lediglich Anhörungsrechte. Die persönlichen Qualifikationsvoraussetzungen entsprechen auch nicht jenen eines unabhängigen[18] Richters (vgl. § 91b Abs 1 SPG). Der RSB entspricht daher nicht den vom EGMR geforderten Kriterien einer unabhängigen Kontrollinstanz. Schließlich besteht das praktisch schwerwiegendste Problem darin, dass die Einrichtung des Rechtsschutzbeauftragten nicht einmal annähernd ausreichend ausgestattet ist, um einen effektiven kommissarischen Rechtsschutz zu bieten. Selbst wenn eine Ermittlungsmaßnahme nur aufgrund einer Ermächtigung des RSB zulässig ist (wie zB nach § 12 PStSG), muss diese Ermächtigung allenfalls verpflichteten Dritten (zB Telekom-Anbieter) gegenüber nicht offen gelegt werden. 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), einem Referenten und einer Sekretariatsstelle. 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. 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. gg Österreich) anhängig ist. Es besteht eine hohe Chance und jedenfalls große Hoffnung, dass ein Urteil dazu noch im Jahr 2015 ergehen wird.[19]

§ 17: Information Betroffener

[18] http://www.bmi.gv.at/cms/BMI_Rechtsschutzbeauftragter/personen/start.aspx.

[19] Anlass war die SPG Novelle 2007 und ein dagegen an den Verfassungsgerichtshof gerichteter Individualantrag, ausgearbeitet von Ewald Scheucher und Christof Tschohl; dieses Verfahren war gewissermaßen die „Vorübung" der beiden zur erfolgreichen Anfechtung der Vorratsdatenspeicherung.

„(1) Nimmt der Rechtsschutzbeauftragte wahr, dass durch Verwenden personenbezogener Daten Rechte von Betroffenen verletzt worden sind, die von dieser Datenverwendung keine Kenntnis haben, so ist er zu deren Information oder, sofern eine solche aus den Gründen des § 26 Abs. 2 DSG 2000 nicht erfolgen kann, zur Erhebung einer Beschwerde an die Datenschutzbehörde nach § 90 SPG verpflichtet. In einem solchen Verfahren vor der Datenschutzbehörde ist auf § 26 Abs. 2 DSG 2000 über die Beschränkung des Auskunftsrechtes Bedacht zu nehmen.

(2) Nach Ablauf der Zeit, für die die Ermächtigung erteilt wurde, ist der Betroffene vom Bundesoder Landesamt über Grund, Art und Dauer sowie die Rechtsgrundlage der gesetzten Maßnahmen zu informieren. Über die durchgeführte Information Betroffener ist der Rechtsschutzbeauftragte in Kenntnis zu setzen.

(3) Die Information kann mit Zustimmung des Rechtsschutzbeauftragten aufgeschoben werden, solange durch sie die Aufgabenerfüllung gefährdet wäre, und unterbleiben, wenn der Betroffene bereits nachweislich Kenntnis erlangt hat, die Information des Betroffenen unmöglich ist oder aus den Gründen des § 26 Abs. 2 DSG 2000 nicht erfolgen kann.“

§ 18: Berichte über den polizeilichen Staatsschutz

„(1) Das Bundesamt hat jährlich einen Bericht zu erstellen, mit dem die Öffentlichkeit, unter Einhaltung von gesetzlichen Verschwiegenheitspflichten, über aktuelle und mögliche staatsschutzrelevante Entwicklungen informiert wird.

(2) Über die Erfüllung der Aufgaben nach diesem Bundesgesetz sowie über die Information Betroffener nach § 17 hat der Bundesminister für Inneres dem ständigen Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit jedenfalls halbjährlich zu berichten.

(3) Den Bericht des Rechtsschutzbeauftragten gemäß § 16 Abs. 3 hat der Bundesminister für Inneres dem ständigen Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit im Rahmen des Auskunfts- und Einsichtsrechtes nach Art. 52a Abs. 2 B-VG zugänglich zu machen.“

§ 19: Inkrafttreten

„(1) Dieses Bundesgesetz tritt mit 1. Jänner 2016 in Kraft.

(2) Verordnungen auf Grund dieses Bundesgesetzes können bereits ab dem auf seine Kundmachung folgenden Tag erlassen werden; sie dürfen jedoch frühestens mit dem Inkrafttreten dieses Bundesgesetzes in Kraft gesetzt werden.“

§ 20: Sprachliche Gleichbehandlung

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

§ 21: Verweisungen

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

§ 22: Übergangsbestimmungen

„(1) Vor Inkrafttreten dieses Bundesgesetzes erteilte Ermächtigungen gemäß § 91c Abs. 3 SPG in der Fassung vor Inkrafttreten dieses Bundesgesetzes gelten als Ermächtigungen gemäß § 15 Abs. 2 und bleiben bis zum festgesetzten Zeitpunkt, längstens bis zum 30. Juni 2016, weiterhin gültig; für diese gelten die Löschungsfristen nach § 14 Abs. 2.

(2) Personenbezogene Daten, die vor Inkrafttreten dieses Bundesgesetzes vom Bundes- oder Landesamt rechtmäßig ermittelt wurden, dürfen nach Maßgabe des § 11 Abs. 1 und 3 in der Datenanwendung gemäß § 11 verarbeitet werden.

(3) Personen, die im Zeitpunkt des Inkrafttretens dieses Bundesgesetzes bereits Bedienstete des Bundes- oder Landesamtes sind, haben die in § 2 Abs. 3 vorgesehene spezielle Ausbildung für Verfassungsschutz und Terrorismusbekämpfung innerhalb von zwei Jahren ab dem Tag des Inkrafttretens zu absolvieren.“

§ 23: Vollziehung

„Mit der Vollziehung dieses Bundesgesetzes ist der Bundesminister für Inneres betraut.“

Bundesgesetz, mit dem das Sicherheitspolizeigesetz geändert wird

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

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

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

Kommentar:

Das Problem dieser Norm ist, das damit praktisch die Generalermächtigung für die Polizei, bei jedem Einsatz jederzeit Video- und Tonaufzeichnungen vorzunehmen erteilt wird, weil potentiell jederzeit zumindest der Einsatz von Befehlsgewalt (wenn schon nicht Zwangsgewalt) angebracht sein könnte. Unabhängig davon, ob das angefertigte Material tatsächlich indiziert, dass es „zur Kontrolle der Rechtmäßigkeit der Amtshandlung ausgewertet werden“ muss, dürfen alle Aufzeichnungen auch „zur Verfolgung von strafbaren Handlungen“ aufbewahrt und bei Bedarf ausgewertet werden. Es macht den Anschein, dass die „Kontrolle der Rechtmäßigkeit der Amtshandlung“ als Vorwand vorgeschoben wird, um den Spielraum für eine Überwachung mit Aufzeichnung der Umgebung unkompliziert und beinahe uferlos ausweiten zu können.

Ein weiteres Problem liegt darin, dass keine Unterscheidung getroffen wird, ob die Aufzeichnung durch private oder dienstliche Geräte hergestellt werden dürfen. Was daran problematisch ist, zeigt ein Artikel in der Zeitschrift *Polizei Oberösterreich - Das Info-Magazin der Landespolizeidirektion*, von RevInsp Simone Mayr und OR MMag. David Furtner, Seite 27 f., bei dem die Autoren zum Ergebnis gelangen, dass *„das Filmen und Fotografieren dienstlicher Inhalte durch Polizistinnen und Polizisten mit privaten (!) Geräten () grundsätzlich untersagt (ist). Also beispielsweise das Aufnehmen einer Amtshandlung mit dem privaten Smartphone. Das mag nun für manche/n unbefriedigend sein, ist aber ganz klar durch die österreichische Rechtsordnung und den zitierten Erlass so vorgegeben. (…) Auch wenn die gegenständlichen Ausführungen bei manchen Unverständnis auslösen – aus Sicht der Autoren sind sie jedenfalls berechtigt. Der Vergleich mit Unternehmen in der Privatwirtschaft macht auch hier sicher. Keiner von uns würde darüber erfreut sein, wenn etwa ein Angestellter einer Bank die Daten von Kunden über sein privates Mobiltelefon mit der Öffentlichkeit teilt. Man erinnere sich an den berechtigten Aufschrei in der Kollegenschaft, als die Daten tausender Polizeibeamter gehackt und veröffentlicht wurden. Wer von uns kann ausschließen, dass sich auf dem privaten Telefon Viren befinden oder unberechtigte Dritte mitlesen? Auch bei Fahndungen nach Abgängigen sollten ausschließlich die dienstlichen Möglichkeiten – und derer gibt es viele – erschöpfend ausgenutzt*

werden und keine privaten Endgeräte genutzt werden. Selbst wenn das Ziel oft ein heres ist, gilt auch hier der Grundsatz, dass weniger oft mehr ist."

Nachsatz der Verfasser dieser Stellungnahme: Ob es um die Datensicherheit bei dienstlichen Mobiltelefonen bzw. Smartphones so viel besser bestellt ist, wie bei privaten Endgeräten, darf angesichts des durch Edward Snowden verbreiteten Wissens in Zweifel gezogen werden – an dieser Stelle sei daran erinnert, dass die „Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses zugunsten des Auslands" (§ 124 StGB) auch ein „verfassungsgefährdender Angriff" gemäß § 6 Abs. 2 Z 4 PStSG ist.

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

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

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

7. Die Überschrift des § 25 wird das Wort „Kriminalpolizeiliche" durch das Wort „Sicherheitspolizeiliche" ersetzt.

8. In § 53 entfallen in Abs. 1 die Z 2a und 7, in Abs. 3 der Beistrich nach dem Wort „Angriffe" und die
Wortfolge „für die erweiterte Gefahrenerforschung unter den Voraussetzungen nach Abs. 1" sowie in
Abs. 5 die Wortfolge „für die erweiterte Gefahrenerforschung (§ 21 Abs. 3)".

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

Kommentar:

Diese Ausdehnung ist schwer kritikwürdig. Bis jetzt darf die Polizei ohne Gerichtsbeschluss nur die gefährdeten Menschen unter Rückgriff auf Daten der Mobiltelefonie aufspüren. Diese Befugnis stand schon bisher unter Kritik, weil sie ohne richterliche Kontrolle zusteht und nicht einmal eine (vorab) Ermächtigung des Rechtschutzbeauftragten erfordert (lediglich eine Meldung an den RSB). In der öffentlichen Debatte wurde seitens des BM.I bzw. der Polizei stets hervorgehoben, dass damit vor allem Lawinenopfer und vermisste Wanderer lokalisiert werden sollen. Durch die vorgeschlagene Änderung soll künftig auch die „Gefährder", also die mutmaßlichen Täter nach dieser Befugnis geortet werden dürfen. Damit werden – im Vergleich zur StPO – sehr niederschwellige Standortdatenauskünfte ohne vergleichbaren Rechtsschutz und Kontrolle erlaubt. Dieses Problem wird verstärkt durch die (implizite) Ermächtigung zum Einsatz des sog. „IMSI-Catcher" und die niederschwellige Befugnis zur Auskunft über die IMSI (International Mobile Subscriber Identifier), das ist die weltweit eindeutige Kennung einer sim-Karte, unabhängig von der zugewiesenen Rufnummer. Der Einsatz eines „IMSI-Catcher" ermöglicht der Polizei nämlich nicht nur den Standort zu orten, sondern auch eine Inhaltsüberwachung des Endgeräts mit dieser IMSI ohne Unterstützung des Mobilfunkanbieters. Dies ist zwar gesetzlich unzulässig, aber technisch einfach und ohne Spuren zu hinterlassen möglich. Nach dem Vorschlag soll es der Polizei also künftig erlaubt sein, die Standortdatenfeststellung auch in Bezug auf Verdächtige („Gefährder") durch den IMSI-Catcher vorzunehmen. Häufig wird anschießend an die Lokalisierung eine Observation folgen, die in der

Praxis durch den IMSI-Catcher unterstützt wird. Aber woher weiß die Polizei, ob der mutmaßliche „Gefährder“ auch tatsächlich selbst das lokalisierte Gerät eingesteckt hat? Eine einfache Möglichkeit wäre, in Gesprächsinhalte hineinzuhören, um den gesuchten Teilnehmer zu identifizieren. Trotz der gesetzlichen Unzulässigkeit könnte die Verlockung selbst für die absolute Mehrheit der grundsätzlich rechtstreuen Polizeibeamten groß sein, weil man schließlich ja eine Gefahr für Menschen rasch und zuverlässig abwehren möchte und so das Risiko vermeiden könnte, der falschen Person nachzueilen. Die vorgeschlagene Änderung könnte selbst die integersten Beamten dazu verleiten, für den guten Zweck einen Befugnismissbrauch zu begehen, der ohnehin nicht nachvollzogen werden könnte.

Im Hinblick auf das frühere Argument, dass die Bestimmung nur verwendet wird, um vermisste Tourengeher usw. zu finden, stellt sich jedenfalls die dringende Frage, in welchem Verhältnis diese Rechtfertigung zu den jetzigen Vorschlägen steht.

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

11. In § 53a entfällt in Abs. 1 die Wortfolge „den Personen- und Objektschutz und“ und es werden folgende Absätze ein- bzw. angefügt:

„(1a) Die Sicherheitsbehörden dürfen für den Personen- und Objektschutz Erreichbarkeits- und Identifikationsdaten über die gefährdete natürliche oder juristische Person, die erforderlichen Sachdaten einschließlich KFZ-Kennzeichen zu den zu schützenden Objekten, Angaben zu Zeit, Ort, Grund und Art des Einschreitens sowie Verwaltungsdaten verarbeiten.

(5a) Datenanwendungen nach Abs. 1a zum Schutz von verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit (§ 22 Abs. 1 Z 2), der Vertreter ausländischer Staaten, internationaler Organisationen und anderer Völkerrechtssubjekte (§ 22 Abs. 1 Z 3) sowie kritischen Infrastrukturen (§ 22 Abs. 1 Z 6) dürfen das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung und die Landesämter Verfassungsschutz (§ 1 Abs. 3 Polizeiliches Staatsschutzgesetz - PStSG, BGBl. I Nr. xx/2015) im Informationsverbundsystem führen. Übermittlungen der gemäß Abs. 1a verarbeiteten Daten sind an Sicherheitsbehörden für Zwecke der Sicherheitspolizei und Strafrechtspflege, an Staatsanwaltschaften und ordentliche Gerichte für Zwecke der Strafrechtspflege, an Dienststellen inländischer Behörden, soweit dies eine wesentliche Voraussetzung zur Wahrnehmung einer ihr gesetzlich übertragenen Aufgabe ist, an ausländische Sicherheitsbehörden entsprechend den Bestimmungen über die internationale polizeiliche Amtshilfe und im Übrigen nur zulässig, wenn hierfür eine ausdrückliche gesetzliche Ermächtigung besteht.“

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

13. § 54 Abs. 3 lautet:

„(3) Das Einholen von Auskünften durch die Sicherheitsbehörde ohne Hinweis gemäß Abs. 1 oder durch andere Personen im Auftrag der Sicherheitsbehörde, 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).“

14. Nach § 54 Abs. 3 wird folgender Abs. 3a eingefügt:

„(3a) Der verdeckte Ermittler ist von der Sicherheitsbehörde zu führen und regelmäßig zu überwachen. Sein Einsatz und dessen nähere Umstände sowie Auskünfte und Mitteilungen, die durch ihn erlangt werden, sind zu dokumentieren (§ 13a), sofern sie für die Aufgabenerfüllung von Bedeutung sein können.“

15. In § 54 Abs. 5 wird im ersten Satz vor der Wortfolge „einer Zusammenkunft“ die Wortfolge „oder im Zusammenhang mit“ eingefügt, das Wort „Anwesender“ gestrichen und lautet der letzte Satz:

„Die auf diese Weise ermittelten Daten dürfen auch zur Abwehr gefährlicher Angriffe und Verfolgung strafbarer Handlungen, die sich im Zusammenhang mit oder während der Zusammenkunft ereignen, verarbeitet werden."

16. § 59 Abs. 2 lautet:

„(2) Jede Abfrage und Übermittlung personenbezogener Daten aus der Zentralen Informationssammlung und den übrigen Informationsverbundsystemen ist so zu protokollieren, dass eine Zuordnung der Abfrage oder Übermittlung zu einem bestimmten Organwalter möglich ist. Die Zuordnung zu einem bestimmten Organwalter ist bei automatisierten Abfragen nicht erforderlich. Von der Protokollierung gänzlich ausgenommen sind automatisierte Abfragen gemäß § 54 Abs. 4b, es sei denn, es handelt sich um einen Treffer. Die Protokollaufzeichnungen sind drei Jahre aufzubewahren und danach zu löschen."

17. Nach § 75 Abs. 1 wird folgender Abs. 1a eingefügt:

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

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

19. Nach § 80 Abs. 1 wird folgender Abs. 1a eingefügt:

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

20. In § 91c Abs. 1 entfällt der zweite Satz und es wird das Wort „Kennzeichnerkennungsgeräten" durch das Wort „Kennzeichenerkennungsgeräten" ersetzt.

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

22. Dem § 94 werden folgende Abs. 38 und 39 angefügt:

„(38) Die §§ 13a Abs. 3, 20, 21 Abs. 2a, die Überschrift des § 25, die §§ 54 Abs. 5, 59 Abs. 2, 75 Abs. 1a und 2, 80 Abs. 1a sowie der Eintrag im Inhaltsverzeichnis zu § 25 in der Fassung des Bundesgesetzes BGBl. I Nr. XX/2015 treten mit xx. xx 2015 in Kraft.

(39) Die §§ 6 Abs. 1, 53 Abs. 1, 3, 3b, 4 und 5, 53a Abs. 1, 1a und 5a, 54 Abs. 2, 3, 3a und 4, 91c Abs. 1, 91d Abs. 3 und 4, 96 Abs. 8 sowie das Inhaltsverzeichnis in der Fassung des Bundesgesetzes

BGBl. I Nr. XX/2015 treten mit 1. Jänner 2016 in Kraft. Gleichzeitig treten die §§ 21 Abs. 3, 63 Abs. 1a und 1b, 91c Abs. 3 und 93a samt Überschrift außer Kraft."

23. Dem § 96 wird folgender Abs. 8 angefügt:

„(8) Daten, die auf Grundlage des § 53a Abs. 1 für den Personen- und Objektschutz im Zeitpunkt des Inkrafttretens des Bundesgesetzes BGBl. I Nr. xx/20xx verarbeitet werden, dürfen auf Grundlage des § 53a Abs. 1a weiterverarbeitet sowie unter den Voraussetzungen des § 53a Abs. 5a in der Fassung BGBl. I Nr. xx/20xx auch im Informationsverbund geführt werden."

24. Dem § 97 wird folgender Abs. 4 angefügt:

„(4) § 13a Abs. 3 in der Fassung des Bundesgesetzes BGBl. I Nr. XX/2015 tritt mit Ablauf des 31. Dezember 2018 außer Kraft."

V. Anhang – materielle Straftatbestände zur Definition des „verfassungsgefährdenden Angriffs"

StGB:

Widerrechtlicher Zugriff auf ein Computersystem

§ 118a. (1) Wer sich in der Absicht, sich oder einem anderen Unbefugten von in einem Computersystem gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen Zugang verschafft, indem er spezifische Sicherheitsvorkehrungen im Computersystem überwindet, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

(3) Wer die Tat als Mitglied einer kriminellen Vereinigung begeht, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

Verletzung des Telekommunikationsgeheimnisses

§ 119. (1) Wer in der Absicht, sich oder einem anderen Unbefugten vom Inhalt einer im Wege einer Telekommunikation oder eines Computersystems übermittelten und nicht für ihn bestimmten Nachricht Kenntnis zu verschaffen, eine Vorrichtung, die an der Telekommunikationsanlage oder an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

Missbräuchliches Abfangen von Daten

§ 119a. (1) Wer in der Absicht, sich oder einem anderen Unbefugten von im Wege eines Computersystems übermittelten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich oder einem anderen einen

Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, eine Vorrichtung, die an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt oder die elektromagnetische Abstrahlung eines Computersystems auffängt, ist, wenn die Tat nicht nach § 119 mit Strafe bedroht ist, mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses zugunsten des Auslands

§ 124. (1) Wer ein Geschäfts- oder Betriebsgeheimnis mit dem Vorsatz auskundschaftet, daß es im Ausland verwertet, verwendet oder sonst ausgewertet werde, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen. Daneben kann auf Geldstrafe bis zu 360 Tagessätzen erkannt werden.

(2) Ebenso ist zu bestrafen, wer ein Geschäfts- oder Betriebsgeheimnis, zu dessen Wahrung er verpflichtet ist, der Verwertung, Verwendung oder sonstigen Auswertung im Ausland preisgibt.

Datenbeschädigung

§ 126a. (1) Wer einen anderen dadurch schädigt, daß er automationsunterstützt verarbeitete, übermittelte oder überlassene Daten, über die er nicht oder nicht allein verfügen darf, verändert, löscht oder sonst unbrauchbar macht oder unterdrückt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Wer durch die Tat an den Daten einen 3 000 Euro übersteigenden Schaden herbeiführt, ist mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bis zu 360 Tagessätzen, wer einen 50 000 Euro übersteigenden Schaden herbeiführt oder die Tat als Mitglied einer kriminellen Vereinigung begeht, mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.

Störung der Funktionsfähigkeit eines Computersystems

§ 126b. (1) Wer die Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er Daten eingibt oder übermittelt, ist, wenn die Tat nicht nach § 126a mit Strafe bedroht ist, mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Wer durch die Tat eine längere Zeit andauernde Störung der Funktionsfähigkeit eines Computersystems herbeiführt, ist mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bis zu 360 Tagessätzen, wer die Tat als Mitglied einer kriminellen Vereinigung begeht, mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.

Missbrauch von Computerprogrammen oder Zugangsdaten

§ 126c. (1) Wer

1. ein Computerprogramm, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a), einer Verletzung des Telekommunikationsgeheimnisses (§ 119), eines missbräuchlichen Abfangens von Daten (§ 119a), einer Datenbeschädigung (§ 126a), einer Störung der Funktionsfähigkeit eines Computersystems (§ 126b) oder eines betrügerischen Datenverarbeitungsmissbrauchs (§ 148a) geschaffen oder adaptiert worden ist, oder eine

vergleichbare solche Vorrichtung oder

2. ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen,

mit dem Vorsatz herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt, dass sie zur Begehung einer der in Z 1 genannten strafbaren Handlungen gebraucht werden, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Nach Abs. 1 ist nicht zu bestrafen, wer freiwillig verhindert, dass das in Abs. 1 genannte Computerprogramm oder die damit vergleichbare Vorrichtung oder das Passwort, der Zugangscode oder die damit vergleichbaren Daten in der in den §§ 118a, 119, 119a, 126a, 126b oder 148a bezeichneten Weise gebraucht werden. Besteht die Gefahr eines solchen Gebrauches nicht oder ist sie ohne Zutun des Täters beseitigt worden, so ist er nicht zu bestrafen, wenn er sich in Unkenntnis dessen freiwillig und ernstlich bemüht, sie zu beseitigen.

Geldwäscherei

§ 165 (3) Ebenso ist zu bestrafen, wer wissentlich der Verfügungsmacht einer kriminellen Organisation (§ 278a) oder einer terroristischen Vereinigung (§ 278b) unterliegende Vermögensbestandteile in deren Auftrag oder Interesse an sich bringt, verwahrt, anlegt, verwaltet, umwandelt, verwertet oder einem Dritten überträgt.

Vorbereitung eines Verbrechens durch Kernenergie, ionisierende Strahlen oder Sprengmittel

§ 175. (1) Wer in der Absicht, sich oder einem anderen die Begehung einer nach § 171 oder § 173 mit Strafe bedrohten, wenn auch noch nicht bestimmten Handlung zu ermöglichen, einen Kernbrennstoff, einen radioaktiven Stoff, einen Sprengstoff, einen Bestandteil eines Sprengstoffs oder eine zur Herstellung oder Benutzung eines dieser Stoffe erforderliche Vorrichtung anfertigt, erwirbt oder besitzt, oder einen solchen Stoff einem anderen überläßt, von dem er weiß (§ 5 Abs. 3), daß er ihn zur Vorbereitung einer der genannten mit Strafe bedrohten Handlungen erwirbt, ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.

(2) Der Täter ist nicht zu bestrafen, wenn er freiwillig, bevor die Behörde (§ 151 Abs. 3) von seinem Verschulden erfahren hat, den Gegenstand der Behörde übergibt, es ihr ermöglicht, des Gegenstands habhaft zu werden, oder sonst die Gefahr beseitigt, daß von dem Gegenstand zur Begehung einer nach § 171 oder § 173 mit Strafe bedrohten Handlung Gebrauch gemacht wird.

Herstellung und Verbreitung von Massenvernichtungswaffen

§ 177a. (1) Wer zur Massenvernichtung bestimmte und geeignete atomare, biologische oder chemische Kampfmittel

1. herstellt, verarbeitet oder zum Zweck der Herstellung entwickelt,
2. in das Inland einführt, aus dem Inland ausführt oder durch das Inland durchführt oder
3. erwirbt, besitzt oder einem anderen überläßt oder verschafft,

ist mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.

(2) Weiß der Täter, daß die Kampfmittel in ein Gebiet gelangen sollen, in dem ein Krieg oder ein bewaffneter Konflikt ausgebrochen ist oder unmittelbar auszubrechen droht, so ist er mit Freiheitsstrafe von fünf bis zu fünfzehn Jahren, weiß er aber, daß die Kampfmittel zum Einsatz gelangen sollen, mit Freiheitsstrafe von zehn bis zu zwanzig Jahren oder mit lebenslanger Freiheitsstrafe zu bestrafen.

Unerlaubter Umgang mit Kernmaterial, radioaktiven Stoffen oder Strahleneinrichtungen

§ 177b. (1) Wer entgegen einer Rechtsvorschrift oder einem behördlichen Auftrag Kernmaterial herstellt, bearbeitet, verarbeitet, verwendet, besitzt, beseitigt, befördert, in das Inland einführt, aus dem Inland ausführt oder durch das Inland durchführt, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

(2) Ebenso ist zu bestrafen, wer entgegen einer Rechtsvorschrift oder einem behördlichen Auftrag radioaktive Stoffe oder Strahleneinrichtungen so herstellt, bearbeitet, verarbeitet, verwendet, besitzt, beseitigt, befördert, in das Inland einführt, aus dem Inland ausführt oder durch das Inland durchführt, dass dadurch

1. eine Gefahr für das Leben oder einer schweren Körperverletzung (§ 84 Abs. 1) eines anderen oder sonst für die Gesundheit oder körperliche Sicherheit einer größeren Zahl von Menschen,
2. eine Gefahr für den Tier- oder Pflanzenbestand in erheblichem Ausmaß,
3. eine lange Zeit andauernde Verschlechterung des Zustands eines Gewässers, des Bodens oder der Luft oder
4. ein Beseitigungsaufwand, der 50 000 Euro übersteigt,

entstehen kann.

(3) Wer entgegen einer Rechtsvorschrift oder einem behördlichen Auftrag Kernmaterial oder radioaktive Stoffe herstellt, bearbeitet, verarbeitet, verwendet, besitzt, beseitigt, befördert, in das Inland einführt, aus dem Inland ausführt oder durch das Inland durchführt und dadurch die Gefahr herbeiführt, dass Kernmaterial oder radioaktive Stoffe der Herstellung oder Verarbeitung von zur Massenvernichtung geeigneten atomaren Kampfmitteln zugänglich werden, ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen. Ebenso ist zu bestrafen, wer eine der in Abs. 1 oder Abs. 2 erwähnten Handlungen gewerbsmäßig begeht.

(4) Wird durch eine der im Abs. 1 oder Abs. 2 erwähnten Handlungen die im § 171 Abs. 1 genannte Gefahr herbeigeführt, der Tier- oder Pflanzenbestand erheblich geschädigt oder eine lange Zeit andauernde Verschlechterung des Zustands eines Gewässers, des Bodens oder der Luft bewirkt, so ist der Täter mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen. Hat die Tat eine der im § 169 Abs. 3 genannten Folgen, so sind die dort angedrohten Strafen zu verhängen.

(5) Der Begriff Kernmaterial bezeichnet Ausgangsmaterial und besonderes spaltbares Material sowie Ausrüstung, Technologie und Material, die dem Sicherheitskontrollsystem nach dem Sicherheitskontrollgesetz 1991, BGBl. Nr. 415/1992, unterliegen. Der Begriff radioaktive Stoffe bezeichnet Stoffe, die ein oder mehrere Radionuklide enthalten, sofern deren Aktivität oder Konzentration nach dem Stand der Technik im Zusammenhang mit dem Strahlenschutz nicht außer Acht gelassen werden kann; Gegenstände, die radioaktive Stoffe enthalten oder an deren Oberfläche sich solche Stoffe befinden, stehen radioaktiven Stoffen

gleich. Unter Strahleneinrichtungen sind solche Geräte oder Anlagen zu verstehen, die, ohne radioaktive Stoffe zu enthalten, imstande sind, ionisierende Strahlung auszusenden, und deren Betrieb einer Bewilligungspflicht nach dem Strahlenschutzgesetz,BGBl. Nr. 227/1969 in der jeweils geltenden Fassung, unterliegt.

Hochverrat und andere Angriffe gegen den Staat

Hochverrat

§ 242. (1) Wer es unternimmt, mit Gewalt oder durch Drohung mit Gewalt die Verfassung der Republik Österreich oder eines ihrer Bundesländer zu ändern oder ein zur Republik Österreich gehörendes Gebiet abzutrennen, ist mit Freiheitsstrafe von zehn bis zu zwanzig Jahren zu bestrafen.

(2) Ein Unternehmen im Sinn des Abs. 1 liegt auch schon bei einem Versuch vor.

Tätige Reue

§ 243. (1) Der Täter ist wegen Hochverrats nicht zu bestrafen, wenn er freiwillig die Ausführung aufgibt oder diese, falls mehrere an dem Vorhaben beteiligt sind, verhindert oder wenn er freiwillig den Erfolg abwendet.

(2) Der Täter ist auch dann nicht zu bestrafen, wenn die Ausführung oder der Erfolg ohne sein Zutun unterbleibt, er sich jedoch in Unkenntnis dessen freiwillig und ernstlich bemüht, die Ausführung zu verhindern oder den Erfolg abzuwenden.

Vorbereitung eines Hochverrats

§ 244. (1) Wer mit einem anderen die gemeinsame Begehung eines Hochverrats verabredet, ist mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.

(2) Ebenso ist zu bestrafen, wer einen Hochverrat in anderer Weise vorbereitet und dadurch die Gefahr eines hochverräterischen Unternehmens herbeiführt oder erheblich vergrößert oder wer einen Hochverrat im Zusammenwirken mit einer ausländischen Macht vorbereitet.

Tätige Reue

§ 245. (1) Der Täter ist wegen Vorbereitung eines Hochverrats nicht zu bestrafen, wenn er freiwillig seine Tätigkeit aufgibt oder, falls mehrere an der Vorbereitung beteiligt sind, den Hochverrat verhindert.

(2) § 243 Abs. 2 gilt entsprechend.

Staatsfeindliche Verbindungen

§ 246. (1) Wer eine Verbindung gründet, deren wenn auch nicht ausschließlicher Zweck es ist, auf gesetzwidrige Weise die Unabhängigkeit, die in der Verfassung festgelegte Staatsform oder eine verfassungsmäßige Einrichtung der Republik Österreich oder eines ihrer Bundesländer zu erschüttern, ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.

(2) Ebenso ist zu bestrafen, wer sich in einer solchen Verbindung führend betätigt, für sie Mitglieder wirbt oder sie mit Geldmitteln oder sonst in erheblicher Weise unterstützt.

(3) Wer an einer solchen Verbindung sonst teilnimmt oder sie auf eine andere als die im Abs. 2 bezeichnete Weise unterstützt, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

Tätige Reue

§ 247. Nach § 246 ist nicht zu bestrafen, wer freiwillig, bevor die Behörde (§ 151 Abs. 3) von seinem Verschulden erfahren hat, alles, was ihm von der Verbindung und ihren Plänen bekannt ist, zu einer Zeit, da es noch geheim ist, einer solchen Behörde aufdeckt.

Herabwürdigung des Staates und seiner Symbole

§ 248. (1) Wer auf eine Art, daß die Tat einer breiten Öffentlichkeit bekannt wird, in gehässiger Weise die Republik Österreich oder eines ihrer Bundesländer beschimpft oder verächtlich macht, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

(2) Wer in der im Abs. 1 bezeichneten Art in gehässiger Weise eine aus einem öffentlichen Anlaß oder bei einer allgemein zugänglichen Veranstaltung gezeigte Fahne der Republik Österreich oder eines ihrer Bundesländer, ein von einer österreichischen Behörde angebrachtes Hoheitszeichen, die Bundeshymne oder eine Landeshymne beschimpft, verächtlich macht oder sonst herabwürdigt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Angriffe auf oberste Staatsorgane

Gewalt und gefährliche Drohung gegen den Bundespräsidenten

§ 249. Wer es unternimmt (§ 242 Abs. 2), mit Gewalt oder durch gefährliche Drohung den Bundespräsidenten abzusetzen oder durch eines dieser Mittel zu nötigen oder zu hindern, seine Befugnisse überhaupt oder in einem bestimmten Sinn auszuüben, ist mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.

Nötigung eines verfassungsmäßigen Vertretungskörpers, einer Regierung, des Verfassungsgerichtshofs, des Verwaltungsgerichtshofs oder des Obersten Gerichtshofs

§ 250. Wer es unternimmt (§ 242 Abs. 2), den Nationalrat, den Bundesrat, die Bundesversammlung, die Bundesregierung, einen Landtag, eine Landesregierung, den Verfassungsgerichtshof, den Verwaltungsgerichtshof oder den Obersten Gerichtshof mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder zu hindern, ihre Befugnisse überhaupt oder in einem bestimmten Sinn auszuüben, ist mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.

Nötigung von Mitgliedern eines verfassungsmäßigen Vertretungskörpers, einer Regierung, des Verfassungsgerichtshofs, des Verwaltungsgerichtshofs oder des Obersten Gerichtshofs oder des Präsidenten des Rechnungshofs oder des Leiters eines Landesrechnungshofs

§ 251. Wer ein Mitglied des Nationalrats, des Bundesrats, der Bundesversammlung, der Bundesregierung, eines Landtags, einer Landesregierung, des Verfassungsgerichtshofs, des Verwaltungsgerichtshofs oder des Obersten Gerichtshofs oder den Präsidenten des Rechnungshofs, den Leiter eines Landesrechnungshofs oder deren Stellvertreter mit Gewalt oder durch gefährliche Drohung nötigt oder hindert, seine Befugnisse überhaupt oder in einem bestimmten Sinn auszuüben, ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren und im Fall einer schweren Nötigung (§ 106) mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.

Landesverrat

Verrat von Staatsgeheimnissen

§ 252. (1) Wer einer fremden Macht oder einer über- oder zwischenstaatlichen Einrichtung ein Staatsgeheimnis bekannt oder zugänglich macht, ist mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.

(2) Wer der Öffentlichkeit ein Staatsgeheimnis bekannt oder zugänglich macht, ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen. Betrifft das Staatsgeheimnis verfassungsgefährdende Tatsachen (Abs. 3), so ist der Täter jedoch nur zu bestrafen, wenn er in der Absicht handelt, der Republik Österreich einen Nachteil zuzufügen. Die irrtümliche Annahme verfassungsgefährdender Tatsachen befreit den Täter nicht von Strafe.

(3) Verfassungsgefährdende Tatsachen sind solche, die Bestrebungen offenbaren, in verfassungswidriger Weise den demokratischen, bundesstaatlichen oder rechtsstaatlichen Aufbau der Republik Österreich zu beseitigen, deren dauernde Neutralität aufzuheben oder ein verfassungsgesetzlich gewährleistetes Recht abzuschaffen oder einzuschränken oder wiederholt gegen ein solches Recht zu verstoßen.

Preisgabe von Staatsgeheimnissen

§ 253. (1) Wer zufolge einer ihn im besonderen treffenden rechtlichen Verpflichtung dazu verhalten ist, ein Geheimnis zu wahren, von dem er weiß, daß es ein Staatsgeheimnis ist, und diese Verpflichtung unter Umständen verletzt, unter denen das Geheimnis einer fremden Macht, einer über- oder zwischenstaatlichen Einrichtung oder der Öffentlichkeit bekannt oder zugänglich werden kann, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

(2) Betrifft das Staatsgeheimnis verfassungsgefährdende Tatsachen (§ 252 Abs. 3), so ist der Täter jedoch nur zu bestrafen, wenn er in der Absicht handelt, der Republik Österreich einen Nachteil zuzufügen. Die irrtümliche Annahme verfassungsgefährdender Tatsachen befreit den Täter nicht von Strafe.

Ausspähung von Staatsgeheimnissen

§ 254. (1) Wer ein Staatsgeheimnis mit dem Vorsatz zurückhält oder sich verschafft, es einer fremden Macht einer über- oder zwischenstaatlichen Einrichtung oder der Öffentlichkeit bekannt oder zugänglich zu machen und dadurch die Gefahr eines schweren Nachteils für die Landesverteidigung der Republik Österreich oder für die Beziehungen der Republik Österreich zu einer fremden Macht oder einer über- oder zwischenstaatlichen Einrichtung herbeizuführen, ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.

(2) § 253 Abs. 2 gilt entsprechend.

Begriff des Staatsgeheimnisses

§ 255. Staatsgeheimnisse im Sinn dieses Abschnitts sind Tatsachen, Gegenstände oder Erkenntnisse, insbesondere Schriften, Zeichnungen, Modelle und Formeln, und Nachrichten darüber, die nur einem begrenzten Personenkreis zugänglich sind und vor einer fremden Macht oder einer über- oder zwischenstaatlichen Einrichtung geheimgehalten werden müssen, um die Gefahr eines schweren Nachteils für die Landesverteidigung der Republik Österreich oder für die Beziehungen der Republik Österreich zu einer fremden Macht oder einer über- oder zwischenstaatlichen Einrichtung hintanzuhalten.

Geheimer Nachrichtendienst zum Nachteil Österreichs

§ 256. Wer zum Nachteil der Republik Österreich einen geheimen Nachrichtendienst einrichtet oder betreibt oder einen solchen Nachrichtendienst wie immer unterstützt, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

Begünstigung feindlicher Streitkräfte

§ 257. (1) Ein Österreicher, der während eines Krieges oder eines bewaffneten Konfliktes, an denen die Republik Österreich beteiligt ist, in den Dienst der feindlichen Streitkräfte tritt

oder gegen die Republik Österreich Waffen trägt, ist mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.

(2) Ebenso ist zu bestrafen, wer während eines Krieges oder eines bewaffneten Konfliktes, an denen die Republik Österreich beteiligt ist, oder bei unmittelbar drohender Gefahr eines solchen Krieges oder bewaffneten Konfliktes den feindlichen Streitkräften einen Vorteil verschafft oder dem österreichischen Bundesheer einen Nachteil zufügt. Ausländer sind nach dieser Bestimmung nur zu bestrafen, wenn sie die Tat begehen, während sie sich im Inland befinden.

Landesverräterische Fälschung und Vernichtung von Beweisen
§ 258. (1) Wer

1. über ein Rechtsverhältnis zwischen der Republik Österreich oder einem ihrer Bundesländer und einer fremden Macht oder einer über- oder zwischenstaatlichen Einrichtung oder
2. über eine Tatsache, die für die Beziehungen zwischen der Republik Österreich oder einem ihrer Bundesländer und einer fremden Macht oder einer über- oder zwischenstaatlichen Einrichtung von Bedeutung ist,

ein falsches Beweismittel herstellt oder ein echtes verfälscht, vernichtet, beschädigt oder beseitigt und dadurch die Interessen der Republik Österreich oder eines ihrer Bundesländer gefährdet, ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.

(2) Ebenso ist zu bestrafen, wer von einem solchen falschen oder verfälschten Beweismittel Gebrauch macht und dadurch die Interessen der Republik Österreich oder eines ihrer Bundesländer gefährdet.

Landfriedensbruch
274. (1) Wer wissentlich an einer Zusammenrottung einer Menschenmenge teilnimmt, die darauf abzielt, daß unter ihrem Einfluß ein Mord (§ 75), ein Totschlag (§ 76), eine Körperverletzung (§§ 83 bis 87) oder eine schwere Sachbeschädigung (§ 126) begangen werde, ist, wenn es zu einer solchen Gewalttat gekommen ist, mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

(2) Wer an der Zusammenrottung führend teilnimmt oder als Teilnehmer eine der im Abs. 1 angeführten strafbaren Handlungen ausführt oder zu ihrer Ausführung beigetragen hat (§ 12), ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

(3) Nach Abs. 1 ist nicht zu bestrafen, wer sich freiwillig aus der Zusammenrottung zurückzieht oder ernstlich zurückzuziehen sucht, bevor sie zu einer Gewaltanwendung geführt hat, es sei denn, daß er an der Zusammenrottung führend teilgenommen hat.

Terroristische Vereinigung
§ 278b. (1) Wer eine terroristische Vereinigung (Abs. 3) anführt, ist mit Freiheitsstrafe von fünf bis zu fünfzehn Jahren zu bestrafen. Wer eine terroristische Vereinigung anführt, die sich auf die Drohung mit terroristischen Straftaten (§ 278c Abs. 1) oder Terrorismusfinanzierung (§ 278d) beschränkt, ist mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.

(2) Wer sich als Mitglied (§ 278 Abs. 3) an einer terroristischen Vereinigung beteiligt, ist mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.

(3) Eine terroristische Vereinigung ist ein auf längere Zeit angelegter Zusammenschluss von mehr als zwei Personen, der darauf ausgerichtet ist, dass von einem oder mehreren Mitgliedern dieser Vereinigung eine oder mehrere terroristische Straftaten (§ 278c) ausgeführt werden oder Terrorismusfinanzierung (§ 278d) betrieben wird.

Terroristische Straftaten

§ 278c. (1) Terroristische Straftaten sind

1. Mord (§ 75),
2. Körperverletzungen nach den §§ 84 bis 87,
3. erpresserische Entführung (§ 102),
4. schwere Nötigung (§ 106),
5. gefährliche Drohung nach § 107 Abs. 2,
6. schwere Sachbeschädigung (§ 126) und Datenbeschädigung (§ 126a), wenn dadurch eine Gefahr für das Leben eines anderen oder für fremdes Eigentum in großem Ausmaß entstehen kann,
7. vorsätzliche Gemeingefährdungsdelikte (§§ 169, 171, 173, 175, 176, 177a, 177b, 178) oder vorsätzliche Beeinträchtigung der Umwelt (§ 180),
8. Luftpiraterie (§ 185),
9. vorsätzliche Gefährdung der Sicherheit der Luftfahrt (§ 186),

9a. Aufforderung zu terroristischen Straftaten und Gutheißung terroristischer Straftaten (§ 282a) oder

10. eine nach § 50 des Waffengesetzes 1996 oder § 7 des Kriegsmaterialgesetzes strafbare Handlung,

wenn die Tat geeignet ist, eine schwere oder längere Zeit anhaltende Störung des öffentlichen Lebens oder eine schwere Schädigung des Wirtschaftslebens herbeizuführen, und mit dem Vorsatz begangen wird, die Bevölkerung auf schwerwiegende Weise einzuschüchtern, öffentliche Stellen oder eine internationale Organisation zu einer Handlung, Duldung oder Unterlassung zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation ernsthaft zu erschüttern oder zu zerstören.

(2) Wer eine terroristische Straftat im Sinne des Abs. 1 begeht, ist nach dem auf die dort genannte Tat anwendbaren Gesetz zu bestrafen, wobei das Höchstmaß der jeweils angedrohten Strafe um die Hälfte, höchstens jedoch auf zwanzig Jahre, hinaufgesetzt wird.

(3) Die Tat gilt nicht als terroristische Straftat, wenn sie auf die Herstellung oder Wiederherstellung demokratischer und rechtsstaatlicher Verhältnisse oder die Ausübung oder Wahrung von Menschenrechten ausgerichtet ist.

Terrorismusfinanzierung

§ 278d. (1) Wer Vermögenswerte mit dem Vorsatz bereitstellt oder sammelt, dass sie, wenn auch nur zum Teil, zur Ausführung

1. einer Luftpiraterie (§ 185) oder einer vorsätzlichen Gefährdung der Sicherheit der Luftfahrt (§ 186),
2. einer erpresserischen Entführung (§ 102) oder einer Drohung damit,
3. eines Angriffs auf Leib, Leben oder Freiheit einer völkerrechtlich geschützten Person oder

eines gewaltsamen Angriffs auf eine Wohnung, einen Dienstraum oder ein Beförderungsmittel einer solchen Person, der geeignet ist, Leib, Leben oder Freiheit dieser Person zu gefährden, oder einer Drohung damit,

4. einer vorsätzlichen Gefährdung durch Kernenergie oder ionisierende Strahlen (§ 171), einer Drohung damit, eines unerlaubten Umgangs mit Kernmaterial oder radioaktiven Stoffen (§ 177b), einer sonstigen strafbaren Handlung zur Erlangung von Kernmaterial oder radioaktiven Stoffen oder einer Drohung mit der Begehung eines Diebstahls oder Raubes von Kernmaterial oder radioaktiven Stoffen, um einen anderen zu einer Handlung, Duldung oder Unterlassung zu nötigen,
5. eines erheblichen Angriffs auf Leib oder Leben eines anderen auf einem Flughafen, der der internationalen Zivilluftfahrt dient, einer Zerstörung oder erheblichen Beschädigung eines solchen Flughafens oder eines darauf befindlichen Luftfahrzeugs oder einer Unterbrechung der Dienste des Flughafens, sofern die Tat unter Verwendung einer Waffe oder sonstigen Vorrichtung begangen wird und geeignet ist, die Sicherheit auf dem Flughafen zu gefährden,
6. einer strafbaren Handlung, die auf eine in den §§ 185 oder 186 geschilderte Weise gegen ein Schiff oder eine feste Plattform, gegen eine Person, die sich an Bord eines Schiffes oder auf einer festen Plattform befindet, gegen die Ladung eines Schiffes oder eine Schifffahrtseinrichtung begangen wird,
7. der Beförderung eines Sprengsatzes oder einer anderen tödlichen Vorrichtung an einen öffentlichen Ort, zu einer staatlichen oder öffentlichen Einrichtung, einem öffentlichen Verkehrssystem oder einer Versorgungseinrichtung oder des Einsatzes solcher Mittel mit dem Ziel, den Tod oder eine schwere Körperverletzung eines anderen oder eine weitgehende Zerstörung des Ortes, der Einrichtung oder des Systems zu verursachen, sofern die Zerstörung geeignet ist, einen erheblichen wirtschaftlichen Schaden herbeizuführen,
8. einer strafbaren Handlung, die den Tod oder eine schwere Körperverletzung einer Zivilperson oder einer anderen Person, die in einem bewaffneten Konflikt nicht aktiv an den Feindseligkeiten teilnimmt, herbeiführen soll, wenn diese Handlung auf Grund ihres Wesens oder der Umstände darauf abzielt, eine Bevölkerungsgruppe einzuschüchtern oder eine Regierung oder eine internationale Organisation zu einem Tun oder Unterlassen zu nötigen,

verwendet werden, ist mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.

(1a) Ebenso ist zu bestrafen, wer Vermögenswerte für

1. eine andere Person, von der er weiß, dass sie Handlungen nach Abs. 1 begeht, oder
2. ein Mitglied einer terroristischen Vereinigung, von der er weiß, dass sie darauf ausgerichtet ist, Handlungen nach Abs. 1 zu begehen,

bereitstellt oder sammelt.

(2) Der Täter ist nach Abs. 1 oder Abs. 1a nicht zu bestrafen, wenn die Tat nach einer anderen Bestimmung mit strengerer Strafe bedroht ist.

Ausbildung für terroristische Zwecke

§ 278e. (1) Wer eine andere Person in der Herstellung oder im Gebrauch von Sprengstoff, Schuss- oder sonstigen Waffen oder schädlichen oder gefährlichen Stoffen oder in einer anderen ebenso schädlichen oder gefährlichen spezifisch zur Begehung einer terroristischen Straftat nach § 278c Abs. 1 Z 1 bis 9 oder 10 geeigneten Methode oder einem solchen

Verfahren zum Zweck der Begehung einer solchen terroristischen Straftat unterweist, ist mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen, wenn er weiß, dass die vermittelten Fähigkeiten für diesen Zweck eingesetzt werden sollen.

(2) Wer sich in der Herstellung oder im Gebrauch von Sprengstoff, Schuss- oder sonstigen Waffen oder schädlichen oder gefährlichen Stoffen oder in einer anderen ebenso schädlichen oder gefährlichen spezifisch zur Begehung einer terroristischen Straftat nach § 278c Abs. 1 Z 1 bis 9 oder 10 geeigneten Methode oder einem solchen Verfahren unterweisen lässt, um eine solche terroristische Straftat unter Einsatz der erworbenen Fähigkeiten zu begehen, ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen. Die Strafe darf jedoch nach Art und Maß nicht strenger sein, als sie das Gesetz für die beabsichtigte Tat androht.

Anleitung zur Begehung einer terroristischen Straftat

§ 278f. (1) Wer ein Medienwerk, das nach seinem Inhalt dazu bestimmt ist, zur Begehung einer terroristischen Straftat (§ 278c Abs. 1 Z 1 bis 9 oder 10) mit den im § 278e genannten Mitteln anzuleiten, oder solche Informationen im Internet in einer Art anbietet oder einer anderen Person zugänglich macht, um zur Begehung einer terroristischen Straftat aufzureizen, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

(2) Ebenso ist zu bestrafen, wer sich ein Medienwerk im Sinne des Abs. 1 oder solche Informationen aus dem Internet verschafft, um eine terroristische Straftat (§ 278c Abs. 1 Z 1 bis 9 oder 10) zu begehen.

Bewaffnete Verbindungen

§ 279. (1) Wer unbefugt eine bewaffnete oder zur Bewaffnung bestimmte Verbindung aufstellt oder eine bestehende Verbindung bewaffnet, sich in dieser Verbindung führend betätigt, für sie Mitglieder wirbt, aushebt oder militärisch oder sonst zum Kampf ausbildet oder die Verbindung mit Kampfmitteln, Verkehrsmitteln oder Einrichtungen zur Nachrichtenübermittlung ausrüstet oder mit Geldmitteln oder sonst in erheblicher Weise unterstützt, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

(2) Nach Abs. 1 ist nicht zu bestrafen, wer freiwillig, bevor die Behörde (§ 151 Abs. 3) von seinem Verschulden erfahren hat, alles, was ihm von der Verbindung und ihren Plänen bekannt ist, zu einer Zeit, da es noch geheim ist, einer solchen Behörde aufdeckt.

Ansammeln von Kampfmitteln

§ 280. (1) Wer Waffen, Munition oder andere Kampfmittel an sich bringt, besitzt oder einem anderen verschafft, um eine größere Zahl von Menschen zum Kampf auszurüsten, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

(2) Nach Abs. 1 ist nicht zu bestrafen, wer freiwillig, bevor die Behörde (§ 151 Abs. 3) von seinem Verschulden erfahren hat, die Kampfmittel auf Dauer unbrauchbar macht, einer solchen Behörde übergibt oder es ihr ermöglicht, der Kampfmittel habhaft zu werden.

Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen

§ 282. (1) Wer in einem Druckwerk, im Rundfunk oder sonst auf eine Weise, daß es einer breiten Öffentlichkeit zugänglich wird, zu einer mit Strafe bedrohten Handlung auffordert, ist, wenn er nicht als an dieser Handlung Beteiligter (§ 12) mit strengerer Strafe bedroht ist, mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

(2) Ebenso ist zu bestrafen, wer auf die im Abs. 1 bezeichnete Weise eine vorsätzlich begangene, mit einer ein Jahr übersteigenden Freiheitsstrafe bedrohte Handlung in einer Art gutheißt, die geeignet ist, das allgemeine Rechtsempfinden zu empören oder zur Begehung einer solchen Handlung aufzureizen.

Verhetzung

§ 283. (1) Wer öffentlich auf eine Weise, die geeignet ist, die öffentliche Ordnung zu gefährden, oder wer für eine breite Öffentlichkeit wahrnehmbar zu Gewalt gegen eine Kirche oder Religionsgesellschaft oder eine andere nach den Kriterien der Rasse, der Hautfarbe, der Sprache, der Religion oder Weltanschauung, der Staatsangehörigkeit, der Abstammung oder nationalen oder ethnischen Herkunft, des Geschlechts, einer Behinderung, des Alters oder der sexuellen Ausrichtung definierte Gruppe von Personen oder gegen ein Mitglied einer solchen Gruppe ausdrücklich wegen dessen Zugehörigkeit zu dieser Gruppe auffordert oder aufreizt, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

(2) Ebenso ist zu bestrafen, wer für eine breite Öffentlichkeit wahrnehmbar gegen eine in Abs. 1 bezeichnete Gruppe hetzt oder sie in einer die Menschenwürde verletzenden Weise beschimpft und dadurch verächtlich zu machen sucht.

Sprengung einer Versammlung

§ 284. Wer eine Versammlung, einen Aufmarsch oder eine ähnliche Kundgebung, die nicht verboten sind, mit Gewalt oder durch Drohung mit Gewalt verhindert oder sprengt, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

Verhinderung oder Störung einer Versammlung

§ 285. Wer eine nicht verbotene Versammlung dadurch verhindert oder erheblich stört, daß er

1. den Versammlungsraum unzugänglich macht,
2. eine zur Teilnahme berechtigte Person am Zutritt hindert oder ihr den Zutritt erschwert oder ihr die Teilnahme an der Versammlung durch schwere Belästigungen unmöglich macht oder erschwert,
3. in die Versammlung unbefugt eindringt oder
4. eine zur Leitung oder Aufrechterhaltung der Ordnung berufene Person verdrängt oder sich einer ihrer auf den Verlauf der Versammlung bezüglichen Anordnungen tätlich widersetzt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Hochverräterische Angriffe gegen einen fremden Staat

§ 316. (1) Wer es im Inland unternimmt (§ 242 Abs. 2), mit Gewalt oder durch Drohung mit Gewalt die Verfassung eines fremden Staates zu ändern oder ein zu einem fremden Staat gehörendes Gebiet abzutrennen, ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.

(2) § 243 gilt entsprechend.

Militärischer Nachrichtendienst für einen fremden Staat

§ 319. Wer im Inland für eine fremde Macht oder eine über- oder zwischenstaatliche Einrichtung einen militärischen Nachrichtendienst einrichtet oder betreibt oder einen solchen Nachrichtendienst wie immer unterstützt, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

Verbotene Unterstützung von Parteien bewaffneter Konflikte

§ 320. (1) Wer wissentlich im Inland während eines Krieges oder eines bewaffneten Konfliktes, an denen die Republik Österreich nicht beteiligt ist, oder bei unmittelbar drohender Gefahr eines solchen Krieges oder Konfliktes für eine der Parteien

1. eine militärische Formation oder ein Wasser-, ein Land- oder ein Luftfahrzeug einer der Parteien zur Teilnahme an den kriegerischen Unternehmungen ausrüstet oder bewaffnet,
2. ein Freiwilligenkorps bildet oder unterhält oder eine Werbestelle hiefür oder für den Wehrdienst einer der Parteien errichtet oder betreibt,
3. Kampfmittel entgegen den bestehenden Vorschriften aus dem Inland ausführt oder durch das Inland durchführt,
4. für militärische Zwecke einen Finanzkredit gewährt oder eine öffentliche Sammlung veranstaltet oder
5. unbefugt eine militärische Nachricht übermittelt oder zu diesem Zweck eine Fernmeldeanlage errichtet oder gebraucht, ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.

(2) Abs. 1 ist in den Fällen nicht anzuwenden, in denen

1. ein Beschluss des Sicherheitsrates der Vereinten Nationen,
2. ein Beschluss auf Grund des Titels V des Vertrages über die Europäische Union,
3. ein Beschluss im Rahmen der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) oder
4. eine sonstige Friedensoperation entsprechend den Grundsätzen der Satzung der Vereinten Nationen, wie etwa Maßnahmen zur Abwendung einer humanitären Katastrophe oder zur Unterbindung schwerer und systematischer Menschenrechtsverletzungen, im Rahmen einer internationalen Organisation

durchgeführt wird.

Verbotsgesetz (gesamtes Verbotsgesetz)

AußWG (Außenwirtschaftsgesetz 2011)

Gerichtlich strafbare Handlungen im Verkehr mit Drittstaaten
§ 79. (1) Wer

1. entgegen einem Verbot gemäß diesem Bundesgesetz, gemäß einer auf seiner Grundlage erlassenen Verordnung oder aufgrund von unmittelbar anwendbarem Recht der Europäischen Union im Sinne von § 1 Abs. 1 Z 24 lit. a oder b Güter einführt, ausführt, durchführt oder zwischen Drittstaaten vermittelt, technische Unterstützung leistet oder einen sonstigen Vorgang durchführt,
2. ohne eine gemäß diesem Bundesgesetz, gemäß einer auf seiner Grundlage erlassenen Verordnung oder einem auf seiner Grundlage erlassenen Bescheid oder aufgrund von unmittelbar anwendbarem Recht der Europäischen Union im Sinne von § 1 Abs. 1 Z 24 lit. a oder b erforderliche Genehmigung Güter einführt, ausführt, durchführt oder zwischen Drittstaaten vermittelt, technische Unterstützung leistet oder einen sonstigen Vorgang durchführt,
3. eine Genehmigung im Sinne von Z 2 durch unrichtige oder unvollständige Angaben erschleicht,
4. einen Genehmigungsbescheid im Sinne von Z 2 zur Verwendung durch einen Nichtberechtigten entgeltlich oder unentgeltlich überlässt oder übernimmt,
5. Güter, für deren Ausfuhr, Durchfuhr oder Vermittlung zwischen Drittstaaten eine Genehmigung im Sinne von Z 2 erteilt wurde, nach der zollamtlichen Abfertigung in ein anderes als das in der Genehmigung genannte Bestimmungsland verbringt oder verbringen lässt, sofern die Ausfuhr in dieses Land aufgrund dieses Bundesgesetzes, aufgrund einer auf dessen Grundlage erlassenen Verordnung oder einem auf dessen Grundlage erlassenen Bescheid oder aufgrund von unmittelbar anwendbarem Recht der Europäischen Union im Sinne von § 1 Abs. 1 Z 24 lit. a oder b verboten oder genehmigungspflichtig ist,
6. zur Umgehung einer Genehmigungspflicht im Sinne von Z 2 oder eines Verbotes im Sinne von Z 1 Güter zunächst in einen anderen EU-Mitgliedstaat verbringt oder in einen Drittstaat ausführt, um sie in weiterer Folge in einen anderen Drittstaat weiterzuleiten oder weiterleiten zu lassen, für den eine Genehmigungspflicht oder ein Verbot aufgrund dieses Bundesgesetzes oder aufgrund von unmittelbar anwendbarem Recht der Europäischen Union im Sinne von § 1 Abs. 1 Z 24 lit. a oder b gilt,
7. für die in Z 2 genannten Vorgänge durch unrichtige oder unvollständige Angaben die Erteilung einer Globalgenehmigung gemäß § 17 erschleicht,
8. eine Allgemeingenehmigung im Sinne von § 1 Abs. 1 Z 26 lit. a oder b für die Ausfuhr, Durchfuhr oder Vermittlung zwischen Drittstaaten von Gütern mit doppeltem Verwendungszweck entgegen den Vorschriften dieses Bundesgesetzes, einer auf seiner Grundlage erlassenen Verordnung oder aufgrund von unmittelbar anwendbarem Recht der Europäischen Union im Sinne von § 1 Abs. 1 Z 24 lit. a verwendet,
9. eine Allgemeingenehmigung im Sinne von Z 8 verwendet, obwohl er das Recht dazu gemäß § 60 Abs. 1 verloren hat oder dieses Recht ihm gegenüber gemäß § 60 Abs. 3 ausgesetzt ist,

10. gegen eine Auflage in einem Genehmigungsbescheid im Sinne von Z 2 verstößt,
11. die Vorschreibung einer Auflage in einem Genehmigungsbescheid im Sinne von Z 2 durch unrichtige oder unvollständige Angaben hintanhält,
12. Güter entgegen einer gemäß § 32 Abs. 2 vorgeschriebenen Ausfuhrbeschränkung aus der Europäischen Union ausführt, ohne die Zustimmung Österreichs gemäß § 35 erhalten zu haben,
13. durch Unterlassen der Information gemäß § 55 Abs. 1 die Erteilung einer Ausfuhrgenehmigung erschleicht oder die Vorschreibung einer Auflage im Ausfuhrgenehmigungsbescheid hintanhält,
14. den Widerruf gemäß § 57 einer Genehmigung im Sinne von Z 2 oder die Vorschreibung einer nachträglichen Auflage gemäß § 57 in einer solchen Genehmigung durch unrichtige oder unvollständige Angaben hintanhält,
15. eine Genehmigung im Sinne von Z 2 entgegen einem Widerruf gemäß § 57 weiter verwendet,
16. einen Vorgang gemäß § 15 Abs. 1 nach Mitteilung des Bestehens der Genehmigungspflicht ohne Genehmigung durchführt,
17. einen gemäß § 19 gemeldeten Vorgang vor Ablauf einer der in § 19 Abs. 6 genannten Fristen durchführt,
18. durch Verletzung einer in einer Verordnung aufgrund von § 19 Abs. 1 iVm § 25, in einer Verordnung aufgrund von § 19 Abs. 2 oder 3 oder aufgrund von unmittelbar anwendbarem Recht der Europäischen Union im Sinne von § 1 Abs. 1 Z 24 lit. a oder b festgelegten Meldepflicht oder durch Verletzung der in einer Verordnung aufgrund von § 19 Abs. 5 festgelegten Nachweispflicht die Vorschreibung einer Genehmigungspflicht gemäß § 19 Abs. 7 oder eine Mitteilung über das Bestehen einer Genehmigungspflicht gemäß § 15 Abs. 1 hintanhält,
19. Güter im Widerspruch zu einem Untersagungsbescheid gemäß § 20 Abs. 3 Z 2 ausführt oder durchführt,
20. die Erlassung eines Untersagungsbescheides gemäß § 20 Abs. 3 Z 2 durch unrichtige oder unvollständige Angaben hintanhält,
21. durch unrichtige oder unvollständige Angaben einen Bescheid aufgrund einer Voranfrage gemäß § 62 über das Nichtbestehen eines Verbots oder einer Genehmigungspflicht für die Einfuhr, Ausfuhr, Durchfuhr, Vermittlung zwischen Drittstaaten, für technische Unterstützung oder sonstige Vorgänge oder über den Umstand, dass ein solcher Vorgang genehmigt werden kann oder dass eine Auflage nicht vorzuschreiben ist, erschleicht,
22. Güter aus der Europäischen Union ohne die für den Vorgang nach dem Recht des EU-Mitgliedstaates, aus dem die Ausfuhr erfolgt, erforderliche Ausfuhrgenehmigung vermittelt,
23. eine Genehmigungspflicht für oder ein Verbot von technischer Unterstützung dadurch umgeht, dass diese technische Unterstützung innerhalb des Bundesgebietes an Personen erbracht wird, die dieses technische Wissen danach außerhalb der Europäischen Union verwerten oder weitergeben sollen, oder
24. ein Verbot im Sinne von Z 1 oder eine Genehmigungspflicht im Sinne von Z 2 dadurch umgeht, dass er Rechte zur Produktion von Gütern in einem Drittstaat oder Immaterialgüterrechte zur Verwertung in einem Drittstaat überträgt,

25. einen Vorgang im Sinne von § 1 Abs. 1 Z 10 lit. b ohne Genehmigung gemäß § 25a Abs. 2 oder 11 durchführt oder gegen eine Auflage in einem Genehmigungsbescheid gemäß § 25a Abs. 9 Z 2 lit. a oder gemäß § 25a Abs. 12 iVm Abs. 9 Z 2 lit. a verstößt oder
26. durch unrichtige oder unvollständige Angaben eine Genehmigung gemäß § 25a Abs. 8, 9 oder Abs. 12 erschleicht oder die Vorschreibung von Auflagen in einem Genehmigungsbescheid gemäß § 25a Abs. 9 oder Abs. 12 hintanhält,

ist vom Gericht mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

(2) Wer eine der in Abs. 1 mit Strafe bedrohten Handlungen

1. gewerbsmäßig, oder
2. durch Täuschung über Tatsachen unter Benützung einer falschen oder verfälschten Urkunde, falscher oder verfälschter Daten, eines anderen solchen Beweismittels oder eines unrichtigen Messgeräts

begeht, ist vom Gericht mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.

(3) Wer fahrlässig eine der in den Abs. 1 Z 1, 2, 4, 8, 9, 10, 12, 15, 16, 17 oder 19 bezeichneten Handlungen begeht, ist mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Gerichtlich strafbare Handlungen im Verkehr innerhalb der Europäischen Union
§ 80. (1) Wer

1. Güter innerhalb der Europäischen Union ohne eine nach diesem Bundesgesetz, gemäß einer auf seiner Grundlage erlassenen Verordnung oder eines auf seiner Grundlage erlassenen Bescheides oder aufgrund von unmittelbar anwendbarem Recht der Europäischen Union im Sinne von § 1 Abs. 1 Z 24 lit. a erforderliche Genehmigung oder ohne Genehmigung eines anderen EU-Mitgliedstaates gemäß § 33 verbringt,
2. eine Genehmigung für die Verbringung von Gütern innerhalb der Europäischen Union im Sinne von Z 1 durch unrichtige oder unvollständige Angaben erschleicht,
3. einen Genehmigungsbescheid im Sinne von Z 1 zur Verwendung durch einen Nichtberechtigten entgeltlich oder unentgeltlich überlässt oder übernimmt,
4. zur Umgehung einer Genehmigungspflicht im Sinne von Z 1 Güter zunächst in einen anderen EU-Mitgliedstaat verbringt, um sie in weiterer Folge in einen weiteren EU-Mitgliedstaat weiterzuleiten oder weiterleiten zu lassen, für den eine Genehmigungspflicht aufgrund dieses Bundesgesetzes oder aufgrund von unmittelbar anwendbarem Recht der Europäischen Union im Sinne von § 1 Abs. 1 Z 24 lit. a gilt,
5. für die in Z 1 genannten Vorgänge durch unrichtige oder unvollständige Angaben die Erteilung einer Globalgenehmigung gemäß § 30 erschleicht,
6. eine Globalgenehmigung im Widerspruch zu § 30 Abs. 3 verwendet,
7. für die in Z 1 genannten Vorgänge eine Allgemeingenehmigung im Sinne von § 1 Abs. 1 Z 24 lit. c entgegen den Bestimmungen dieses Bundesgesetzes oder einer auf seiner Grundlage erlassenen Verordnung verwendet,
8. eine Allgemeingenehmigung im Sinne von Z 7 verwendet, obwohl er das Recht dazu gemäß § 60 Abs. 1 verloren hat oder dieses Recht ihm gegenüber gemäß § 60 Abs. 3 ausgesetzt ist,
9. eine Allgemeingenehmigung im Sinne von Z 7 gegenüber einem Unternehmen

verwendet, gegenüber dem die Geltung dieser Allgemeingenehmigung gemäß § 29 Abs. 2 ausgesetzt ist,

10. gegen eine Auflage in einem Genehmigungsbescheid im Sinne von Z 1 verstößt,
11. die Vorschreibung einer Auflage in einem Genehmigungsbescheid im Sinne von Z 1 durch unrichtige oder unvollständige Angaben hintanhält,
12. den Widerruf gemäß § 57 einer Genehmigung im Sinne von Z 1 oder die Vorschreibung einer nachträglichen Auflage gemäß § 57 in einer solchen Genehmigung durch unrichtige oder unvollständige Angaben hintanhält,
13. eine Genehmigung im Sinne von Z 1 entgegen einem Widerruf gemäß § 57 weiter verwendet,
14. gegen eine Auflage in einem Genehmigungsbescheid eines anderen EU-Mitgliedstaates gemäß § 33 verstößt,
15. durch Unterlassung einer Meldung gemäß § 33 Abs. 3 die Vorschreibung einer Genehmigungspflicht gemäß § 33 Abs. 2 hintanhält,
16. eine Verbringung innerhalb der Europäischen Union vor Ablauf der in § 33 Abs. 2 und 4 genannten Fristen durchführt, oder
17. einen Zustimmungsbescheid gemäß § 35 durch unrichtige oder unvollständige Angaben erschleicht,
18. durch unrichtige oder unvollständige Angaben einen Bescheid aufgrund einer Voranfrage gemäß § 62 über das Nichtbestehen einer Genehmigungspflicht für eine Verbringung innerhalb der Europäischen Union oder über den Umstand, dass ein solcher Vorgang genehmigt werden kann oder dass eine Auflage nicht vorzuschreiben ist, erschleicht,

ist vom Gericht mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

(2) Ebenso ist zu bestrafen, wer

1. durch unrichtige oder unvollständige Angaben
   a) die Erlassung eines Zertifizierungsbescheides gemäß § 37 erschleicht,
   b) die Verlängerung der Geltungsdauer eines solchen Bescheids gemäß § 38 Abs. 2 oder 3 erschleicht oder
   c) die Festlegung einer Auflage in einem solchen Bescheid hintanhält, oder
2. eine Überprüfung gemäß § 39 durch unrichtige oder unvollständige Angaben oder durch Unterlassung einer Meldung gemäß § 37 Abs. 2 Z 2 oder § 39 Abs. 1 hintanhält,
3. durch unrichtige oder unvollständige Angaben einen Bestätigungsbescheid gemäß § 39 Abs. 3 erschleicht oder die Vorschreibung einer Auflage in einem solchen Bescheid hintanhält, oder
4. einen Bescheid zum Widerruf oder zur Aussetzung eines Zertifikats gemäß § 40 durch unrichtige oder unvollständige Angaben oder durch Unterlassung einer Meldung gemäß § 37 Abs. 2 Z 2 oder § 39 Abs. 1 hintanhält.

(3) Wer eine der in den Abs. 1 und 2 mit Strafe bedrohten Handlungen

1. gewerbsmäßig, oder
2. durch Täuschung über Tatsachen unter Benützung einer falschen oder verfälschten Urkunde, fa eines unrichtigen Messgeräts

begeht, ist vom Gericht mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

(4) Wer fahrlässig eine der in Abs. 1 Z 1, 3, 6, 7, 8, 9, 10, 13, 14 oder 16 bezeichneten Handlungen begeht, ist mit Freiheitsstrafe bis zu sechs Monaten oder Geldstrafe bis zu 180 Tagessätzen zu bestrafen.

Gerichtlich strafbare Handlungen im Zusammenhang mit Chemikalien und Gütern, die der BTK unterliegen

§ 81. (1) Wer

1. einem Verbot gemäß § 41 zuwiderhandelt,
2. eine in § 42 Abs. 1 oder 2 genannte Tätigkeit oder einen dort genannten Vorgang ohne Genehmigung durchführt,
3. eine Genehmigung im Sinne von Z 2 durch unrichtige oder unvollständige Angaben erschleicht,
4. einen Genehmigungsbescheid im Sinne von Z 2 zur Verwendung durch einen Nichtberechtigten entgeltlich oder unentgeltlich überlässt oder übernimmt,
5. für die in Z 2 genannten Tätigkeiten und Vorgänge durch unrichtige oder unvollständige Angaben die Erteilung einer Globalgenehmigung gemäß § 43 erschleicht,
6. gegen eine Auflage in einem Genehmigungsbescheid im Sinne von Z 2 verstößt,
7. die Vorschreibung einer Auflage gemäß § 54 in einem Genehmigungsbescheid im Sinne von Z 2 durch unrichtige oder unvollständige Angaben hintanhält,
8. den Widerruf oder die Festlegung einer nachträglichen Auflage gemäß § 57 Abs. 2 in einem Genehmigungsbescheid im Sinne von Z 2 durch unrichtige oder unvollständige Angaben hintanhält, oder
9. durch unrichtige oder unvollständige Angaben einen Bescheid aufgrund einer Voranfrage gemäß § 62 über das Nichtbestehen eines Verbots im Sinne von Z 1 oder einer Genehmigungspflicht im Sinne von Z 2 oder über den Umstand, dass ein solcher Vorgang genehmigt werden kann oder dass eine Auflage nicht vorzuschreiben ist, erschleicht,

ist vom Gericht mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

(2) Wer eine der in Abs. 1 mit Strafe bedrohten Handlungen

1. gewerbsmäßig, oder
2. durch Täuschung über Tatsachen unter Benützung einer falschen oder verfälschten Urkunde, falscher oder verfälschter Daten, eines anderen solchen Beweismittels oder eines unrichtigen Messgeräts

begeht, ist vom Gericht mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.

(3) Wer fahrlässig eine der in den Abs. 1 Z 1, 2, 4 oder 6 bezeichneten Handlungen begeht, ist mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Beitrag zu ABC-Waffen

§ 82. (1) Wer durch eine der in den §§ 79 bis 81 mit Strafe bedrohten Handlungen einen Beitrag zur Herstellung, Verbreitung, Prüfung oder Instandhaltung von ABC-Waffen sowie ABC-waffenfähigen Trägersystemen leistet, ist vom Gericht mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.

(2) Wer eine der in Abs. 1 mit Strafe bedrohten Handlungen

1. gewerbsmäßig, oder
2. durch Täuschung über Tatsachen unter Benützung einer falschen oder verfälschten Urkunde, falscher oder verfälschter Daten, eines anderen solchen Beweismittels oder eines unrichtigen Messgeräts

begeht, ist mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren zu bestrafen.

(3) Wer fahrlässig eine der in den §§ 79 bis 81 mit Strafe bedrohten Handlungen begeht und dadurch einen Beitrag zur Herstellung, Verbreitung, Prüfung oder Instandhaltung von ABC-Waffen sowie ABC-waffenfähigen Trägersystemen leistet, ist vom Gericht mit Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

KMG (Kriegsmaterialgesetz)

Gerichtliche Strafbestimmungen
§ 7. (1) Wer

1. Kriegsmaterial ohne die hiefür nach diesem Bundesgesetz erforderliche Bewilligung ein-, aus- oder durchführt oder vermittelt oder, im Falle des Verbringens durch einen Transporteur, von diesem ein-, aus- oder durchführen lässt oder
2. durch unrichtige oder unvollständige Angaben, Erklärungen oder Nachweise die Erteilung einer Bewilligung erschleicht oder
3. durch unrichtige oder unvollständige Angaben, Erklärungen oder Nachweise die Erteilung von Ausfuhrbeschränkungen, die Festlegung von Bedingungen, die Vornahme einer Einschränkung oder den Widerruf einer Bewilligung hintanhält oder
4. Informationspflichten gemäß § 4 Abs. 4 nicht erfüllt,

ist, sofern die Tat nicht nach anderen Bestimmungen mit strengerer Strafe bedroht ist, vom ordentlichen Gericht mit Freiheitsstrafe bis zu drei Jahren zu bestrafen. Wer die Tat gewerbsmäßig oder durch Täuschung über Tatsachen unter Benützung einer falschen oder verfälschten Urkunde, falscher oder verfälschter Daten oder eines anderen solchen Beweismittels begeht, ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.

(2) Ebenso ist zu bestrafen, wer Kriegsmaterial entgegen unmittelbar anwendbarem Recht der Europäischen Union ein-, aus- oder durchführt oder vermittelt.

(2a) Wer fahrlässig eine der in Abs. 1 Z 1, 3 oder 4 oder Abs. 2 bezeichneten Handlungen begeht, ist, sofern die Tat nicht nach anderen Bestimmungen mit strengerer Strafe bedroht ist, vom ordentlichen Gericht mit Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(3) Wird Kriegsmaterial entsprechend den zollrechtlichen Vorschriften zum Grenzzollamt verbracht und diesem ordnungsgemäß gestellt und erklärt, so tritt die Strafbarkeit nach Abs. 1 oder 2 erst ein, wenn das Kriegsmaterial trotz Fehlens der erforderlichen Bewilligung in einer für die Ein-, Aus- oder Durchfuhr vorgesehenen Art des Zollverfahrens abgefertigt worden ist.

SPG (Sicherheitspolizeigesetz)

Vorbeugender Schutz von Rechtsgütern

§ 22. (1) Den Sicherheitsbehörden obliegt der besondere Schutz

2. der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit;

6. von Einrichtungen, Anlagen, Systemen oder Teilen davon, die eine wesentliche Bedeutung für die Aufrechterhaltung der öffentlichen Sicherheit, die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie, die Verhütung oder Bekämpfung von Katastrophen, den öffentlichen Gesundheitsdienst, die öffentliche Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern oder den öffentlichen Verkehr haben (kritische Infrastrukturen).