Policy Brief
Polizeiliches Staatsschutzgesetz

Verein Arbeitskreis Vorratsdaten (ZVR: 140062668)
Kirchberggasse 7/5, 1070 Wien, www.akvorrat.at
3. September 2015

1. Vorwort

Der Arbeitskreis Vorratsdaten befürwortet an sich die Einführung einer eigenen Gesetzesgrundlage für das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung und die neun Landesämter für Verfassungsschutz (in der Folge: Staatsschutz) und die Entkoppelung der Aufgaben vom Sicherheitspolizeigesetz. Jedoch fehlt aus Sicht des AKVorrat eine grundlegende Evaluierung der bisherigen Überwachungssituation in Österreich als Vorbedingung für die Normierung weiterer Überwachungsbefugnisse[1]. Dies vorausschickend ist der AKVorrat wie immer bemüht, sich trotz dieses grundlegenden Mangels konstruktiv im gesellschaftspolitischen Diskurs einzubringen. In diesem Sinne versucht der folgende Überblick dennoch, abseits dieser fehlenden Grundlage, die Probleme des vorliegenden Entwurfs darzulegen und Lösungen anzubieten.

[1] Siehe das laufende Projekt zur Erstellung eines **H**andlungskatalogs zur **E**valuierung von **A**nti-**T**error-Gesetzen (kurz: HEAT) https://akvorrat.at/heat

2. Detailbemerkungen

a) Richtervorbehalt neben Rechtsschutzbeauftragtem

Problembeschreibung: Im aktuellen Entwurf gibt es keine unabhängige Kontrollinstanz, einzig der Rechtsschutzbeauftragte (RSB) beim BM.I ist für die Überprüfung/Einschränkung von Überwachungsmaßnahmen vorgesehen. Der Österreichische Rechtsanwaltskammertag hat in seiner Stellungnahme bereits von einem „*inner circle*" im Innenministerium gewarnt[2]. Diese Kritik zielt richtigerweise auf die mangelnde Distanz und Unabhängigkeit des Kontrollorgans gegenüber dem zu kontrollierenden BM.I ab. Der Staatsschutz kann auf alle sensiblen Datenquellen (inkl. Finanz- und Gesundheitsdaten) aus öffentlichen und privaten Quellen zugreifen, trotzdem ist der Rechtsschutz niedriger angesetzt, als im kürzlich verabschiedeten Finanzstrafgesetz.

Lösungsvorschlag: Nach dem Vorbild der kürzlich beschlossenen Reform zum Finanzstrafgesetz ist die interne Kontrolle des (im BMF neu geschaffenen) RSB durch eine externe gerichtliche Kontrolle („Richtervorbehalt") im Rahmen der Verwaltungsgerichtbarkeit zu ergänzen. Im Finanzstrafgesetz ist diese ergänzende Rechtsschutz-Architektur nicht nur für die Abfrage von Kontodaten sondern auch für IP-Adressen vorgesehen und daher absolut vergleichbar. Bei Fällen der Gefahr im Verzug kann eine Nachtragsmöglichkeit der gerichtlichen Genehmigung nach dem Vorbild der Strafprozessordnung normiert werden.

b) Gefährderdatenbank

Problembeschreibung: In der Gefährderdatenbank werden vom Staatsschutz die Daten von verdächtigen, aber auch komplett unbescholtenen, Menschen für 6 Jahre lang gespeichert. Der Zweck für die Datenverarbeitung und die Anforderungen an „Betroffene" und „Kontakt- und Begleitpersonen" sind mangels Definition potentiell so breit zu verstehen, dass jeder Facebook Freund oder einmalige Besucher eines Vereinslokals betroffen sein kann. Durch den enorm breit gefassten Zweck „*Bewertung von wahrscheinlichen Gefährdungen sowie zum Erkennen von Zusammenhängen und Strukturen*" können auch sensible Daten wie Gewerkschaftszugehörigkeit, sexuelle Orientierung oder Religion über all diese Personen gespeichert werden. Ein Datenaustausch mit internationalen Geheimdiensten ist explizit vorgesehen. Das Grundrecht

[2] Siehe Seite 2 http://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_03716/imfname_412688.pdf

der Betroffenen auf den Schutz ihrer persönlichen Daten ist im aktuellen Entwurf nicht gewahrt.

Lösungsvorschlag:

- Senkung der Gesamtspeicherdauer und der Prüfungsabstände für die Datenlöschung.
- Der Zweck der Datenanwendung in PStSG §12 sollte wie folgt geändert werden: „zum Zweck der Bewertung von ~~warhscheinlichen~~ **konkreten** Gefährdungen ~~sowie zum Erkennen von Zusammenhängen und Strukturen~~ mittels operativer oder strategischer Analyse."
- Materielle Einschränkungen (konkrete Verdachtsbegründungen) sollten in der Datenbank festgehalten werden müssen. Sie dokumentieren die Begründung der Speicherung und können zur Überprüfung der Zweckwidmung (Löschung) herangezogen werden.
- Die Generalvollmacht zur Speicherung sensibler Daten in §12 Abs 1 Ziffer 5, letzter Satz muss gestrichen werden.

c) Konkretisierung von "Gruppierungen"

Problembeschreibung: Überwachungsbefugnisse können für ganze „Gruppierungen" erteilt werden. Eine Gruppierung ist weder legal definiert, noch muss sie im konkreten Einzelfall für eine Überwachungsbefugnis genau spezifiziert werden. Dadurch wird eine Verhältnismäßigkeitsprüfung im Einzelfall praktisch unmöglich gemacht und es entsteht die Gefahr von blanko Überwachungsbefugnissen für ganze Bevölkerungsschichten. Ab wann eine Person einer Gruppierung zuzurechnen ist und was eine Gruppierung ausmacht ist im Gesetz nicht spezifiziert.

Lösungsvorschlag: Notwendig ist eine Legaldefinition einer „Gruppierung" und vor dem Einleiten von Überwachungsmaßnahmen muss eine Konkretisierung der spezifischen Gruppierung im Rahmen der Begründung der Maßnahme erfolgen. Die Maßnahme muss auf den notwendigsten Rahmen an "Verdächtigen" beschränkt sein. (Schlagwort gelindestes Mittel) (PStSG §6 + §11)

d) Definition eines „verfassungsgefährdenden Angriffs"

Problembeschreibung: Ein Ziel der vorliegenden Reform ist die klare Abgrenzung der Aufgabengebiete von Staatsschutz und Polizeibehörden. Dem Staatsschutz obliegt unter Anderem der Schutz vor „verfassungsgefährdenden Angriffen". Eben jener Begriff ist jedoch zu breit und sehr unklar definiert. Einer der Kritikpunkte der Bischofskonferenz und

der Evangelischen Kirche in deren Stellungnahmen im Begutachtungsverfahren [3] war - neben der defakto Abschaffung des Beichtgeheimnisses - das Kriterium der „religiösen oder weltanschaulichen Motivation“, um Straftaten auf die Stufe eines „verfassungsgefährdenden Angriffes“ zu heben. Religiöse Beweggründe erschweren für sich genommen keine Straftaten. Die Motivation fast jeder Straftat könnte letztlich weltanschaulich begründet werden (Regeln des Charma). Eine klarere Definition diesen zentralen Begriffes, sowie trennschärfere Kriterien für die Abgrenzung zu anderen Tatbeständen, wären dringend notwendig.

Lösungsvorschlag: Klare Legaldefinition eines verfassungsgefährdenden Angriffs, anstatt verschachtelter Verweise auf andere Paragraphen, und Einschränkung auf wirklich schwere Straftaten. Statt dem Kriterium der „religiösen oder weltanschaulichen Motivation“ könnte die „demokratiefeindliche Ausrichtung“ gewisse Straftaten auf die Stufe eines „verfassungsgefährdenden Angriffs“ heben.
(PStSG § 6 Abs 1 Z 2+ § 10 Abs 1 Z 2)

e) Schranken zur Internetüberwachung

Problembeschreibung: Alle im Internet öffentlich verfügbaren Quellen sollen für Ermittlungen herangezogen werden können (Stichwort: „Open Source Intelligence“ oder OSINT). Im Rahmen der StPO gibt es für diese Ermittlungsmaßnahme keine Rechtsgrundlage. Somit überragen die Befugnisse des BVT hier die Befugnisse der Kriminalpolizei bei der Erfüllung ihrer Aufgaben nach der StPO.

Lösungsvorschlag: Jede zur Internetüberwachung eingesetzte Software muss in einer Verordnung des Innenministeriums taxativ aufgelistet werden (PStSG §10). Die Beschaffungsprozesse müssen transparent gestaltet werden und die Funktionalität der eingesetzten Software muss klar spezifiziert sein und auf diese Funktionsbeschreibung beschränkt werden.

f) Kontroll- und Transparenzdefizite im Staatsschutz

Problembeschreibung: Neben dem internen Rechtsschutzbeauftragten und seinem jährlichen Sicherheitsbericht, welcher dem Vernehmen nach nur einen Bruchteil der bereits aktuell aufkommenden Konflikte widerspiegelt, und dem Verfassungsschutzbericht, welcher nur die Selbstdarstellung der Behörde zusammenfasst, fehlt es gänzlich an Transparenz- und

[3] Siehe http://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_03734/index.shtml und http://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_03730/index.shtml

Kontrollmechanismen. Angesichts der massiven Befugnisse des Staatsschutzes sind diese Defizite unverantwortlich.
Weder sind die neun Landesämter dem Bundesamt für Verfassungsschutz unterstellt, noch gibt es eine klare Aufgabentrennung oder Kompetenzbündelung zwischen ihnen oder explizite Regeln zu deren Organisation oder Geschäftsordnung[4].
Wie der Innsbrucker Rechtsanwalt Christian Ortner in seiner Stellungnahme herausstrich, können der Direktor für Öffentliche Sicherheit und der Direktor des Staatsschutzes unter einander ausmachen, in welchen Fällen die Innenministerin entscheidet und wann sie selbst entscheiden[5].

Lösungsvorschlag: Es braucht umfängliche Transparenz- und Kontrollmechanismen im Bezug auf die Datenerhebung, -verarbeitung und -weitergabe durch den Staatsschutz. Für die Datenerhebung im Bereich Telekommunikation und Internetzugang muss die „Durchlaufstelle“ aus der Einführung der Vorratsdatenspeicherung zu Anwendung kommen. Dieses bereits existierende, österreichische System garantiert die Vertraulichkeit und Nachvollziehbarkeit im Datenaustausch zwischen Behörden und privaten Firmen. Ein Parlamentarisches Kontrollgremium mit voller Akteneinsicht wäre demokratiepolitisch angesichts der fehlenden Kontrolle der Innenministerin ebenfalls sinnvoll.

g) Vertrauenspersonen

Problembeschreibung: Es bedarf keiner Begründung der Sicherheitsbehörde, warum eine Vertrauensperson (V-Person) als vertrauenswürdig eingestuft wird und warum ihr Einsatz notwendig ist. Des Weiteren gibt es keine Rechtsgrundlage für die Offenlegung der Identität des „Spitzels“ vor Gericht bei benötigter Zeugenaussage. Hier besteht das Risiko, dass die zentralen Garantien für ein faires Verfahren erodiert werden. Dadurch schwebt über jedem, aufgrund von Informationen einer V-Person entschiedenen Verfahren, potentiell ein Nichtigkeitsgrund.

Lösungsvorschlag: Streichung der V-Leute; Alternativ: Stärkere Hürden in der Strafprozessordnung für die Wahl und den Einsatz von V-Leuten. Klare Regeln zu den Grenzen anonymer Aussagen von V-Leuten und schließlich Beweisverwertungsverbote.

---

[4] siehe PStSG §2 und §3
[5] siehe Seite 5 http://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_03750/index.shtml und http://johanneshuber.me/2015/08/27/brisante-reform-allwissender-staatsschutz-halbwissende-innenministerin/

h) begründeter Gefahrenverdacht

Problembeschreibung: Zur Einleitung von Ermittlungen gibt es laut Regierungsvorlage keine Notwendigkeit einer Begründung eines Verdachtes. Es bedarf zwar einer Begründung des Gefahrendverdachts, jedoch ist nicht geregelt, wen die Beweislast trifft, an wen die Begründung zur Überprüfung zu ergehen hat und wer über die Statthaftigkeit der Begründung entscheidet. Hier ist eine prozessuale Absicherung der Begründung jedes Verdachtes ex-ante, wie zum Beispiel Genehmigung und Bestätigung eines Richters, unabdingbar.

Lösungsvorschlag: Es braucht eine klare Regelung über die Beweislast der Begründung und wo diese festzuhalten ist.
(§ 6 Abs 1 Z 2 iV § 22 Abs 2 SPG + § 10 Abs 1 Z 1)

i) Verdachtsmeldungen aus dem Ausland

Problembeschreibung: Im Gegensatz zu Verdachtsmeldungen bei verfassungsgefährdenden Angriffen im Inland bedarf es bei Verdachtsmeldungen von ausländischen Sicherheitsbehörden (bei verfassungsgefährdenden Angriffen im Ausland) keiner Begründung. Bei Meldungen aus dem Ausland bestehen also deutlich niedrigere Rechtsschutzanforderungen als bei Verdachtsmeldungen von inländischen Sicherheitsbehörden.

Lösungsvorschlag: "...,die im **begründeten** Verdacht stehen,..."
(§ 6 Abs 1 Z 3 + § 10 Abs 1 Z 3)

3. Schlussbemerkungen

Der geplante Staatsschutz etabliert in Österreich einen Inlandsgeheimdienst mit hierzulande bisher unbekannten Überwachungsbefugnissen, welche nicht einmal vor dem Amtsgeheimnis halt machen, gleichzeitig ist es aber eine Kapitulation in Sachen Rechtsschutz, Behördenkontrolle und Transparenz.
Unter dem Deckmantel der Extremismus-Bekämpfung wird mit diesem Gesetz die rechtsstaatliche Trennung zwischen Polizeilichem und Geheimdienst-Bereich abgeschafft. Der Name „**polizeiliches** Staatsschutzgesetz“ erscheint wie eine bewusste Ablenkung. Der vom Leiter des BVT erhoffte internationale Datenaustausch mit anderen Diensten[6], der Fokus auf Extremismus, die große Intransparenz und die fehlenden Kontrollmechanismen bestätigen dies. Unverständlich sind auch die

[6] siehe https://www.youtube.com/watch?v=ROMR0ZV5vZk

fehlende parlamentarische Kontrolle und die scheinbare Aufgabe der Kontrolle durch die Innenministerin selbst. Angesichts der insbesondere durch Edward Snowden losgetretenen Debatte um unkontrollierbare Geheimdienste und weltweite Überwachungsskandale sollte Österreich aus diesen Erfahrungen lernen, anstatt wie im Fall der V-Leute Probleme mit Anlauf zu wiederholen.

Alle Erfahrungen der letzten Jahrzehnte haben gezeigt: einmal erteilte Überwachungsbefugnisse sind im Nachhinein nicht mehr abzubauen. Die Politik geht hier immer nur in eine Richtung. Wenn im parlamentarischen Prozess für dieses Gesetz nicht jetzt die notwendigen Sicherheitsschranken eingezogen werden, ist es zu spät.

Weitere Dokumente

- Analyse der Regierungsvorlage: http://is.gd/fB7ePC
- Analyse des Begutachtungsentwurfes: http://is.gd/ZdhIo7
- Handout zum Staatsschutzgesetz: http://is.gd/fGDh2E
- Kampagne zum Staatsschutzgesetz: https://www.staatsschutz.at

Rückfragekontakte

Ing. Mag. Dr. jur. Christof Tschohl
0650 7503718
christof.tschohl@akvorrat.at

Mag. Ewald Scheucher
+43 1 7109251
scheucher@scheucher.at

Thomas Lohninger BA
+43 680 123 86 11
thomas.lohninger@akvorrat.at