



PRESSE

KONFERENZ

VON

Peter Pilz

Sicherheitssprecher der Grünen

Freibrief für NSA und CIA

**DAS STAATSSCHUTZGESETZ,
SEINE DATENBANK, BND, NSA UND CIA**

WIEN, PRESSEBÜRO DER GRÜNEN

10.06.2015

Freibrief für NSA und CIA: DAS STAATSSCHUTZGESETZ, SEINE DATENBANK, BND, NSA UND CIA

Die CIA-Klausel

§ 11 Abs 2 PStSG:

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.

Diese Bestimmungen über die Amtshilfe finden sich in völkerrechtlichen Verträgen, im Polizeikooperationsgesetz und dem EU-Polizeikooperationsgesetz. Sie sind sehr weitgehend. Nur in Ausnahmefällen kann die Amtshilfe nach diesen Regeln abgelehnt werden.

In Zukunft sollen aber sogar die Daten der Analysedatenbank, in der zB bloße Kontaktpersonen und andere zur „Beurteilung der Wahrscheinlichkeit verfassungsgefährdender Angriffe“ gespeichert werden können, an ausländische Behörden weitergegeben werden dürfen.

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

Wie war es bisher? Analysedatenbanken waren im SPG vorgesehen um die Häufung bestimmter Delikte, zB Einbrüche, zur Kriminalitätsbekämpfung analysieren zu können. Die Weitergabe der Daten daraus war nach § 53a Abs 6 SPG aber auf die Strafverfolgung beschränkt:

Übermittlungen sind an Sicherheitsbehörden, Staatsanwaltschaften und ordentliche Gerichte für Zwecke der Strafrechtspflege und im Übrigen nur zulässig, wenn hierfür eine ausdrückliche gesetzliche Ermächtigung besteht.

Bei der neuen, umfassenden Analysedatenbank des Verfassungsschutzes sind dagegen jetzt ausdrücklich auch Übermittlungen aller darin gespeicherten Daten – und nicht etwa nur der Analyseergebnisse – an ausländische Sicherheitsbehörden vorgesehen.

Die Innenministerin erfüllt damit den amerikanischen Wunsch – und opfert den Datenschutz in Österreich.

Terrorist Screening Database

Bereits 2009 gab es Druck aus den USA, dass Österreich an der sogenannten „Terrorist Screening Database“ (TSDB) teilnimmt. Diese vom FBI geführte Liste enthält über 400.000 Personen.

So berichtete die „Presse“ am 25.3.2009¹:

Funktionieren soll der Datentausch auf zwei Ebenen. Für (mutmaßliche) Terroristen gibt es das sogenannte Terrorist Screening Center (TSC), eine Organisation des FBI, die bis heute die Namen von etwa 16.000 Personen gesammelt hat. Für „normale“ Verdächtige, die – in welchem Zusammenhang auch immer – in den Polizeicomputer geraten sind, gibt es eine zweite Datenbank. Nach Angaben des Heimatschutzes kooperieren bereits 25 Staaten mit den USA. Welche das sind, ist geheim.

Die Daten, die in das System gelangen, werden von den Amerikanern auch nicht auf ihre Zuverlässigkeit überprüft. Was bei Informationen von Nachrichtendiensten problematisch ist, weil es dafür keinen Rechtsschutz gibt. So wurde etwa ein in einem sensiblen Bereich tätiger Mitarbeiter des Flughafens Schwechat vom österreichischen Verfassungsschutz aufgrund nachweislich falscher Geheiminformationen für nicht vertrauenswürdig befunden und gekündigt. Problematisch ist der Datenverbund auch, weil Informationen 99 Jahre lang gespeichert werden sollen.

Weil auch Suchabfragen von Namen, die gar keine Treffer ergaben, 25 Jahre im System bleiben, können reisefreudige Personen und auch Geschäftsleute nach mehreren Abfragen automatisch zu Verdächtigen werden, befürchten Datenschützer. Bei der nächsten Einreise liege für den kontrollierenden Beamten der Verdacht nahe, dass die vielen Abfragen der Vergangenheit wohl einen speziellen Grund gehabt hätten. Das System produziere so seine Verdächtigen mit der Zeit selbst. Unabhängig davon, ob zur geprüften Person etwas vorliege oder nicht.

Während mittlerweile das zweite damals von den USA geforderte Abkommen – das sogenannte „Prüm-like Abkommen“ über den Austausch von Polizeidaten wie DNA oder Fingerabdrücken abgeschlossen wurde, verliefen die Verhandlungen über eine Teilnahme Österreichs an TSDB im Sand – unter anderem, weil Österreich über keine geeignete Datenbank zur Teilnahme verfügte.

Damit war der erste Versuch zur Eingliederung Österreichs in den US-Diensteverbund gescheitert. Jetzt unternimmt die Innenministerin den zweiten Versuch.

¹ <http://diepresse.com/home/politik/innenpolitik/464471/index>

Die Analysedatenbank

Fall 1:

Sitzblockaden gegen Nazi-Demos

In der letzten Zeit hat die Polizei in Wien vermehrt Personen, die Demonstrationen von Rechtsextremen zB mit Sitzblockaden behinderten, wegen § 285 StGB (Verhinderung oder Störung einer Versammlung) angezeigt. (siehe etwa die Anfrage 2253/J und die Beantwortung 2131/AB der XXV. GP).

Eine solche Tat gilt als „verfassungsgefährdender Angriff“ nach § 6 Abs 2 Z 3 PStSG.

Wenn also das BVT oder LVT im Vorfeld einer rechtsextremen Demo im Internet von Plänen über Sitzblockaden liest, könnte es einen Fall des „vorbeugenden Schutzes gegen verfassungsgefährdende Angriffe“ (§ 6 Abs 1 Z 2 PStSG) eröffnen und dann:

- über Anfragen an die Telekombetreiber nach § 12 Z 5 PStSG die Personen hinter den Usernamen und IP-Adressen abfragen
- diese offen oder verdeckt, evt. auch mit Peilsendern observieren
- Auskünfte über sie bei anderen Körperschaften des öffentlichen Rechts (zB Unis, Sozialversicherungsträger) einholen (die von dort erteilt werden müssen)
- und all die in § 11 genannten Datenarten (inkl. Lebensverhältnisse, Namen der Eltern, erkennungsdienstliche Daten, finanzielle Verhältnisse....) in der Analysedatenbank speichern und dort für die Analyse von „Strukturen und Zusammenhängen“ verarbeiten.

All diese Daten könnten vom BVT auch an andere Sicherheitsbehörden – auch im Ausland – weitergeben werden.

Konkretes Beispiel: Bei der NOPEGIDA Demonstration am 2. Februar 2015 wurden 456 Personen eingekesselt und wegen § 285 StGB angezeigt (siehe AB 3517/AB). Darunter befanden sich auch 10 Journalisten, die über die Ereignisse berichteten. Sie alle können in Zukunft nach § 11 Abs 1 Z 2 PStSG als „Verdächtige eines verfassungsgefährdenden Angriffs“ in der Analysedatenbank gespeichert werden – mit allen Folgen.

Fall 2:

Beschimpfung der Landeshymne

Auch dieser Straftatbestand nach § 248 StGB stellt einen „verfassungsgefährdenden Angriff“ dar.

Die Möglichkeiten des BVT sind dieselben wie eben geschildert.

Wenn die Beschimpfung der Landeshymne vielleicht sogar bei einer öffentlichen Veranstaltung in Anwesenheit des Landeshauptmannes geplant ist, dann wäre dieser nach § 8 PStSG vorab zu informieren, damit sein Ansehen gewahrt bleiben möge.

Fall 3:

Fußballfans und § 274 StGB (Landfriedensbruch)...

Fall 4:

Schriftsteller, Journalisten und Karikaturisten und § 248 StGB (Herabwürdigung des Staates und seiner Symbole)...

Die Datenbank

Bereits zum Zweck der „*Bewertung der Wahrscheinlichkeit einer Gefährdung sowie zum Erkennen von Zusammenhängen und Strukturen mittels operativer oder strategischer Analyse*“ dürfen BVT und die neuen LVTs in einer gemeinsamen Datenbank zahlreiche Personendaten speichern: die Namen der Eltern, Beruf, Lebensverhältnisse, Kommunikations- und Verkehrsmittel bis zu wirtschaftlichen und finanziellen Verhältnissen. Dazu kommt auch noch die Generalklausel der „*tat- und fallbezogenen Informationen und Verwaltungsdaten*.“ De facto kann also alles, was BVT und LVT zu einer Person wissen, in dieser Datenbank gespeichert und mittels „*operativer oder strategischer Analyse*“ ausgewertet werden.

In dieser Datenbank können gespeichert werden:

- Betroffene einer Maßnahme nach § 6 PStSG, der drei Fälle umfasst:
 - o Mitglieder einer Gruppe, gegen die eine „erweiterte Gefahrenforschung“ läuft
 - o Personen, bei denen der Verfassungsschutz die Begehung eines der aufgezählten über 100 Delikte für „wahrscheinlich“ hält
 - o Personen, bei denen ausländische Dienste auf die Begehung von Taten aus dem Deliktskatalog im Ausland hingewiesen haben.
- „Verdächtige“ solcher Delikte, gegen die als Verdächtige oder Beschuldigte in einem Strafverfahren ermittelt wird. Es fehlt aber eine Bestimmung, dass die Daten etwa nach Einstellung des Verfahrens oder Freispruch zu löschen wären.
- Kontakt- und Begleitpersonen der genannten Personen.
- Informanten und sonstige Auskunftspersonen.

Während bei den Kontakt- und Begleitpersonen sowie Informanten zwar einige Datenarten nicht gespeichert werden dürfen (zB über finanzielle Verhältnisse), ist andererseits auch hier die Speicherung „tat- und fallbezogener Informationen“ zulässig, so dass diese Beschränkung wiederum umgangen werden kann.

Im Gesetz nicht geregelt sind die zulässigen Quellen für die Analysedatenbank. Der Gesetzesentwurf ist hier widersprüchlich: §10 erlaubt die Ermittlung von Daten nämlich nur für bestimmte Aufgaben, bei denen die Führung der Analysedatenbank nicht erwähnt wird. Da die Datenbank andererseits genau für die Bewertung der Wahrscheinlichkeit eines „verfassungsgefährdenden Angriffs“ dienen soll, beabsichtigt die Regierung offenbar die Befüllung mit jenen Daten die eben zur Vorbeugung solcher Angriffe dienen sollen. Damit stehen aber alle im PStSG genannten Ermittlungsmaßnahmen zur Verfügung: von den Anfragen an andere Behörden in § 10 Abs 3, der Beschaffung privater Videoaufnahmen in § 10 Abs 4 über die Auswertung offener Quellen wie insbesondere dem Internet in § 10 Abs 5 bis zu den besonderen Ermittlungsbefugnissen des §12 mit entsprechender Ermächtigung durch den Rechtsschutzbeauftragten (Observation, verdeckte Ermittlung, verdeckter Einsatz von Bild- und Tonaufzeichnungsgeräten, Verkehrsdatenanfragen an Telekom-Provider usw.).

Das Innenministerium will die Daten offensichtlich unbeschränkt aufbewahren können: Nach § 11 Abs 2 beträgt die Speicherfrist 5 Jahre. Diese Frist beginnt aber mit jeder weiteren Speicherung zu einer Person neu, und kann damit de facto unbeschränkt verlängert werden.

Der Rechtsschutzbeauftragte ist für die Analysedatenbank nicht zuständig.

Mit dem Staatsschutzgesetz plant die Innenministerin, eine umfassende Staatsicherheits-Datenbank einzuführen, die Daten der Betroffenen unbeschränkt aufzubewahren und sie nach Belieben an ausländische Dienste unkontrolliert weitergeben zu dürfen.

Damit wird die gesetzliche Basis für eine offene Eingliederung des BVT in den von CIA und NSA geführten Geheimdienstverbund geschaffen.

Peter Pilz

Wien, 10.06.2015