



Fig. 1

# 1. Datenbanken von Polizei und Verfassungsschutz

Innerhalb der BRD führen Datenbanken:

- Die Landespolizeien
  - Das BKA
  - Verfassungsschutz
  - MAD, BND
  - Jede Menge öffentliche Stellen (AZR, BZR, ZEVIS, Meldeämter, Rentenversicherung). Das AZR ist das Ausländerzentralregister, geführt vom Bundesverwaltungsamt; das BZR ist das Bundeszentralregister, das von der Bundesanwaltschaft geführt wird und Vorstrafen und ähnliches speichert; ZEVIS ist das Zentrale Verkehrs-Informationssystem und speichert, wer welches Kennzeichen fährt und was er oder sie so an Punkten hat. Diese Dateien stellen letztlich den größten Teil unserer Datenspuren – allein die Meldeämter halten 200 verschiedene Daten über alle BürgerInnen vor.
  - Jede Menge Privatfirmen (Banken, Payback, Telekom, ISPs, Web...)
  - Uns soll es hier um die ersten drei gehen. Das soll nicht heißen, dass die Bedrohung durch die anderen Datenbanken vernachlässigbar ist, zumal teilweise reger Datenaustausch stattfindet. Aber erstens ist das Feld schon so zu weit, und zweitens ist zu privaten Datenbanken meist noch schwerer auch nur irgendwas rauszukriegen.
- (vgl. Fig. 1)

## Grundsätzliches

Leider ist in die Datenhaltung der GesetzeshüterInnen nicht immer einfach Einblick zu gewinnen.

Mögliche Quellen sind

- Berichte der Datenschutzbeauftragten – hier ist der Nachteil, dass meistens nur das verzeichnet ist, was den LfDs und BfDs so auffällt und was offensichtlich illegal ist. Spätestens nach den Ottokatalogen ist jedoch bereits die legale und alltägliche Praxis hochgefährlich für Menschen, die sich politisch betätigen.
- Informationen der Behörden selbst – hier werden zwar manchmal erstaunlich offenerzig recht grobe Hämmer verbreitet, aber typischerweise haben die Pressestellen der Behörden keine Ahnung, wovon sie so schreiben, und natürlich wird auch hier nur in Ausnahmefällen wirklich Relevantes preisgegeben.
- Einrichtungsanordnungen – diese sind an sich zum Betrieb einer Datenbank nötig, aber oft genug werden gerade die übelsten Datenbanken über Jahre „einfach so“ betrieben, ohne dass sich irgendwer dran stören würde. Dazu kommt, dass die Einrichtungsanordnungen offenbar von den Innenministerien erlassen werden können, und an deren Schriftstücke ist auch nur mit Mühe zu kommen. Selbst wenn sie verfügbar sind, sind die Einrichtungsanordnung typischerweise voll mit Gummiregelungen aller Art, die kaum Rückschlüsse auf die tatsächlich gespeicherten Daten und den Umgang mit ihnen zulassen.
- Berichte von Dritten (Telepolis, Cilip und Co) – hier ist das Problem, dass auch diesen in der Regel nicht wesentlich mehr Quellen offen stehen als uns.

- Polizeiliche und Juristische Fachliteratur – hier lagern gewiss noch Schätze, die nur darauf warten, gehoben zu werden.

Die schwierige Quellenlage bewirkt, dass wir vor allem Pannen kennen. Die wahrscheinlich viel größere Bedrohung durch die alltägliche Sammel- und Auswertewut kann man allenfalls abschätzen.

Mehr Infos:

<http://www.datenschmutz.de>

## 2. NADIS und Gendatei

Das Nachrichtendienstliche Informationssystem wird gemeinsam von den drei Geheimdiensten der BRD betrieben.

Es ist größtenteils ein Nachweissystem: Gespeichert sind Gruppen oder Personen samt Merkmalen zur Identifikation mit Verweisen auf Daten an anderer Stelle.

Enthalten sind:

- MAD-Daten über KD-pflichtige (ca. 4 Mio)
- BND-Daten (angeblich 1 Million Personen)
- VS-Daten über „Extremisten“ (rund 2 Mio)

Die VS-Daten sind zur Hälfte auf sicherheitsrelevante Personen bezogen (AKW-ArbeiterInnen, Rüstungsindustrie usw.), zur anderen Hälfte aus Unterschriftenlisten, Zeitungen u.ä. (80%) und VS-Ermittlungen gespeist.

NADIS ist auf etwas unklare Weise mit INPOL gekoppelt. Speicherfrist in NADIS in der Regel 15 Jahre.

1996 kritisiert der LfD BaWü, dass das Ordnungsamt Stuttgart ohne Zögern Namen und Adressen von AnmelderInnen von Infoständen an den VS weitergegeben hat.

### Gendatei

Seit 4/1998 eingerichtet. Nettes Beispiel für das Wachstum solcher Dateien: Ende 2000 80 000, Anfang 2002 150 000, November 2002 236 000 Datensätze.

Treffer in der Gendatei „weit überwiegend“ Eigentumsdelikte.

Ähnlich in UK: „Viele Tausend“ Verurteilungen durch dortige Gendatenbank, zu 95% Trivialkriminalität.

### 3. INPOL

INPOL ist das Datenbanksystem des BKA, eingerichtet 1972 unter Horst Herold, SPD-Sonnenstaatstheoretiker.

Datenhaltung zu Straftaten „länderübergreifender, internationaler oder erheblicher Bedeutung“ für Länder, BKA, BGS, Zoll.

Früher: Aufteilung in eine Unzahl von Spezialdateien (KAN, FDR, LIMO, usf)

- Dabei steht KAN für Kriminalaktennachweis – in dieser Datei wurde zu Personen ein Verweis auf eine Kriminalakte (aus Papier) geführt –, FDR für Falldatei Rauschgift – hier wurde noch der letzte Kiffer gespeichert –, LIMO für Linksextremistisch motivierte Kriminalität. In letzterer fanden sich („erhebliche Bedeutung“) auch Platzverweise, Ingewahrsamnahmen und Personalienfeststellungen. Sie waren im „offenen Bereich“ für alle anfragenden Dienststellen zugänglich.

□

Seit 16.8.2003: Inpol-Neu. Darin „Anwendungsunabhängige Einfacherfassung“.

Geplant für Inpol-Neu: Operativer und dispositiver Bereich. Laufen tut wohl nur der operative.

- Dabei hat man sich unter „operativ“ Abfragen wie „Was weißt du über Hubert Mayer?“ vorzustellen, unter „dispositiv“ Abfragen wie „Siehst du in deinen Daten, wo die nächste Hausbesetzung stattfinden wird?“, entlang dem Herold'schen Traum, Verbrechen vorhersagen zu können. Der dispositive Teil wurde wohl 2001 aufgegeben, nachdem das komplette Projekt INPOL-Neu kurz vor dem Scheitern stand.

- Es gibt Grund zur Annahme, dass 2001 beschlossen wurde, das POLAS-System der Länder aufzubohren und die bis dahin in INPOL-neu geflossene Arbeit abzuschreiben.

Da Daten eigentlich nur mit Zweckbindung, daher nun Kontrolle des Zugriffs („komplexes Berechtigungssystem“).

- Soweit jetzt abzusehen ist, ist dieses „komplexe Berechtigungssystem“ einfach eine im wesentliche dreistufige Hierarchie, wobei die übergeordneten Ebenen alle Rechte der niedrigeren haben:

- Grundbereich: Siehe unten. Da dies der niedrigst priorisierte Bereich ist, haben alle NutzerInnen Zugriff auf diese Daten.
- Fallbereich: Ex-PIOS-Daten, Fallanwendungen mit Ausnahme OK, Geldwäsche, „Innere Sicherheit“. Hier insbesondere Daten „Unbeteiligter“. Partiiell sollen diese Daten auch in den Grundbereich diffundieren können (etwa Auskünfte über die Straftaten, die eine Person begangen hat). Zugriff sollen „polizeiliche Ermittler“ haben.
- „Organisierte Kriminalität“, „Geldwäsche“ und „Innere Sicherheit“: Analog Fallbereich, nur eben auf die genannten Felder bezogen.

Es gibt offenbar noch separate Bereiche Spudok (siehe unten) und „Temporäre Fallanwendungen“, worunter spezielle Befugnisweiterungen etwa für SoKos und ähnliches zu verstehen sind. Selbst wenn diese zum Einsatz kommen, kann von einem „komplexen Berechtigungssystem“ nicht die Rede sein, eher von einem Ende des Finalitätsprinzips (Zweckbindung von der Erhebung der Daten bis zu ihrer Löschung).

- „Grundinformation“: Personen- oder Sachdaten, Daten aus ED-Behandlung, Haftdaten, Personenbeschreibungen, PHWs, Fundort für Kriminalakten, Marker für Verfügbarkeit von Gendaten.

- PHWs (Personenbezogene Hinweise) sind dabei so nette Dinge wie „Geisteskrank“ (früher gerne ohne Mitsprache von Ärzten vergeben) oder „BTM-Missbrauch“, vergeben, weil jemand mal ein Bröckchen Dope dabei hatte.

- Dabei werden offenbar schon im Grundbereich auch *Tatvorwürfe* gespeichert.

„Der KAN kann Daten enthalten, die als solche selbst nicht ohne Weiteres die KAN-Zugangskriterien erfüllen, jedoch aufgrund einer Bewertung (Prognose) ergeben, dass diese zur Verhütung von Straftaten von länderübergreifender, internationaler oder erheblicher Bedeutung beitragen können“ (aus der Einrichtungsanordnung von KAN).

- Konkret meint dies etwa Personen, die in Notizbüchern Beschuldigter gefunden wurden. So schnell kanns gehen.

Generell wird juristisch, in den Datenbanken aber offenbar in der Regel nicht faktisch zwischen „harten“, d.h. durch Gerichte bestätigten, und „weichen“, d.h. einfach mal von irgendwem gespeicherten Daten unterschieden. Im Prinzip besteht Anspruch auf Löschung der weichen Daten

- nach Abschluss des Verfahrens.

### Spudok

Spurendokumentationsdateien gehören zum Fiesesten, was INPOL (und andere Polizeidatenbanken) so zu bieten haben. Hier wird alles gespeichert, was nur irgendwie zu speichern ist.

- Spudok-Skandal: Widerrechtlich wurden Anfang der 80er große Mengen Daten erhoben und mussten auf Gerichtsbeschluss hin 1985 gelöscht werden. Damals waren 20% der BürgerInnen des Wendlands in der betreffenden Spudok-Datei geführt. Im Anschluss an einen Anschlag aufs Göttinger Arbeitsamt 1997 tauchten diese Daten plötzlich wieder auf.

Daten vom Spudok-Typ gab es früher auch in PIOS, speziell über eine Datei namens APIS. Sie wurden wohl größtenteils in den Fallbereich von INPOL-neu übernommen.

- Wesentliche Rolle von Spudok auch bei der Rasterfahndung.
- Spudok gibts nicht nur in INPOL: In Bayern musste die Spudok-Datei OFR-GEPE-S (das steht für Gewaltbereite Personen aus den Bereichen Rechts- und Linksextremismus, politisch motivierte Skinheads und Ausländergruppen) 1996 gelöscht werden. Grund war, dass Spudok-Dateien eigentlich nur für konkrete Ermittlungsverfahren, etwa die klassische Antifa-M-Geschichte, zulässig sind. Die Daten allerdings wurden vor der Löschung noch schnell in die Staatsschutzdatei Bayern übertragen. . .

## 4. POLAS und PAD

Da Polizei in der Regel Ländersache ist, sollten die Länder auch „in der Regel“ die Daten ihrer BürgerInnen verwalten. Angesichts des Umfangs von INPOL dürfte das nicht der Fall sein, aber die Länder unterhalten trotzdem eigene Datenbanken, die allerdings häufig auch in Wiesbaden laufen (Auftrags-DV, seit 10/2000 sogar legal).

In BaWü war das früher PAD (plus MOD), 2003 Übernahme des von Hamburg entwickelten POLAS, das auch in anderen Ländern eingesetzt wird.

- In NRW hängen am dortigen POLAS 26 000 Rechner, der Umstieg hat 2.6 Millionen Euro gekostet. Entsprechende Zahlen für BaWü haben wir nicht. Allerdings ist bekannt, dass es 2002 in BaWü rund 15 000 Arbeitsplatzrechner bei der Polizei gab und dass zwischen 1999 und 2002 ein Extraprogramm über 20 Millionen Euro zur Verbesserung der EDV-Infrastruktur lief. Alle Dienststellen mit mehr als 10 MitarbeiterInnen sind vernetzt.

- Einige der in PAD erfassten Felder sind bekannt: PGB, PVN, PHW, PLD, TSD, TGM, TSH, TTZ, TSS, Kriminalakten führende Dienststelle. Übersetzung: PGB: Geburtsname – PVN: Vorname – PLD: Löschungstermin, TSD: zu einer Tat sachbearbeitende Polizeidienststelle TGM: Tatortgemeinde – TSH: Straftat – TTZ: Tatzeit – TSS: Schaden. Man darf davon ausgehen, dass dies recht typische Felder in den „normalen“ Datenbanken sind. Spudok und Freunde sehen bestimmt anders aus.

Interessant dabei: Die Daten werden offenbar, wie sich das aus Informatiksicht gehört, in verschiedenen Tabellen geführt. Zwischen diesen gibt es Verweise (Tat x wurde von Täter y ausgeführt, Täter x hat Taten y und z begangen). Es ist unklar, was passiert, wenn der Löszeitpunkt für den Eintrag in einer Tabelle gekommen ist, nicht aber für den in einer anderen – dessen

- Verweis ja ungültig würde.

Der LfD BaWü rügt jedes Jahr wieder viele Praktiken rund um PAD. Auch wenn der eigentliche Skandal der Normalbetrieb ist, hier trotzdem ein paar lustige Geschichten:

- ⌋

U

  - PHW BTMK oder DROG – der LfD fand 2002 1320 Personen in PAD, die diesen PHW hatten, für die aber kein einschlägiges Delikt vorlag. Die Einträge kamen durch liberalen Abgleich mit Inpol.
- ⌋

  - KAN-Marker – „besonders schwere“ Verbrechen gehören ins INPOL. Das würde früher durch einen Marker erledigt, durch den die Speicherfrist auch gleich auf 10 Jahre erhöht wurden. Ein paar dieser besonders schweren Verbrechen: Ein Mann hat zwei Ster Kirschbaumholz im Wert von 100 DM statt beim Auftraggeber bei sich zu Hause abgeladen; vier Anti-Jagd-AktivistInnen, die mit Transpis und Trillis eine Jagd störten, bekamen wegen Nötigung ihren KAN-Marker; ein Bauherr, der Differenzen mit dem Bürgermeister hatte, drohte, zwei Polizeibeamte, die ihn beim Bauen stören wollte, umzufahren; ein Fliesenleger hat schwarz gearbeitet, kam mit einem Auftraggeber in Konflikt und stieg in dessen Wohnung ein, um offensichtlich sein eigenes Arbeitsmaterial zurückzuholen – der KAN-Marker blieb trotz Einstellung des Verfahrens. Bei der PD Balingen bekamen 66% aller PAD-Einträge einen KAN-Marker.

U
- ⌋

  - Polizist checkt Kandidaten aus – 1995 ließ ein Mannheimer Polizist sieben Leute über PAD und INPOL abchecken, um zu sehen, ob sie seiner Partei würdig seien. Er wurde zu einer Geldbuße verurteilt.

U
- ⌋

  - Drogen sind immer schlimm: Transfer vom PAD ins FDR (INPOL) – dieser Transfer wurde routinemäßig für völlige Bagatellfälle gemacht: über einen Ulmer Studenten war 1997 in der FDR immer noch gespeichert, daß er im September 1990 auf dem Gelände der Universität Ulm einmal Haschisch eraucht haben soll; über einen 37 Jahre alten Feinmechaniker in der FDR immer noch gespeichert, daß er im Sommer 1992 in Esslingen einmal Haschisch erworben haben soll; über einen amerikanischen Soldaten in der FDR immer noch festgehalten, daß er vor mehr als 10 Jahren einmal Haschisch besessen haben soll. Die entsprechenden Datensätze hatten die überlangen Löschrfristen, weil sie aus PAD nach INPOL und nach der Löschung in PAD wieder aus INPOL zurückkamen.

U
- ⌋

  - Offenherzige Auskünfte unter befreundeten Dienststellen – 1997 teilte der Staatsschutz BaWü auf eine Anfrage aus Hessen nicht nur der anfragenden Stelle, sondern auch noch gleich den beiden LKAs mit, dass eine Person in den 80ern an einer Pershing-Sitzblockade teilgenommen hat. Abgesehen von dem absurden Dienstleister, der sich in dem Vorgang zeigt, hätten die Daten ohnehin längst gelöscht sein müssen.

U
- ⌋

  - Offenherzige Auskünfte unter Freunden – 1997 hat eine Frau bei der Reorganisation einer Behörde die Arschkarte gezogen und wurde dann auch noch sicherheitsüberprüft. Hintergrund: Ein Staatsschutz-Mitarbeiter hatte privaten Kontakt zu einem Kollegen der Frau und hat durchblicken lassen, sie sei als (ehemaliges) Mitglied der autonomen Szene bekannt, der Kollege ist zum Chef gelaufen. All das (inkl. Sicherheitsüberprüfung) war natürlich illegal.

U