

1. Polizeidatenbanken

Für die Eiligen:

- Es ist scheiße – der Staat baut eine gigantische Drohkulisse auf, so dass er mit Hämmern wie Vorratsdatenspeicherung und Fingerabdrücken in Ausweisen durchgekommen ist –, aber...
- ... Widerstand lohnt sich noch. Verloren haben wir schon, wenn wir glauben, dass „die“ ja eh alles machen und können. Beides ist falsch, und es gibt viel, um das zu kämpfen sich lohnt.
- Auskunft ersuchen, aber...
- politische Fragen suchen. Das heißt vor allem: Der Rahmen des bürgerlichen Datenschutzes hilft, aber er reflektiert letztlich notwendig die Gesetze. Da eigentlich alle Parlamente komplett versagt haben, diese auch nur bürgerrechtskonform zu gestalten, müssen bürgerliche wie linksradikale AktivistInnen deutlich mehr tun als nur auf die Einhaltung der Gesetze zu achten.
- Gespeicherte Daten sind verlorene Daten. Das heißt: Wenn Daten irgendwo gespeichert sind, sind sie vor dem Zugriff des Staates nicht mehr sicher. Insofern muss Ziel unseres Handelns immer sein, die Speicherung von und nicht den Zugriff auf Daten zu regulieren – was uns jedenfalls vom bürgerlichen Datenschutz absetzt.

2. Eure Datenspur

Daten von euch speichern und verarbeiten:

- Die Landespolizeien
- Das BKA
- Der Zoll, Bundespolizei, ...
- Europäische Stellen
- Verfassungsschutz, MAD, BND
- Jede Menge öffentliche Stellen (AZR, BZR, ZEVIS, Meldeämter, Rentenversicherung usw). 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.
- Jede Menge Privatfirmen (Banken, Payback, Fluglinien, Telekom, ISPs, Web...)

Hier geht es erstmal nur um den unmittelbaren Sicherheitsapparat, also die Polizeien. Das soll nicht heißen, dass die Bedrohung durch die anderen Datenbanken vernachlässigbar ist, zumal teilweise reger Datenaustausch stattfindet bzw. polizeilicher Zugriff auf Datenbestände gesetzlich geregelt ist (z.B. für Meldedaten, Stammdaten von Bankkonten, Flugpassagierdaten usw.).

Im Rahmen dieser Veranstaltung müssen diese Hinweise aber reichen, denn schon die Polizeidatenbanken selbst sind ein weites Feld.

3. Nach Tonga?

Drei Dinge sind oft auf unserer Seite:

- Unfähigkeit der Betreiber der Systeme
- „Sie“ haben Interessenkonflikte
- Marktwirtschaft braucht Rechtssicherheit

Der letzte Punkt erklärt wesentlich, warum der Staat sich nicht noch größere Züge aus der Datenpulle genehmigt. Marktwirtschaften geben den Rechtsstaat weder aus Großzügigkeit noch aus Menschenfreundlichkeit. Nein, zur funktionierenden Kapitalakkumulation und gepflegten Konkurrenz gehört ein Rechtssystem, in dem sich Unternehmen wie Privatpersonen darauf verlassen können, dass die Rechtsstandards so angewandt werden, wie sie im Gesetz stehen (vgl. auch das Insistieren der von Nazi-Zwangsarbeit profitiert habenden Firmen auf „Rechtssicherheit“ in der Entschädigungsfrage) – und auch, ihren Geschäften in der Regel unbehindert nachgehen zu können.

Er ist aber kein Trumpf, den wir einfach spielen können. Rechtssicherheit für Linke (und erst recht etwa für AusländerInnen, soweit sich nicht als InvestorInnen kommen) ist nämlich nicht ganz so wichtig, und die Behörden können sich hier viel leisten, solange die breitere Öffentlichkeit meint, nicht betroffen zu sein oder wenig von den Praktiken der Behörden ahnt (vgl. Diskussion Feindstrafrecht, Sicherungsverwahrung usw).

Unsere Aufgabe in der Kontrolle staatlicher Überwachungswut ist mithin abgesehen von einem vernünftigen Umgang mit Information in unseren Strukturen auch die Herstellung von Öffentlichkeit über die Überwachungspraktiken („Bürger beobachten die Polizei“).

Aber: In Zeiten der (imaginierten) Krise (z.B. 1977 in der BRD, 2001f in den USA) vergisst der Staat, warum es den Rechtsstaat gibt – und dann ist der Kampf gegen Überwachung ein „ganz normaler Befreiungskampf“, der unter Umständen ohne Rechtsstaat geführt werden muss. Gerade dann ist es wichtig, einschätzen zu können, was „die können“ und was nicht.

Auch der Punkt mit den auch in diesem Bereich häufig konfligierenden Interessen der verschiedenen staatlichen und nichtstaatlichen Beteiligten ist oft hilfreich. Klassisch sichtbar ist das beispielsweise in der Debatte um die Einrichtung der „Anti-Terror“-Datenbank, in der zwar alle möglichst weitgehenden Einblick in die Daten anderer haben wollten, aber vor allem die Dienste ihre Daten nicht hergeben wollten.

In einigen Fällen sind Telekommunikationsunternehmen auf „unserer“ Seite, teils, weil sie den Überwachungsaufwand nicht finanzieren wollen, teils aber auch, weil sie wissen, dass ihre KundInnen allzu weitgehende Überwachungsmöglichkeiten mit einer Änderung ihres Konsumverhaltens zum Nachteil der Unternehmen quittieren könnten (wer macht schon „richtiges“ Breitband ohne Filesharing). Dabei sind andere Teile der Industrie auf der Seite der Überwachungsfanatiker, hier etwa die „Content-Industrie“. Natürlich sind solche Konflikte dann immer auch auf der politischen Bühne reflektiert.

Kurz: „Sie“ sind nicht in jedem Fall die Gleichen. In der derzeitigen Entwicklung sind „Sie“ aber trotzdem recht erfolgreich.

Datenschutz

Bahnbrechend: Das „Volkszählungsurteil“ von 1983. Es definiert

- Grundrecht auf informationelle Selbstbestimmung, in das nur aufgrund eines Gesetzes eingegriffen werden kann.
- Zweckbindung. Von der Erhebung bis zur Löschung muss immer klar sein, wofür Daten da sind, der Zweck darf sich in der Regel auch nicht ändern. Für die Behörden ist das natürlich hart, weshalb es auch regelmäßig ignoriert wird oder hahnebüchene Konstrukte gezimert werden. Im Fall der Polizeidatenbanken wird als Zweck mittlerweile pauschal „Aufklärung und Vorbeugung von Straftaten“ akzeptiert, was dieses Prinzip ein wenig zahnlos macht sowie, nebenbei, auch föderalismustheoretisch extrem gewagt ist.

- Datensparsamkeit. Gespeichert werden darf nur, was zur Erfüllung eines genau definierten, verhältnismäßigen Zwecks unverzichtbar ist. Spätestens seit dem Abnicken der Vorratsdatenspeicherung ist klar, dass aus den Parlamenten in dieser Hinsicht keine Prüfung kommen wird.
- Speicherfristen. Straftaten verjähren. Straftaten, die verjährt sind, sind nicht mehr rechtsrelevant, nach dem Finalitätsprinzip dürfen Daten, die zu ihrer Aufklärung beitragen könnten, also nicht mehr gespeichert werden. Leider ist das in der Praxis nicht so einfach, weil ja niemand wissen kann, welche Straftaten eine Person einmal begehen wird ob ein bestimmtes Datum mal zur Klärung helfen kann. Daher geben die Errichtungsanordnungen in der Regel „Aussonderungsprüffristen“ vor, nach denen „geprüft“ werden muss, ob Daten noch gespeichert werden dürfen, bzw. Löschrufen, nach denen Daten zu löschen sind. Normalerweise sollten das höchstens 5 Jahre sein, bei Jugendstrafen in der Regel darunter. In der Realität wird im Politbereich meistens für 10 Jahre gespeichert, der VS speichert 15 Jahre.

Mantra: So löchrig die Datenschutzgesetze sind: Wir wären schon viel weiter, wenn die permanenten Rechtsbrüche der Behörden aufhören würden.

Genau aus diesem Grund sind die Datenschutzbeauftragten – trotz aller Unzulänglichkeiten – unsere natürlichen Verbündeten, wenn sie nicht gerade Vorratsdatenspeicherung für eine Woche fordern. Sie sind meist der einfachste Weg, um den Staat zur Einhaltung seiner eigenen Regeln zu mahnen.

Sie helfen natürlich nicht, wenn diese Regeln selbst schon schlecht sind und sind dann im Gegenteil sogar schädlich, denn natürlich tragen sie zur Legitimation des Gesamtsystems bei.

4. INPOL

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

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

INPOL ist in zahlreiche Unterdateien aufgeteilt. Dabei

- Verbunddateien – Daten der Einspeiser für alle
- Zentraldateien – Daten des BKA für alle
- Amtsdateien – Daten des BKA fürs BKA

Die Diskussion 2008-2010 um die Datei Gewalttäter Sport ging übrigens um Verbunddateien an sich. Polizei ist ja erstmal Ländersache, und wenn sich die Länder einer Datei bedienen, muss es dazu eigentlich auch eine Rechtsgrundlage auf Länderebene geben. Eine solche hatte der Bundesrat für Verbunddateien nicht gegeben, was dann dazu führte, dass die Gewalttäter Sport sogar vom Bundesverwaltungsgericht als unzulässig eingestuft wurde. Inzwischen hat der Bundesrat eine entsprechende Verordnung abgenickt.

Einzeldateien: KAN, Innere Sicherheit, IgaSt, ViCLAS, DAD, AFIS. . .

Dabei steht KAN für Kriminalaktennachweis – in dieser Datei wird zu Personen (auch Opfern) ein Verweis auf eine Kriminalakte (aus Papier) geführt, sie ist quasi das Herzstück von INPOL.

Die Datei Innere Sicherheit ist mit rund einer Million Datensätzen die zentrale Datei im politischen Bereich. Sie ist offizieller Nachfolger der skandalgeschwängerten Datei APIS (Arbeitsdatei PIOS Innere Sicherheit), über die in älteren Texten gerne mal geschimpft wird.

IgaSt ist eine Zentraldatei, in der das BKA seit 2003 Daten zu globalisierungskritischen Bewegungen sammelt. Aus ihr wurden Grundlagen für „Gefährderschreiben“ (AktivistInnen bekommen im Vorfeld etwa von Gipfeln den „guten Rat“, zuhause zu bleiben; werden trotz zwischenzeitlichem Verbots offenbar immer noch verschickt), Meldeauflagen und Ausreiseverbote gezogen.

ViCLAS ist das Violent Crime Linkage and Analysis System, eine Profiling-Anwendung aus Kanada.

AFIS sind zwei Dateien mit Fingerabdruckdaten (einmal für AusländerInnen, und dann nochmal für ED-Behandelte bzw. Spuren); sie werden wohl allmählich durch die neuen, auf Biometrie basierenden Datenbanken für digitalisierte Fingerabdrücke abgelöst – bisher basieren sie auf den alten Beschreibungen, bei denen „ExpertInnen“ das Bild des Abdrucks manuell in passende Zahlencodes wandeln.

Eine Auswahl weiterer bemerkenswerter Dateien:

- Verbunddatei FDR für Falldatei Rauschgift – hier wurde noch der letzte Kiffer gespeichert.
- LIMO für Linksextremistisch motivierte Kriminalität – darin fanden sich („erhebliche Bedeutung“) auch Platzverweise, Ingewahrsamnahmen und Personalienfeststellungen. Sie waren im „offenen Bereich“ für alle anfragenden Dienststellen zugänglich. LIMO gibt es nicht mehr.
- Verbunddateien Gewalttäter Rechts/Sport/Links – während die Rechts- und Links-Varianten schon vom Umfang her (nur 1000 für Gewalttäter Links) eher nebensächlich erscheinen, war die Sport-Datei mit immerhin 10000 Datensätzen während der WM schwer in der Diskussion.
- Verbunddatei HAFTDATEI – Infos zu rund 100000 Menschen, die im Knast sind oder sein sollten oder gerade auf Bewährung draußen sind. Reizvoll waren hier verzögerte Löschrufen.
- Verbunddatei Schläfer – hier hatte das BKA seine Rasterfahndungsdaten
- Verbunddatei FUSION – unglaubliche 40000 Datensätze zur Bekämpfung der „Rockerkriminalität“.

Die „Dateien“ in INPOL darf man sich dabei nicht vorstellen wie Dateien auf einem üblichen Rechner, noch nicht einmal als separate Datenbanken innerhalb eines DBMS. Tatsächlich liegen alle INPOL-Daten in einer physikalischen Datenbank mit entsprechend vielen Tabellen. Die tatsächlichen Dateien sind vermutlich lediglich Views auf die zugrundeliegenden Bestände (plus manchmal ordentlich Code, z.B. bei ViCLAS).

5. INPOL war neu

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

Geplant war: Operativer und dispositiver Bereich.

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.

Die Geschichte des Neuaufsetzens von INPOL-Neu ist ein Krimi für sich.

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

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

- Grundbereich: Siehe unten. Alle NutzerInnen können diese Daten nutzen.
- Fallbereich: Ex-PIOS-Daten, Fallanwendungen mit Ausnahme OK, Geldwäsche, „Innere Sicherheit“. Hier insbesondere auch Daten „Unbeteiligter“. Partiiell sollen diese Daten 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.

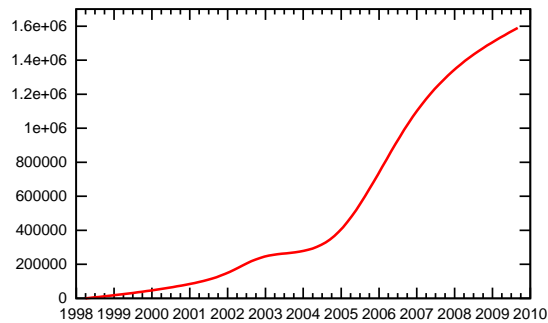


Fig. 1

Selbst wenn diese zum Einsatz kommen, kann von einem „komplexen Berechtigungssystem“ nicht die Rede sein, eher von einem Ende des Finalitätsprinzips.

„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. LfDs wie BfD äußern regelmäßig Kritik an Auswahl wie Vergabe von PHWs („schwul“, „Landfahrer“).

„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 Errichtungsanordnung von KAN).

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

Generell wurde früher gerne zwischen „harten“, d.h. durch Gerichte bestätigten, und „weichen“, d.h. einfach mal von irgendwem gespeicherten Daten unterschieden.

Inzwischen sind die Polizeien aber auf den Trichter gekommen, einfach mal ein Verfahren einzuleiten und es dann von der Staatsanwaltschaft nach §170 (2) StGB einstellen zu lassen. Damit war zwar noch kein Gericht damit befasst, aber immerhin kann man so ein „Fakt“ speichern („Ermittlungsverfahren wegen versuchten Totschlags, Ausgang unbekannt“), von dem niemand sagen kann, es wäre weich. Gerichte haben solche Praktiken in vielen Einzelfällen gerügt, konsistent aber bestätigt, dass 170(2)-Daten *grundsätzlich* gespeichert werden dürfen.

6. DAD (Gendatei)

(vgl. Fig. 1)

Rapides Wachstum seit 4/1998. Rund 1.5 Millionen Datensätze, ca 50% mit Personen.

Treffer in der Gendatei „weit überwiegend“ Eigentumsdelikte. Diese Einschätzung des BfD zeigt wieder, dass „konsensfähig“ verabscheuungswürdige Kriminalität zum Einreißen von Barrieren dient, die resultierende Repression aber viel weitere Gruppen trifft – nicht zuletzt versucht die Polizei auch in politischen Verfahren schon fast routinemäßig, DNA-Proben zu nehmen.

Bei der Gelegenheit sollte noch angemerkt werden, dass der regelmäßig bei allem möglichen mit großer Geste verteidigte „Richtervorbehalt“ (die Analyse – nicht jedoch die Abnahme – von

Körperzellen gegen den Willen des Betroffenen bedarf der Anordnung durch einen Richter) offensichtlich recht wertlos ist. Angesichts der bekannten Geschwindigkeit juristischer Entscheidungen scheint es nachgerade unglaublich, dass in den letzten vier Jahren tatsächlich eine runde halbe Million sorgfältiger Abwägungen von „Sicherheitsinteressen“ und Persönlichkeitsrechten stattgefunden hätte. In der Tat ist die Behauptung der Polizeien, die überwiegende Mehrzahl der DNA-Analysen habe mit Zustimmung der Analysierten stattgefunden.

Zahlen in UK: „Viele Tausend“ Verurteilungen durch dortige Gendatenbank, zu 95% Triviale Kriminalität.

7. Länder

Da Polizei Ländersache ist, soweit sie nicht als Arm der Staatsanwaltschaft operiert, sollten die Länder normalerweise die Daten ihrer BürgerInnen selbst verwalten.

Wenn man von der ganz normalen Straßenpolizei kontrolliert wird, wird i.d.R. die Landesdatenbank und SIS abgefragt.

Dabei gibt es meist eine operative Datenbank (typisch POLAS) und eine Vorgangsverwaltung (typisch ComVor).

Für die operativen Datenbanken gilt weitgehend das für die BKA-Datenbanken gesagte, nur dass die Speicherschwelle geringer ist – eine Straftat, der vorgebeugt werden soll, muss hier auch offiziell nicht mehr schwer sein oder nationale Bedeutung haben; außer in BaWü muss es aber immer noch eine plausible Erklärung geben, warum eine Speicherung nötig ist.

Die Vorgangsverwaltungen sind eine neue und dramatische Entwicklung. Sie sind zunächst der Ersatz der alten Schreibmaschine durch zumeist haarsträubende Microsoft-Hackereien. Es gibt aber hinter all den Systemen auch Datenbanken, in die die Vorgänge abgekippt werden, bis hin zu schlichten Anrufen bei den Bullen.

Vven sind typischerweise nicht explizit gesetzlich geregelt; wenn überhaupt, gibt es irgendwelche Verordnungen, die nicht öffentlich sind (IFG-Anfragen bei den Innenministerien sind willkommen!). Wo etwas bekannt ist, sind die Dinge schlimm: Selbst trivialste Polizeikontakte sind noch nach sechs und mehr Monaten auf der Basis des Namens findbar. Vven werden vorläufig nicht bei Personenkontrollen abgefragt; es ist aber sehr wahrscheinlich, dass die Daten bei weiteren Polizeimaßnahmen zumindest wahrgenommen werden.

Bei Vven haben wir noch nicht viele Erfahrungen mit Löschersuchen.

8. Anekdoten von 1984

- PHW BTMK oder DROG – der Lfd BaWü 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.
- Polizist checkt Kandidaten aus – 2009 musste ein CDU-Abgeordneter in Rheinland-Pfalz zurücktreten, weil er alte Freunde seine politischen Gegner im Zusammenhang mit dem Nürburgringskandal in verschiedenen Polizeidatenbanken auschecken ließ. Solche Ideen sind beileibe nicht neu: Schon 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.
- Offenherzige Auskünfte unter 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.
- 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.
- AD PMK Die „Arbeitsdatei Politisch Motivierte Kriminalität“ gibt es seit 2003 am LKA Baden-Württemberg. 2005 waren darin 40000 Personen (!) erfasst. Diese atemberaubende Zahl kam vor allem daher, dass die Polizei darin blind alles gespeichert hat, was irgendwie islamisch geschmeckt hat: Ein Gastwirt, der die Sperrstunde verletzt hat und aus der Türkei kam, ein Mensch, der Residenzpflicht hatte und ihr nicht nachkam, zusätzlich aber aus Kamerun war, ein anderer Mensch, weil er ein Taxiunternehmen angemeldet hat und aus der Türkei kam. Dazu kamen natürlich die üblichen Spiele – 2005 waren trotz nur dreijähriger Speicherfrist 2001 noch Daten einer Castorgegnerin enthalten, die 2001 aufgefallen war – die Frist lief erst bei der Einspeicherung los.

9. Anti-Terror-Datei

Gemeinsame Datei der Dienste und der Polizeien mit einem bunten Strauß von Daten zu Mitgliedern, UnterstützerInnen und SympathisantInnen von nach 129b bzw. 129a mit Auslandsbezug verfolgten Organisationen sowie Leuten, die sie kennen.

Verletzung sämtlicher Grundsätze des Datenschutzes:

- Zweckbindung: Die beteiligten Behörden sollen ihre Daten einspeisen, egal, warum sie erhoben wurden.
- Datensparsamkeit: Bereits „erhobene“ Daten sollen eingespeist werden.
- Auskunftsanspruch: Die Daten gehören rechtlich weiter den Einspeisern, das BKA erteilt keine Auskunft darüber.
- Normenklarheit: Spätestens durch Speicherung von „Kontaktpersonen“ kann praktisch jeder gespeichert werden – für die meisten wird das trotzdem nicht passieren.

10. Auskunft fordern

Folgen polizeilicher Speicherwut im Normalbetrieb:

- Angst – werde ich gespeichert, wenn ich...?
- Terror – bei entsprechenden Speicherungen wird jeder Polizeikontakt zu einer Tortur
- Lähmung – Gefahrderanschreiben und Ausreiseverbote werden aus Datenbanken generiert (wobei beide Praktiken schon mehrfach ganz oder teilweise für illegal erklärt wurden, aber das stört die Polizei natürlich nicht)
- Einfahren – gerade ED-Behandlungen sorgen für eine partielle Umkehr der Unschuldsumutung (wobei das mit Verbreitung des neuen Passes demnächst wohl hinfällig wird; die Fingerabdruckdaten darauf stehen schon fest auf der Wunschliste der Law-and-Order-Fraktion)

Über mögliche Folgen bei einem weiteren Heißlaufen des staatlichen Paranoiaapparats – Stichwort etwa Data Mining – will ich gar nicht anfangen.

Erster (und manchmal letzter) Schritt dagegen:

Das Auskunftersuchen

Natürlich kann mensch damit nichts gegen legale Repression unternehmen. Aber zumindest im Politbereich ist die Polizei-EDV nach wie vor in der Regel rechtswidrig, und die Polizei weiß das auch. Auskunftersuchen und ggf. leichtes Stupsen hilft, die Staatsgewalt an die Grenzen zu erinnern, die sie sich selbst gesetzt hat.

11. Auskunftersuchen?

Gegen Auskunftersuchen könnten sprechen:

- Weitere Daten für die Polizei – aber: das sind langweilige Daten, und sie wären wieder nur illegal speicherbar
- Lüge und Unfähigkeit bei der Auskunftserteilung – hier hilft reger Austausch unter uns, Aufmerksamkeit, Rückfragen bei den Datenschutzbeauftragten
- Es gibt Ausnahmetatbestände, bei deren Zutreffen die Auskunft verweigert wird; dies betrifft insbesondere den Schutz von InformantInnen. Wenn die Polizei mit sowas kommt, *kann* es sinnvoll sein, den zuständigen Datenschutzbeauftragten anzurufen. Vor allem im Castor- und Antifabereich kommt sowas allerdings nicht selten vor, und wir hatten bisher noch keinen Erfolg beim Erzwingen der Herausgabe der Daten.
- Sie wollen „Gründe“ – hier soll mensch meist mutmaßen, was „sie“ von einer/m haben und sagen, warum das so sein soll. Dieser Extraservice für die Repressionsbehörden ist natürlich ein No-no. Die Polizeien dürfen das auch nirgends, auch nicht in Thüringen, obwohl sie dort so tun, als dürften sie. Leider sieht das bei Geheimdiensten anders aus, vor allem auch beim besonders bedrohlichen Bundesamt für Verfassungsschutz. Unter solchen Umständen kann nicht von einem Auskunftsrecht gesprochen werden, und wir raten davon ab, sich diesem Auskunftsunrecht zu unterwerfen.

Zum Thema Unfähigkeit bleibt zu konstatieren, dass die Polizei ihre eigene EDV nur in Ausnahmefällen im Griff hat. Noch weniger verstehen individuelle PolizistInnen, was sie da eigentlich tun. True story, bei der Ausreise am Frankfurter Flughafen:

Grenzer (zieht den Pass durchs Lesegerät und fängt an zu lesen)

Mensch: „Was fragen Sie denn da ab? INPOL?“

G: „Ja.“

M: „Dann können Sie ja nicht viel zu lesen haben. Ich habe gerade erste in Auskunftersuchen gemacht, da steht nichts über mich drin.“

G: „Aber es *stand* mal was über Sie drin.“

M: „???“

Nach Einschaltung des BfD stellte sich heraus: Er hat gar nicht INPOL abgefragt, sondern den damaligen Bundesgrenzschutzaktennachweis.

12. Wie anfangen?

(vgl. Fig. 2)

<https://datenschmutz.de>

Formlose Briefe an die jeweiligen Stellen schicken, ggf. eine Ausweiskopie beilegen.

Wenn beglaubigte Kopien verlangt werden, diese bei der Polizei besorgen. Eure Polizeidienststelle muss diese Bestätigung machen. Wenn sie sich weigern, zeigt den Brief vom BKA oder LKA, wenn sie sich immer noch weigern, lasst dort anrufen.

Leider: Die Auskunft ist Prosa, nicht direkt ein Abzug der DB-Tabellen. Auf diese Weise ist die Auskunft mehr, *worüber* sie speichern als konkret *was*. Besonders schlimm ist das z.B. im Fall der Gendatei, wo je nach Anlage der Tabelle Anfragen wie „haben wir einen engen Verwandten?“ trivial oder fast unmöglich wären.



Fig. 2

13. Löschen lassen

Vieles löscht die Polizei schon, bevor sie Auskunft erteilt.

Wenn sie es nicht freiwillig tut, kann ein Löschersuchen helfen. Dazu immer fragen: „Wie kann dieses Datum helfen, künftige *Verbrechen* aufzuklären oder zu verhindern?“

Gute Kandidaten zum Löschen sind insbesondere Einstellungen nach §170(2) StPO. Wenn es zu einer Verurteilung kam oder nach §15x StPO eingestellt wurde, ist es jedenfalls schwieriger; evtl. muss mensch sich auf die Forderung einer Kürzung der Aussonderungsprüffrist beschränken.

Ggf. uns fragen.

Ggf. den/die LfD oder BfD einschalten.

Aber darüber nicht vergessen: Wie viel sich der Staat erlaubt, bestimmt sich durch unseren Widerstand. Oder eben den Mangel daran – wie viele große Demos gab es gegen Anti-Terror-Datei, neue Polizeigesetze, den ePass usf? Nun, drum gibts den ganzen Mist.