

1. Reclaim Your Data

Datenbanken und Datenaustausch der EU-Repressionsorgane

*What is new is the clear aim of creating the surveillance society and the database state
– Tony Bunyan zum Stockholm-Programm*

- Die EU wird Obrigkeit
- SIS – die große Datenbank
- Europol – BKA reloaded
- Prüm – Modus Operandi der Zukunft

Dazwischenwafen!

2. Die EU wird Obrigkeit

*... examine how operational police cooperation could be stepped up, e. g. as regards
incompatibility of communication systems and other equipment, use of undercover agents...
– Stockholm-Programm*

Wichtigste Quelle von Repression auf EU-Ebene: Schengen. Das ist lustig unter anderem, weil das in der „ersten Säule“ der EU spielte, der wirtschaftlichen Zusammenarbeit, von wegen Abschaffung der Grenzkontrollen. Aber ok, auch die Vorratsdatenspeicherung wurde so hinerklärt. Seit dem Vertrag von Lissabon gibts keine Säulen mehr, insofern ist die Frage in gewisser Weise hinfällig.

Gedanke von Schengen: Wenn die Grenzkontrollen nicht mehr an den Grenzen stattfinden, sollen sie überall sein, und zwar auch außerhalb des Territoriums der einzelnen MS. Also: MS geben sich teilweisen gegenseitigen Zugriff auf ihre Repressionsorgane. Viele der teilweise konfuse Regelungen kommen genau daher, dass zwar jeder Staat möglichst viel von den anderen Staaten haben will, sich selbst aber möglichst wenig reinregieren lassen will.

Weiterer Punkt: Maastricht und der Euro. Die Bestrebungen zu Europol hatten sicher viele Quellen, ein wesentlicher Punkt war aber, dass ja Euro-Falschgeld nicht mehr zwingend von einzelnen Polizeien verfolgt werden kann. Außerdem ist es natürlich einfach schön, zu sehen, wie aus Geld und Grenzen Repression wird. . .

Die EU erlässt seit zehn Jahren regelmäßig Fünfjahrespläne zur Sicherheit:

1. Tampere (2000-2004) – „Gegenseitige Anerkennung“, Bemühungen zu gemeinsamer Migrationspolitik. noch Außenpolitik
2. Den Haag (2005-2009) – u.a. „Prinzip der Verfügbarkeit“, d.h. die Behörden der MS sollen sich gegenseitig Daten geben
3. Stockholm (2010-2015) – „Focus on the citizen“ (vielleicht meinen die das nicht so wie es klingt. . .)

Diese Programme wurden mal „Katalog[e] zur innenpolitischen Staatwerdung der EU“ genannt und enthalten allerlei Schrecklichkeiten, von denen am Ende immer genug auch umgesetzt werden, um heulen zu können.

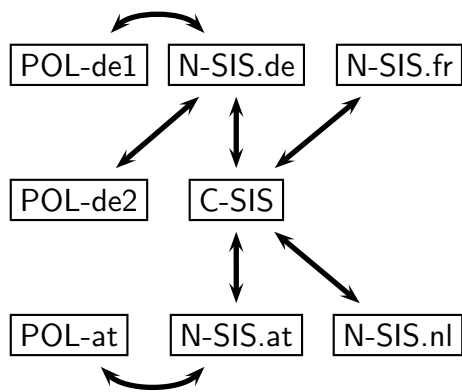


Fig. 1

3. Obrigkeiten untereinander

Mutual trust between authorities and services in the different Member States as well as decision-makers is the basis for efficient cooperation in this area. – Stockholm-Programm

Grundproblem: Die Verfügung über die eigenen Untertanen und die Definition, wer diese sind, ist zweitvornehmstes Privileg jeder Obrigkeit.

(vgl. Fig. 1)

Deshalb: Typische Struktur mit nationalen Kontaktstellen und einem zentralen System.

Hier am Beispiel von SIS: Jedes Land unterhält ein N-SIS, das mehr oder weniger eine vollständige Kopie eines „Masters“, des C-SIS, ist. Die nationalen Polizeien reden nur mit ihrem N-SIS. Soll jemand gespeichert werden, teilt das N-SIS das dem C-SIS mit, haben andere Staaten ausgeschrieben, sieht sich das N-SIS erst die Ausschreibung an, bevor die Polizeien sie sehen. Das N-SIS der BRD ist übrigens beim BKA.

Die Strukturen müssen physikalisch nicht mehr so sein; für SIS II etwa sollen auch „nur“ Views (also quasi vordefinierte Anfragen) für einzelne Staaten über eine standardisierte Schnittstelle angeboten werden.

Das Misstrauen der Obrigkeiten untereinander führt zu recht unterhaltsamen Regelungen, die für SIS im SIRENE-Handbuch stehen; hier ein typisches Beispiel aus dem SIRENE-Handbuch:

- a) Eine Vertragspartei muss immer eine Ausschreibung nach Artikel 96 eingeben können, um den zuständigen Instanzen die Möglichkeit zu erteilen, keine Aufenthaltstitel oder Visa zu erteilen.
- b) Im Konfliktfall mit einer Ausschreibung nach Artikel 95 kann jede Vertragspartei ihre Ausschreibung beibehalten. Die Regeln der Vereinbarkeit finden auf alle anderen Ausschreibungen Anwendung.
- c) Die in Bezug auf die Ausschreibungen zu ergreifenden Maßnahmen werden nach der festgelegten Rangfolge durchgeführt, d. h., dass zunächst die vorläufige Festnahme erfolgt.
- d) Die Vertragsparteien erlassen die erforderlichen nationalen Bestimmungen, um die Benutzer über diese Verfahren zu unterrichten.

Insbesondere können Einzelstaaten Ausschreibungen in manchen Fällen „kennzeichnen“ und sie damit auf ihrem Territorium abmildern oder ganz unterdrücken.

4. SIS: Wer ist drin?

Well-managed migration can be beneficial to all stakeholders. – Stockholm-Programm

Schengen-Informationssystem zur Kompensation des Wegfalls von Grenzkontrollen. Dabei definiert Art. 93 SDÜ auch die Staatsicherheit als Ziel des SIS; natürlich ist unklar, warum ausge-rechnet die Repression typischerweise von InländerInnen durch den Wegfall von Grenzkontrollen gelitten haben sollte.

Die Kategorien von Ausschreibungen (in SIS soll nichts „dispositives“ gespeichert werden):

- Art. 95: Zur Festnahme (25 000)
- Art. 96: Einreiseverweigerung (750 000)
- Art. 97: vorläufiger Gewahrsam (50 000)
- Art. 98: Aufenthaltsermittlung (70 000)
- Art. 99: verdeckte Registrierung oder gezielte Kontrolle (35 000)
- Art. 100: Dinge zur Sicherstellung oder Beweissicherung Kfz, Waffen, Ausweise, Banknoten, Kreditkarten usf. (26 000 000)

Die Artikel kommen aus einer Verordnung namens „Schengener Durchführungs-Übereinkunft“ (SDÜ oder CISA). In Klammern jeweils die Zahl der Einträge aus den entsprechenden Kategorien Anfang 2009.

5. SIS: Was ist drin?

... there is an urgent need for the exchange of data on persons disturbing the public order and/or endangering public security. – Rat der EU, 7558/1/09, 2009-05-27

Ein typischer SIS-Datensatz enthält folgende Felder:

- Name, Vorname (Alias macht normalerweise extra-Record)
- Erkennungszeichen
- Geburtsort und -datum, Geschlecht,
- Staatsangehörigkeit,
- PHW bewaffnet/gewalttätig,
- Art der strafbaren Handlung, Ausschreibungsgrund,
- Maßnahme (Registrierung, Festnahme, Ausweisung, etc)

An sich ist der knappe Umfang des Datensatzes ja zu begrüßen, aber das Problem ist die Verbreitung an sich. Ein Polizist in Transsylvanien sieht im Zweifel nur „Artikel 99, Subversion“ und weiß nicht, ob der Kontrollierte nur ein Haus besetzt hat oder regelmäßig Kasernen sprengt.

Daten in etwa diesem Umfang bekommen Grenzkontrollen, Polizei, Zoll, z.T. Pass- und Ausländer-behörden, Geheimdienste, Europol usf. Es soll eine Liste mit „berechtigten Behörden“ geben. So die aktuell gehalten wird, ist das Ergebnis nicht öffentlich.

Aus der BRD: 2005 70 Millionen Anfragen, 2006 ca. 10500 Terminals, die SIS abfragen konnten.

6. SIS: 99er-Ausschreibungen

In der BRD immer verdeckte Registrierung, weil PolGe in der Regel keine gezielte Kontrolle kennen (aber jetzt neu in BaWü); bei „außergewöhnlich schweren“ Straftaten oder Gefährdung der Staatssicherheit.

Polizei soll beim Antreffen möglichst viele Informationen sammeln (incl. Begleitpersonen, mitgeführte Sachen), ohne dass das Opfer etwas merkt.

Eher bescheiden im Umfang: 2006 376 99er-Ausschreibungen aus BaWü, 118 Staatsschutz. Nach erster Prüfung 67 gelöscht, nach weiterer Prüfung wurden *alle* Staatsschutz-Ausschreibungen der Polizei gelöscht (22 von Justiz blieben). Anekdote am Rande: Die Verzögerung beim Löschen kam, weil die Polizei auf SIS II hoffte; für SIS II sind die Anforderungen, wann jemand eine Gefahr für die Staatssicherheit ist, geringer. BaWü war 2006 übrigens das Land mit den meisten Ausschreibungen; insofern ist der Umfang des Problems aus deutscher Sicht noch handhabbar.

7. SIS: 96er-Ausschreibungen

AusländerInnen zur Einreiseverweigerung, Top-Kategorie in SIS, seit Jahren um die 750000 Personen (kein Wachstum wegen Osterweiterung). Konsequenzen der Ausschreibung: Abweisen an den Grenzen, keine Erteilung von Visa, kein Aufenthaltstitel, wenn Menschen schon in der EU sind. Ein Staat, der davon abweichen will (sowas gibts), muss das mit dem ausschreibenden Staat abkaspeln.

Ausschreibungsgründe: Planung schwerer Straftaten, Ausweisung, Abschiebung usw. Auch nationales Recht wird akzeptiert; die Kommission hat schon mal den Griechen 96er-Ausschreibungen empfohlen, um türkische Fußballfans zu schneiden. Andererseits gibt es Urteile, nach denen die gängige Praxis, bei Abschiebung eine 96er-Ausschreibung vorzunehmen, rechtswidrig ist. In Hessen wurden Menschen nach 96 ausgeschrieben, die zum Verlassen der BRD aufgefordert worden waren und dann nichts mehr von sich hören ließen.

2008, Kreis Bergstraße, Untersuchung, ob 96er-Ausschreibungen nach 3 Jahren auf Löschung geprüft wurden: Von den 25 Ausschreibungen waren 5 komplett illegal, 13 waren gar nicht geprüft worden, die zwei, die ersichtlich geprüft worden waren, wurden auch gelöscht.

8. SIS: Datenschutz

In any event, [das Auskunftsrecht] shall be refused throughout the period of validity of an alert for the purpose of discreet surveillance
– SDÜ, Art. 109 (2)

Auskunftsrecht richtet sich in erster Linie nach nationalem Recht. Der ausschreibende Staat hat aber de facto Vetorecht.

Zu verdeckten 99er-Ausschreibungen gibts nie Auskunft.

Speicherfrist: 1 Jahr für 99, 3 Jahre für 96, aber großzügige Verlängerungspraxis. Die Praktiken unterscheiden sich sicher massiv nach MS und Zeit. In der BRD funktioniert das so, dass die ausschreibenden Behörden bei der ersten Verlängerung zur Löschung ankreuzen, bei der zweiten zur Verlängerung ankreuzen mussten. Irgendwelche Belege für stattgefundene Prüfungen mussten nicht beigebracht werden.

Zweckbindung: „Weltrechtsprinzip“, haha. An sich sollen die MS die SIS-Daten nicht in nationale Datenbanken überführen, und sie dürfen eigentlich auch nicht 96er-Daten z.B. für Drogen geschichten benutzen. De facto wird das aber doch gemacht, und Art. 102 erlaubt das auch, z.B. zwecks Staatssicherheit.

Überwachung von SIS durch die GKI (Gemeinsame Kontrollinstanz, JSB), zusammengesetzt aus DatenschützerInnen der MS. Die TB lassen eine gewisse Zahnlosigkeit ahnen.

9. Europol

Europol is information broker, so in first instance Europol expects information [...] from the MS.
– Europol FAQ on Third Parties and AWFs

Europol ist eine Semigeheimpolizei, die eingerichtet wurde, um MS-übergreifend „serious crimes“ zu bearbeiten. Näher bestimmt: Drogen, Autodiebstahl, OK, Terrorismus, Geldfälschung und -wäsche usf.

Zwei Typen von Datenbanken:

- Informationssystem (Europol-IS)
- Analysedateien (AWF)

10. Europol-IS

The European Council is convinced that the enhancement of actions at European level [...] are essential to protection from trans-national threats
– Stockholm-Programm

Europol-IS ist als eine Art KAN auf europäischer Ebene angelegt; vom Inhalt her ist es weitgehend ein Indexsystem. Der Kriminalaktennachweis KAN wird vom BKA geführt, die Daten kommen aber zu großen Teilen von den LKAN („Verbunddatei“). Abgefragt wird es ebenfalls vor allem von den LKAN.

Zweck: Übereinstimmungen zwischen Daten aus verschiedenen Ländern.

Hätte eigentlich 2004 aus allen Ländern automatisch Daten bekommen sollen, in der Realität BRD ab 11/2005, NL ab 9/2006 usf

Seit Aufnahme automatischer Übermittlungen rasches Wachstum: 2007 35000, 2008 90000 Objekte.

2008 125000 Anfragen.

11. Europol: AWF

... with a view to setting up an Observatory for the Prevention of Crime (OPC), the tasks of which will be to collect, analyse and disseminate knowledge on crime (including statistics) and crime prevention...
– Stockholm-Programm

Das Äquivalent von BKA-Amtdateien: Europol sammelt Infos, versucht sie auszuwerten und gibt sie nur an ausgewählte Dritte (nach Vertrag auch nicht-EU) raus.

Bereich	2007	2004	2003
Drogenhandel	3	4	4
„Verbrechen gegen Personen“	3	3	3
Wirtschaftskriminalität	2	5	5
„Organisierte Kriminalität“	4	2	3
„Terrorismus“	2	2	2
Geldfälschung	2	2	2

Mithin ist Europol im Politbereich gegenwärtig nicht sehr aktiv. Auch die Terror-Geschichte hat mehr religiöse Leute im Fokus.

Am ehesten noch in Frage kommen:

- AWF-03-029 DOLPHIN (seit 2003) – Non-Islamist extremist terrorist organisation. Das bezieht sich auf die EU-Terrorliste; wer PKKlerInnen oder Leute von der DHKP-C kennt, könnte darin landen.
- AWF 05-037 CHECKPOINT (seit 2006) – Facilitated Illegal Immigration. Klingt zwar mehr, als ginge es um Zwangsprostitution und ähnliches, aber im Ziel stehen offenbar Organisationen wie eine „Pachtou“, die angeblich Menschen aus Kurdisch-Irak und Afghanistan in die EU gebracht haben soll.
- AWF 09-041 CYBORG (seit 2009) – soll Organisierte Kriminalität im Netz verfolgen. Na ja.

Die AWF werden physikalisch von einer Software der deutschen Firma rola verhandelt.

12. Europol: Inhalt der AWF

Informationen für die kriminaltechnische Identifizierung wie Fingerabdrücke, [...] DNA-Profile, Stimmprofil, Blutgruppe, Gebiss
– Durchführungsbestimmungen für AWF, Ratsdokument 15140/09

In den AWF darf Europol ungefähr alles speichern, was es will:

- Namen, Geschlecht, Familienstand, gegenwärtige und frühere Wohnsitze, Geburtstag, -ort, Namen von Vater und Mutter
- „Rasse“, Religion, Politische Einstellung, sexuelle Orientierung und Gesundheit (wenn „stricly necessary“)
- Beschreibung, Merkmale
- Ausweispapiere, Biometrische Informationen
- augenblickliche und frühere Lohnarbeit, Ausbildung, Qualifikation, besondere Fertigkeiten
- Konten, Vermögen, Verbindungen zu Firmen, Steuerstatus, Freitext zu Finanzen.
- „Lebensstil“, Bewegungsprofil, Waffen, Einschätzung zur Gefährlichkeit, Drogenabhängigkeit
- Begleitpersonen
- Telefon, E-Mail, Verbindungen zu Internet
- verwendete Fahrzeuge
- Vorstrafen, Modi operandi, Mitgliedschaft und Rolle in kriminellen Vereinigungen, geographische Einordnung, Fotos und Videos aus der Ermittlungsarbeit, Verdacht
- Verweise auf Speicherungen bei Europol, nationalen Polizeien, anderen Behörden, Privatfirmen
- Informationen über Firmen u.ä., die im Zusammenhang mit dem Verdächtigen stehen (für Geldwäschesachen und so).

13. Europol: Datenschutz

In general, new legislative initiatives [...] should be tabled only after verification of the respect for the principles of proportionality and subsidiarity... – Stockholm-Programm

Datenschutz bei Europol klingt in Worten meist nach BRD-Recht.

... the following data [...] may be included where they are strictly necessary for the purpose of the file (das sind die „Rasse“ usf.-Geschichten, und das heißt wohl, dass es die anderen nicht wirklich brauchen muss.

Auskunftsrecht: kostenlos, **aber** nicht, wenn „Rechte und Freiheiten Dritter“ beeinträchtigt werden.

Noch unglaublicher: Auskunft unterbleibt *ohne Hinweis auf Speicherung*, wenn ein „unmittelbar betroffener Mitgliedsstaat“ der Auskunft widerspricht.

So gehts, wenn man eine internationale Geheimpolizei installiert. Übrigens hat auch Europol eine GKI, deren Selbstverständnis sich in einem Satz aus ihrem 4. TB konzentriert: „Aufgrund dieser Erfahrungen konnte die GKI zu einem verlässlichen und konstruktiven Partner für Europol [...] werden.“

14. Muaks!

This was done to increase the influence of the stakeholders and to establish the role of product management in the Europol national units in the member states
– Irgendein Europol-Jahresbericht

Die einzige gute Nachricht: Im Rennen zu den Fleichtöpfen der EU stehen sich alle gegenseitig auf den Füßen.

Beispiel Europol: „However, it was not delivered due to the under-estimation of the number of problems that would arise and/or the overestimation of the Consortium's capacity to deliver“.

Beispiel SIS II: Die Erweiterung von SIS zu biometrischen Daten und weniger strengen Kriterien hätte 2006 in Betrieb gehen sollen. Ende 2009 mahnte der Rat an, die Software hätte aber allmählich wirklich mal ein paar grundlegende Funktionstests zu bestehen, sonst werde der Kram eingestampft.

15. Prüm

...in some Member States the implementation of the Prüm Decision is seriously delayed...
– die österreichische Ratsdelegation 2009

2007 war das SIS II-Fiasko schon absehbar; daher hat die BRD mit ein paar ihrer engsten Freunde den Vertrag von Prüm geschlossen, der seit 2008 zum Acquis gehört.

- Staat A schickt Staat B Fingerabdrücke oder DNA-Profile und kriegt „VerdächtigeR, Tatortspur oder nichts“ zurück. Die Behörden von Staat B kriegen Matches mit und mailen nach Gusto weitere Daten an die Behörden von Staat A.
- Staat B ermittelt auf Anfrage für Staat B Fingerabdrücke oder DNA-Profile
- Bei „Tagungen des europäischen Rats“ un ähnlichem tauschen Staaten „Identifikationsdaten und Tatsachen“ von „Gefährdern“ aus.
- Staat A kann direkt nach Nummernschildern suchen.

16. Prüm: Umsetzung

Ende 2009: BRD tauscht DNA-Daten mit .at, .es, .lu, .sl und .nl, Fingerabdrücke nur mit .at aus. .at, .es, .lu, .nl, .fr können Kfz-Daten abfragen, die BRD kann das nirgends. Die österreichische Delegation sagt allerdings, die BRD könne das sehr wohl, und Österreich liefere Kfz-Daten an .be, .de, .es, .fr, .lu, und .nl. Wer weiß?

Das illustriert ein wenig, dass SIS II zu Prüm das EDV-Desaster nur noch verkompliziert: Wo SIS II nur n Schnittstellen hat (nämlich die „National Interfaces“ zum C-SIS), hat Prüm im Zweifel n^2 (nämlich von jedem Mitgliedsstaat zu jedem anderen Mitgliedsstaat).

Bereits 2008 will der Rat Prüm-Abfragen limitieren, da die Polizeien kleiner Staaten durch die Anfragen der großen völlig überfordert werden.

Bis September 2009: 5000 Treffer im Prüm-Verkehr, 4800 davon Trivialkriminalität oder Migrationskontrolle.

Bei den bekannten Gipfeln hat sich das BKA bei seinem Datenexport noch auf §14 BKAG berufen.

17. Fazit

- Auf EU-Ebene ist die einzige effektive Grenze für den Überwachungsstaat Inkompetenz, Misstrauen und Gier; Datenschutz bzw. Menschenrechte sind fast immer Lippenbekenntnis.
- Derzeit vor allem gegen MigrantInnen gerichtet.
- Daten in europäischen Datenbanken kommen fast immer von BRD-Polizeien, typischerweise rechtswidrig.
- Auskunft verlangen und löschen lassen.

<http://www.datenschmutz.de>