

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

Dazwischenwaffen!

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. MS geben sich teilweisen gegenseitigen Zugriff auf ihre Repressionsorgane.

Weiterer Punkt: Maastricht und der Euro.

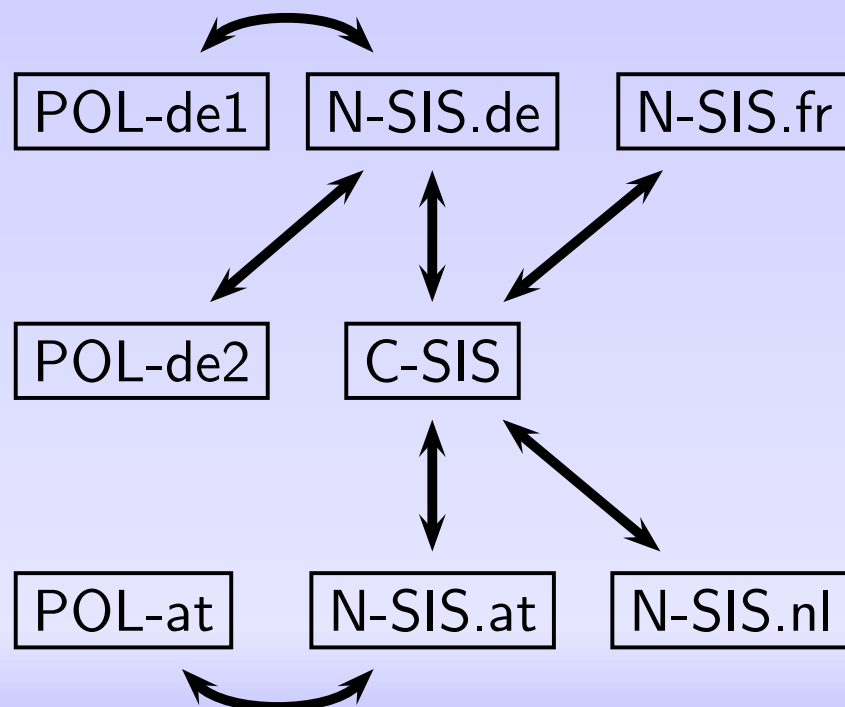
Fünfjahrespläne zur Sicherheit:

1. Tampere (2000-2004)
2. Den Haag (2005-2009)
3. Stockholm (2010-2015)

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.



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

SIS: Wer ist drin?

Well-managed migration can be beneficial to all stakeholders.

– Stockholm-Programm

Schengen-Informationen-System zur Kompensation des Wegfalls von Grenzkontrollen.

- 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 (26 000 000)

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)

SIS: 99er-Ausschreibungen

In der BRD immer verdeckte Registrierung; 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).

SIS: 96er-Ausschreibungen

AusländerInnen zur Einreiseverweigerung, Top-Kategorie in SIS, seit Jahren um die 750000 Personen (kein Wachstum wegen Osterweiterung).

Ausschreibungsgründe: Planung schwerer Straftaten, Ausweisung, Abschiebung usf.

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.

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.

Zweckbindung: „Weltrechtsprinzip“, haha.

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

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)

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.

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.

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

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).

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

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.

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.

Prüm

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

- Staat A schickt Staat B Fingerabdrücke oder DNA-Profile und kriegt „VerdächtigeR, Tatortspur oder nichts“ zurück.
- 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.

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.

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.

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>