

Datenschutz in der Strafverfolgung

Die (un)heimlichen Datensammlungen - von der Deutungsmacht und Deutungshoheit der Polizei

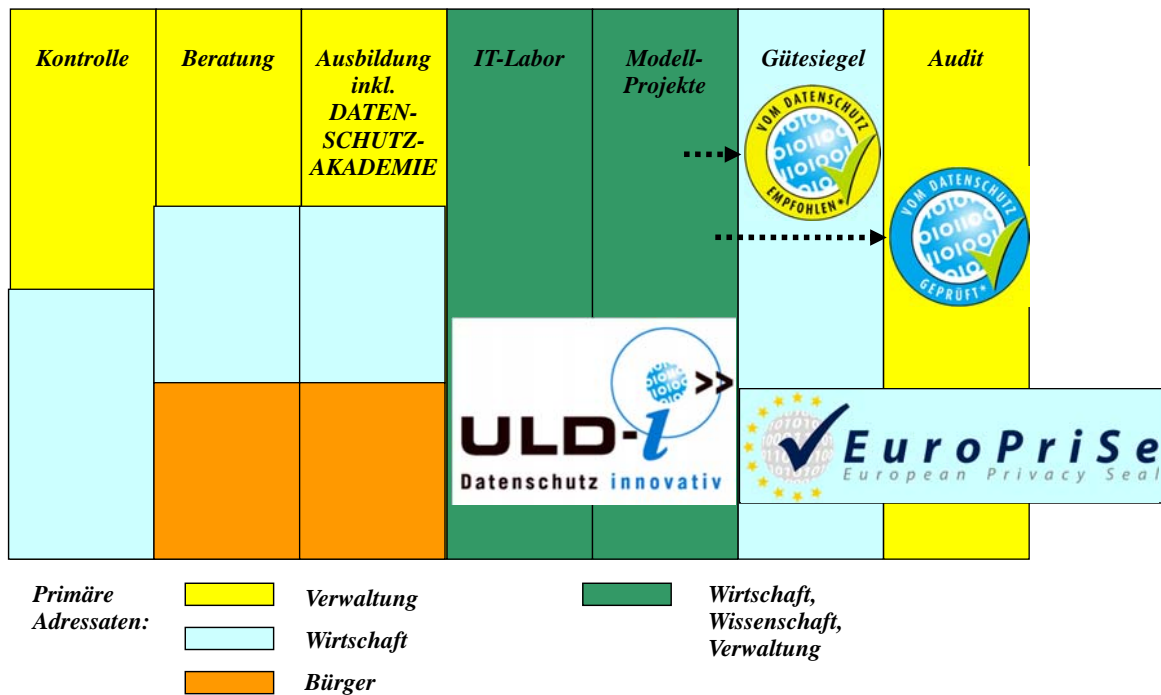
Thilo Weichert, Leiter des ULD
Landesbeauftragter für Datenschutz Schleswig-Holstein
Strafverteidigertag
Berlin, 26.03.2011



Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD
- Entwicklung der polizeilichen Datenverarbeitung
- Informationssystem der Polizei
- Sonstige Verarbeitung bei BKA und Landespolizeien
- Schnittstellen zu anderen Verarbeitern
- Rechtliche Grundlagen
- Datenschutzrechtliche Anforderungen
- Speziell Datenabgleich und Rasterfahndung
- Perspektiven

Unabhängiges Landeszentrum für Datenschutz



Entwicklung polizeiliche Datenverarbeitung

- Seit Bestehen der Kriminalpolizei: Diebeslisten und Register
- Kriminalakten und Aktennachweise, 50er Lochkarten
- 13.11.1972 Inbetriebnahme INPOL-Fahndungsdatei
- 1975 Gesamtkonzeption INPOL
- Anfang 80er PIOS-Dateien (Personen, Institutionen, Objekte, Sachen), SPUDOK (Spurendokumentationen)
- 1990 INPOL-Grundsätze Zusammenarbeit Bund-Länder
- Seit 1988 Vorbereitungen für INPOL-neu (Grobkonzept 92) flexible Datenformate (Text, Bild, Ton ...), Data-Warehouse-Anwendungen, Führungsinformationen und Auswertungs-Tools
- 2003 Start INPOL-neu, 2006 INPOL-neu 5.0

Visionen und Realität des Horst Herold

(Präsident des Bundeskriminalamtes – BKA – 1971-1981)

Kriminalgeografie – raumbezogen

Sozialforschung - milieubezogen

Prädiktive Kriminologie - täterbezogen

- > umfassende Erfassung der Persönlichkeit
- > Zentralisierung, Verwissenschaftlichung und Informatisierung der Kriminalitätsbekämpfung (BKA-Ausbau, INPOL als Verbund mit Spezialdateien)
- > Neue Formen der Fahndung (Elektronische Ausschreibung, Raster-, Schleierfahndung, Profiling)

Transatlantik-Interview (1980): „Sonnenstaat“

Reaktionen

Kritik der Linken und des liberalen Bürgertums : Missachtung der kollektiven und individuellen Selbstbestimmung

Widerstand gegen Volkszählungen 1983/87:

Volkszählungsurteil des BVerfG > Recht auf informationelle Selbstbestimmung

Normative Bindung der Sicherheitsbehörden

(Sicherheitsgesetze, informationelle Gewaltenteilung, Zuerkennung von Betroffenenrechten)

Gesellschaftlicher Diskurs über Sicherheitsinfrastruktur, über justizielle Kontrolle der Polizei, über Transparenz

INPOL I

Verbundteilnehmer: BKA, LKÄ, Landespolizeien, Bundespolizei, Zoll mit Grenzkontrollaufgaben, Zollkriminalamt

- Personenfahndung (4,4 Mio.)
- Kriminalaktennachweis (KAN, 4.3 Mio.)
- Innere Sicherheit (früher APIS, 1,5 Mio.)
- Haftdatei (500 T.)
- Violent Crime Linkage Analysis System (ViCLAS)
- DNS-Auskunftsdatei (DAD – Gendatenbank, 800 T.)
- Erkennungsdienst (ED, 5,9 Mio.)
- Automatisiertes Fingerabdruckidentifikationssystem (AFIS-P, 2,5 Mio.)

INPOL II

- APOK (Organisierte Kriminalität, 270 T.)
- Falldatei Rauschgift (FDR)
- Fedok (Finanzermittlungen, 7 T.)
- FUSION (Rockerkriminalität, 58 T.)
- Schleusungs-, Dokumentenkriminalität (DOMESCH, 120 T.)
- Gewalttäterdateien (u.a. LiMo 1,9 T., ReMo, AuMo)
- Gewalttäter Sport (11 T.)
- USA (11.09.2001, 80 T.)
- Kinderporno (47 T.)

PHW beim INPOL (Bund)

Personengebundene Hinweise (PHW)

§ 7 Abs. 3 BKAG: BEWA, Bewaffnet; GEWA, Gewalttätig; AUSB, Ausbrecher; ANST, Ansteckungsgefahr; GEKR, Geisteskrank; BTMK, BtM-Konsument; FREI, Freitodgefahr; PROS, Prostitution; § 8 Abs. 2 BKAG: VEMO, Straftäter verbotener militanter Organisation/Vereinigung/Partei/ Gruppe; REMO, Straftäter rechtmotiviert; LIMO, Straftäter linksmotiviert; AUMO, Straftäter politisch motivierter Ausländerkriminalität; EXPL, Explosivstoffgefahr; SEXT, Sexualtäter; HWAO, Häufig wechselnder Aufenthaltsort; § 7 oder § 8 BKAG, je nach Fallkonstellation: BEWA, Bewaffnet; GEWA, Gewalttätig; AUSB, Ausbrecher; FREI, Freitodgefahr.

BKA-Dateien

- BKA-Zentraldateien:
BKA-Aktenachweis (2,2 Mio.)
Globalisierung (IgaSt, 3 T.)
ABC-Waffen (4 T.)
VISA-Konsultation zentrale Behörden (2 Mio.)
Islamischer Terrorismus (DABIS, 9 T. Pers., 3 T. Orga.)
u.v.m.
- BKA-Amtsdateien (ca. 100: Schleusung, Nineeleven, Rauschgift, Geldwäsche, Untreue, Menschenhandel, Kindesmissbrauch, Personenschutz...)

Zugriffe auf externe Systeme

- Ausländerzentralregister (AZR)
- (AFIS-A)
- Bundeszentralregister (BZR beim BAJ)
- Zentrales Verkehrsinformationssystem beim KBA (ZEVIS)
- Bundeszentralamt für Steuern (Kontodaten)
- EURODAC (266 T.)
- SIS (Schengen, z.B. Personenfahndung 110 T.)
- Europäisches Informationssystem (EIS) Europol
- Interpol-Zugriffe über BKA

Länder-IT, Geheimdienst-Kooperation

Länder

- Vorgangsdokumentation (z.B. IGVP Bay, @rtus-VBS SH)
- Viele Spezialdateien (analog Zentral- u. Amtsdateien BKA), z.B. Register Sexualstraftäter, Analyse- und Auswertedateien

Geheimdienstkooperation

- Antiterrordatei
- Projektdateien
(Rechtsgrundlage Anti-Terror-Dateigesetz, wird vor dem BVerfG angegriffen)
- Gemeinsame Lagezentren (GIZ, GTAZ, GASIM)

Entwicklungen

- Europäisierung: Schengen, Europol, Eurodac, Prüm, Stockholmer Programm, Euro-PNR, Euro-TFTP
- Internationalisierung (u.a. USA, z.B. PNR, SWIFT/TFTP)
- Vergeheimdienstlichung
- Weiterentwicklung der Technik (DNA-Datei, Biometrie, Internetüberwachung, Data-Warehousing, z.B. PIAV)
- Einbeziehung Privater in polizeiliche Ermittlungen (TK, PNR, SWIFT)

Rechtsgrundlagen

- Bundeskriminalamtgesetz (BKAG), Bundespolizeigesetz, Zollfahndungsdienstgesetz
- Strafprozessordnung (§§ 474 ff. StPO)
- Bundesdatenschutzgesetz (BDSG)
- Landespolizeigesetze
- Bei Speicherung nach StPO und PoIR geht PoIR vor (§ 483 III StPO)

Errichtungsanordnung u. Verordnung

- Errichtungsanordnungen (Verwaltungsvorschriften): Konkretisierung der Datenkategorien, Datenumfang (i.d.R. VS-nfD, teils „geheim“)
- Rechtsverordnung (§ 7 VI BKAG) regelt Einbindung in Verbund und Art der Daten
- VG Hannover 22.05.2008/OVG Nds. 16.12.2008: Verbunddatei Gewalttäter Sport setzt wirksame RVO voraus
- Erlass der RVO vom 04.06.2010, in Kraft ab 09.06.2010
- BVerwG 09.06.2010 Speicherung jetzt rechtmäßig

Zweckbindung

- Grundsätzlich Zweckglocke Gefahrenabwehr-Strafverfolgung (§ 481 StPO), wenn keine besondere Regelung
- Differenzierung der Zwecke: Verfolgung künftiger Straftaten – Vorgangsbearbeitung – Vorgangsdokumentation (papierlose Verarbeitung)
Zweckbindung durch Erforderlichkeitskontrolle (need to know):
- Technische Zweckbindung durch Zugriffsbeschränkung
- Regionale Zugriffsbeschränkung bei örtlichen Vorgängen
- (Automatisierte) Auswertungen müssen auf anonymisierter Basis erfolgen (Führung, Organisation, Statistik)

Rechtmäßigkeit

Materielle Rechtmäßigkeit manchmal fraglich, z.B.:

- SWIFT-Daten an US-Sicherheitsbehörden von Europol
- 3.000 Datensätze wg. Beleidigungen in DAD (DNA-Datenbank) = Erwartung, dass der Beschuldigte „Straftaten von erheblichen Bedeutung“ begeht
- Geruchsprobendatenspeicherung von G8-Gipfel-Gegnern beim BKA

Aber selten rechtliche Anfechtung durch die Betroffenen und Thematisierung in sonstigen Verfahren (evtl. Verwertungsverbot)

Datenqualität

Generell gilt: Immer vor Datenfreigabe Relevanz- und Qualitätsprüfung

- Gerichtsüberprüfte Daten (Verurteilung, Freispruch 1. u. 2. Klasse, Einstellung §§ 153/153a, 170 II StPO)
- Harte Polizeidaten (objektive Feststellungen u. Daten)
- Weiche Daten (Verdacht, Vermutung, fließende Übergänge) > Gefahr der Falschverdächtigung
- Differenzierung nach Sensibilität (vgl. § 3 IX BDSG, Berufsgeheimnisse, heimliche Erhebung, Kernbereichsbezug)
- Betroffenenrechte haben hohe Relevanz für Qualität (Richtigkeit, Rechtmäßigkeit): Berichtigung, Sperrung, Gegendarstellung
- Kontext und Quelle müssen erkennbar sein (z.B. durch Metadaten oder Protokolle)

Betroffenenstatus

- Straftäter
- Beschuldigter
- Straftatverdächtiger
- Gefährder/Störer
- Zeuge, Hinweisgeber
- Opfer, gefährdete Person
- Vermisste/unbekannte/hilflose Person, Tote
- Kontakt- und Begleitperson
- Hilfsperson
- Dritter (Sonstige)

Data-Warehouse

Beim Data-Warehouse besteht grds. Zweckvielfalt

Vor Einstellung: Qualitätsprüfung erforderlich

- Festlegungen: funktionale Anforderungen, Bedarfsträger, Nutzungsszenarien – im Rahmen der Gesetze
- Datensätze müssen Zweck-Metadaten enthalten (Data-Mart)
- Recherchen in Freitexten und Vorgangsdokumentationen nur nach definierten Vorgaben (Technik, Dienstvorschriften)
- Präzise Rollen- und Aufgabenbeschreibungen: Super-User, normaler Ermittler (nur begrenzt fremde Daten), Sachbearbeiter
- Kein Data-Mining

Erforderlichkeit, Datenlöschung

- Organisatorische Erforderlichkeitsregeln genügen nicht, Technikvorgaben sind zwingend
- Relevanzprüfung bei jeder Datennutzung
- Erforderlichkeitsprüfung des Vorgangs bei konkretem Anlass (evtl. Einzelfallbearbeitung) vor Fristablauf
- Aussonderungsprüffristen: Erwachsene bis zu 10, Jugendliche bis zu 5, Kinder bis zu 2 Jahren
- Keine automatische Fristverlängerung
- Verfahrensevaluierung nach Neueinführung (z.B. nach 3 Jahren)

Auskunftserteilung

- § 147 StPO: Akteneinsicht des Verteidigers nicht bei Gefährdung des Untersuchungszwecks
- Auskunftsanspruch an Betroffene
Pauschal-Auskunftsverweigerung unzulässig, Einzelfallbegründung nötig
- Bei Verbunddateien Weiterleitungspflicht an verantwortliche Stelle (§ 6 II BDSG) Umsetzung fraglich
- Bei Auskunftsverweigerung Kontrollmöglichkeit durch zuständigen DSB (LfD, BfDI)

Lokale Schnittstellen

- Zugriff auf (lokales) Melderegister
- Zugriff auf (lokales) Personalausweis-/Passregister
- Kooperation mit Rettungsleitstellen (Feuerwehr, medizinische Notfallversorgung, Katastrophenschutz)
- Kein Zugriff durch Staatsanwaltschaft
- Nutzung für Sicherheitsüberprüfungen, Zuverlässigkeitsüberprüfungen, Einstellungsverfahren

Protokollierung

- Vollprotokollierung sowohl bei lesendem wie bei schreibendem Zugriff (§ 11 VI 1 BKAG, teilw. noch streitig)
- Bei Aktenrückhalt ist klarer Aktenbezug nötig
- Bei rein elektronischer Vorgangsbearbeitung muss Kontext nachvollziehbar (selbstsprechend) sein
- Protokolle müssen automatisiert einfach auswertbar sein
- Protokolle müssen regelmäßig ausgewertet werden
- Befristete Speicherung der Protokolldaten (i.d.R. 1 Jahr bzw. bis Löschung)
- Strenge Zweckbindung (Datensicherheit, Datenschutzkontrolle, Systembetrieb), ausnahmsweise Polizeizwecke

Datenabgleich

- Rechtsgrundlagen § 98c StPO, PolizeiR
- Zweck: Aufklärung einer Straftat/Gefahr, Aufenthaltsklärung von Fahndungszielperson
- Polizeiinterner Abgleich von Datenbeständen (wenn keine besonderen Schutzvorschriften bestehen)
- Ungeschriebene Voraussetzung: Verhältnismäßigkeit

Rasterfahndung

§§ 98a, 98b StPO, Landespolizeigesetze

- Einbeziehung von Unverdächtigen (eigene und fremde – private u. Öffentliche – Datenbanken)
- Hypothese für Verdachtsgewinnung aus Merkmalen
- Anordnungsbefugnis Richter, StA/Leitung bei Gefahr im Verzug
- Tatsächliche Anhaltspunkte, Benachrichtigung, keine besonders geschützten Daten
- Straftat von erheblicher Bedeutung
- Praxis 11.09.2001: Suche nach terroristischen „Schläfern“

Merkmale: unauffälliges Verhalten, männlich, 18-40, Student, Moslem, geboren in Staat mit islamischer Bevölkerung, Datenbeschaffung bei Universitäten, Meldebehörden, AZR, Datenabgleich mit Fluglizenzen, Atomgesetz-Zuverlässigkeitsüberprüfung, Arbeitgebern

BVerfG, B.v. 04.04.2006 (1 BvR 518/02)

Abwägung zw. Eingriffsschwere und Schutzziel

Ziel: Abwehr einer Gefahr für Bestand und Sicherheit v. Bund u. Land, Leib, Leben und Freiheit = hochrangige Verfassungsgüter

Gefahr für Betroffene: sensible Daten, drohende Diskriminierung, nachteilige Auswirkungen, Stigmatisierung

Gesellschaftl. Relevanz: Streubreite, Einschüchterungseffekt

Vorkehrungen: Verfahren, indiv. und gesellschaftliche Transparenz

Gesetz noch in Ordnung, konkrete Maßnahme verfassungswidrig:
Konkrete Gefahr setzt tatsachenbasierte Wahrscheinlichkeitsprognose voraus

Prüfschema

Polizeiliche Aufgabe?

Zulässigkeit der Datenerhebung?

Zulässigkeit der Datenspeicherung (gesetzliche Grundlage, Erforderlichkeit)

Formelle Anforderungen an Datei, Verfahren, Transparenz

Verhältnismäßigkeitsprüfung

Angemessenheit des Verfahrens (Datesparsamkeit)

Bei Rechtsverstößen: Löschung, Sperrung, Berichtigung, Zusatzspeicherung, Schadenersatz, Verwertungsverbot

Perspektiven

- Rasante technische Entwicklung bei Datenerhebung, -speicherung, -auswertung und -übermittlung
- Anwaltliche Befassung mit Datenspeicherung bisher nur rudimentär
- Verhältnis unzulässige Datenspeicherung – Verwertungsverbote noch nicht endgültig geklärt
- Öffentliche Debatte über polizeiliche Datenspeicherung spielt kaum (noch) eine Rolle
- Polizeiliche Datenspeicherung hat angesichts technischer Entwicklungen (IT- und Bio-) sowie Internationalisierung weiterhin höchste Grundrechtsrelevanz

Datenschutz und Strafverfolgung

Dr. Thilo Weichert

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Independent Center for Privacy Protection Schleswig-Holstein (ICPP)

Holstenstr. 98, D- 24103 Kiel

mail@datenschutzzentrum.de

<https://www.datenschutzzentrum.de>