Polizeiliche Datenverarbeitungen: Grundlagen, Praxis und Betroffenenrechte

RAV- ExpertInnentreffen Polizeirecht, Berlin, 13. Januar 2007*

Gliederung:

I. Grundbegriffe

1. Datenverarbeitungsrechtliche Begrifflichkeit
2. Grundrechtsrelevanz und neuere Entwicklungen

II. Polizeiliche Dateien

1. Typen (Amts- /Zentral- / Verbunddateien)
2. Rechtsgrundlagen
3. Polizeiliche Dateien in der BRD (Überblick)
4. Polizeiliche Dateien in der Praxis am Beispiel von Großereignissen

III. Rechtliche Betrachtung: effektive Programmierung polizeilicher Datenverarbeitung und –Übermittlung?

- Grundlagen der Übermittlung im Verhältnis P(räventivp)olizei/ Strafverfolgungsbehörden/ Nachrichtendienste
- Besonderheiten bei Dateien

IV. Datenschutzrechtliche Rechte der Betroffenen

1. Berichtigung/Sperrung/Löschung
2. Auskunft

V. Ausblick: Gemeinsame Dateien Gesetz u.a.

* überarbeitete Fassung des handout

Sönke Hilbrans
Rechtsanwalt und Fachanwalt für Strafrecht
Immanuelkirchstr. 3 – 4
10405 Berlin
hilbrans@diefirma.net

I. Grundbegriffe

1. Das „Kleine Lexikon der Datenverarbeitung“: § 3 BDSG, beschreibt die datenschutzrechtliche Begrifflichkeit. Weitere Merkposten: Das moderne Datenschutzrecht differenziert lediglich noch zwischen Akten und Dateien; begrifflich bedeuten ist auch die Unterscheidung von Spontanübermittlung/ Übermittlung auf Ersuchen/ online- Abruf.

2. Grundrechtliche Problematik (Überblick)

Ausgangspunkt: Volkszählungsurteil 1983. Informationelle Selbstbestimmung (Art. 1 Abs. 1, 2 Abs. 1 GG und besonderes Grundrecht auf Datenschutz im Verfassungsrecht einiger Bundesländer, z.B. Berlin); Datenverarbeitung = Grundrechtseingriff; Gesetzesvorbehalt/ Bestimmtheitsgebot („Straftat von erheblicher Bedeutung“, „Kontakt- und Begleitperson“); datenschutzrechtliche Sicherungsvorkehrungen (Auskunft, Sperrung/ Löschung, Datenschutzbeauftragte usw.). Äußere Grenzen: Totalüberwachung, Kernbereich privater Lebensgestaltung. Neue Entwicklung: Informationsfreiheit.

II. Polizeiliche Dateien

1. Typen: Amts-/Zentral-/Verbunddateien.

2. Rechtsgrundlagen

a) BKA: §§ 7 - 9, 11 – 13 BKAG, §§ 483 ff StPO, auch für polizeiliche Dateien zu Zwecken der (Vorsorge für künftige) Strafverfolgung; Polizeigesetze der Länder, Nachrichtendienstrecht, Sonderbehörden des Bundes.

b) Zusammengreifen verschiedener Rechtsgrundlagen/ Begriff und Bedeutung der datenschutzrechtlichen Verantwortung (Bsp.: § 12 BKAG)

c) Errichtungsanordnungen/ Speicherungsfristen (genauer: Regelprüfungsfristen, da absolute Speicherungshöchstfristen sehr selten sind)/ Zugriffe/ Protokollierung.

3. Polizeiliche Dateien: Die wesentlichen Anwendungen

a) Dateien bei dem Bundeskriminalamt

(nach: www.datenschmutz.de (ist aus juristischer Sicht z.T. kritisch zu lesen) und BT-Drs. 16/2875)

(-> INPOL: § 11 BKAG; schon heute keine durchgehende physikalische Trennung von Datenbeständen))

a Verbunddatei KAN -- der Kriminalaktennachweis (im INPOL-neu mit suchfähigen abstracts von Kriminalakten)

a Verbunddatei AFIS -- Automatisiertes Fingerabdruck-Identifizierungssystem (mit Sonderanwendung für ED- Daten auf aufenthalts- und asylverfahrensrechtlicher Grundlage)

a Verbunddatei DAD -- DNS-Auskunftsdatei, "Gendatenbank"

a Verbunddatei PERSONENFAHNDUNG -- (§ 9 BKAG), Fahndung nach Personen zur Festnahme, Ingewahrsamnahme, Aufenthaltsermittlung, polizeilichen Beobachtung; Überwachung bei Führungsaufsicht, durch Nachrichtendienste und nach zollrechtlichen Bestimmungen. 1999: mehr als 1. Mio. Personen ,2006 ca. 900000 Datensätze , Verbund mit Funkterminals ,

aa dabei: grenzfahnungspolizeiliche Ausschreibungen und nachrichtendienstliche Ausschreibungen (§§ 30, 31 BPolG („Grenzfahndungsbestand")).

aa und „Polizeiliche Beobachtung" (§§ 163e StPO, 9 BKAG) (1999: 2.000 Personen einschließlich Mitteilung von Begleitpersonen, Typ.: PIOS-Fälle).

a Datei APIS -- Arbeitsdatei PIOS Innere Sicherheit

a Verbunddatei "INNERE SICHERHEIT" -- eingerichtet nach Auskunft des BKA 1980 und mithin einer der ältesten Bestandteile von INPOL. 2006 fast 1.5 Millionen Datensätzen.

a Amtsdatei Global – sog. Auswertedatei (Status 2007 unklar)

a Zentraldatei G8 -- Sammlung und Auswertung von Informationen zur Bekämpfung des Widerstands gegen den G8-Gipfel in Heiligendamm. Eingerichtet 2006, im Oktober 2006 gerade mal 162 Datensätze

a Zentraldatei IgaSt -- Sammlung und Auswertung zur Bekämpfung des Widerstands gegen "Globalisierung". Eingerichtet 2003.

a Verbunddatei "GEWALTTÄTER LINKS" -- Eingerichtet Jan 2001, enthielt 2006 lediglich gut 1000 Datensätze

a Verbunddatei "GEWALTTÄTER POLITISCH MOTIVIERTE AUSLÄNDERKRIMINALITÄT" -- Eingerichtet Jan 2001, enthielt 2006 300 Datensätze

a Verbunddatei "GEWALTTÄTER RECHTS" -- Eingerichtet Jan 2001, enthielt 2006 rund 1800 Datensätze

a Verbunddatei "GEWALTTÄTER SPORT" -- Eingerichtet Jan 2001, enthielt 2006 rund 10000 Datensätze

a Verbunddatei FIT -- Fundstellennachweis islamischer Terrorismus

a Verbunddatei ViCLAS -- Violent Crime Analysis System

a Verbunddatei APOK -- Aufklärung/vorbeugende Bekämpfung im Bereich organisierte Kriminalität (Okt 2006: 280000 Datensätze)

a Verbunddatei APR -- Aufklärung/Verhütung von Straftaten im BtmG- Bereich (Okt 2006: 550000 Datensätze)

a Verbunddatei DOMESCH -- zur Bekämpfung von "Schleusungs- und Dokumentenkriminalität" (Okt 2006: 1200000)

a Verbunddatei ERKENNUNGSDIENST -- *Nachweis* von ED-Behandlungen (Okt 2006: 5.8 Millionen Datensätze)

a Verbunddatei FDR -- "Falldatei Rauschgift"

a Verbunddatei FUSION -- "Bekämpfung der Rockerkriminalität"

a Verbunddatei HAFTDATEI

a Verbunddatei KINDERPORNOGRAFIE -- enthielt 2006 rund 320000 Einträge.

a Verbunddatei NSIS-PERSONENFAHNDUNG -- Spiegel des CSIS, 2006 ca. 1.3 Millionen Datensätze

a Verbunddatei NSIS-SACHFAHDNUNG -- 2006 ca. 15.5 Millionen Datensätze

a Verbunddatei SACHFAHNDUNG -- seit 1985, 2006 waren 10.6 Millionen Datensätze gespeichert

a Rund 20 weitere Verbunddateien zu Rauschgift, Falschgeld, Geldwäsche, Korruption (diese 2006 mit lächerlichen 7000 Einträgen), vermissten Personen, Prostitution, Landesverrats, Spionage, 129b [ausländische Terrorgruppen], Computersabotage usf.

a Zentraldatei BKA-Aktennachweis -- Nachweis der Kriminalakten bei BKA (2006: 2.4 Millionen Datensätze)

a Zentraldatei DABIS -- eingerichtet 2002, dient der "Bekämpfung islamistischen Terrorismus. 2006 Nachweis von 22000 Personen und knapp 4000 Organisationen.

a Zentraldatei DAREX -- Auswertedatei zur Verfolgung der Verbreitung aus politischen Gründen zensierter Medien (von Handschriften bis DVDs)

a Zentraldatei FIU-Datei -- Sammlung und Auswertung von Meldungen nach dem Geldwäschegesetz.

a Zentraldatei InTE-Z -- Bekämpfung des "internationalen Terrorismus", 2006 sind knapp 8000 "Objekte" und 17000 "Beziehungen" gespeichert

a Zentraldatei LANDESVERRAT -- 2006 eingerichtet, 180000 Datensätze

a Zentraldatei PERSONENLISTE ST-32 -- Übersicht über "aktuelle Gefährder" im bereich des "islamistischen Terrorismus". 2006 eingerichtet. BKA ST 32 ist zufällig auch Gastgeber des GTAZ.

a Zentraldatei ReKa -- "Rechtsextremistische Kameradschaften". 2001 eingerichtet.

b) (Amts- und Zentral-) Dateien der Länder und der Staatsanwaltschaften (etwa AStA in Berlin)

c) NADIS – NAchrichtenDienstliches InformationsSystem: der Informationsverbund der Verfassungsschutzämter des Bundes und der Länder

d) Nicht- polizeiliche Dateien (hier gibt es z.T. Höchstspeicherungsfristen):

BZR, AZR usw.

ZEVIS (Halterabfragen usw.): Onlinezugriff der Polizei

Melderegister: Nur lokale Onlinegriffe

Sondervorschriften: §§ 22 Abs. 2 Nr. 2 PassG, 2 b Abs. 2 S. 2 PersonalausweisG

e) Zwecke polizeilicher Verbunddateien: Kommunikation vs. „Analyse“: „Projektdateien“; Übermittlungsreflexe, – Standard bei Fall- Dateien in INPOL

4. Praxis bei Großereignissen

a) Organisatorische Umgebung: Verbindungsbeamte, ad-hoc- Lagezentralen (z.B. NICC zur WM 2006), Kompatiblität (z.B.: bislang kein BOS- Digi.funk)

b) Technische Möglichkeiten und Ausstattung

c) Bsp.: Genua 2001:

- Die PIOS-Anwendung APFL (heute wohl Teil der Datei „Innere Sicherheit“) wurde 2001 in den Fahndungsdatenbestand eingegeben (heute würde man wohl sagen: die Nutzung wurde freigeschaltet) und im Wege der Einzelabfrage per Funk bei Beamten, die Zugang zu Sichtterminals hatten, abgerufen.
- Übermittlung bzw. Zugriff von dt. Verbindungsbeamten im Ausland auf INPOL-Anwendungen.

- Lokale Behörden griffen wohl i.W. auf Ländersysteme zurück, um Ausreisesperren zu begründen (da sich die Länder via INPOL aber ohnehin wechselseitig unterrichten, dürfte gegenüber einer Recherche in entspr. INPOL- Beständen kaum ein Nachteil entstehen).

d) Zur Info: § 43 Abs. 2 SOG MV (Datenabgleich zur Erkennung von Kraftfahrzeugkennzeichen):

(1) Die Polizei kann unter den Voraussetzungen der §§ 27a, 29, 32 oder 33 Abs. 1 Nr. 1 im öffentlichen Verkehrsraum personenbezogene Daten durch den offenen Einsatz technischer Mittel zur elektronischen Erkennung von Kraftfahrzeugkennzeichen zum Zwecke des automatisierten Abgleichs mit dem Fahndungsbestand erheben. Eine verdeckte Datenerhebung ist nur unter den Voraussetzungen des § 26 Abs. 2 Satz 2 zulässig. Die Datenerhebung darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen sind.

(2) Der Abgleich erhobener Kennzeichendaten mit anderen polizeilichen Dateien ist nur zulässig, soweit die Dateien zur Abwehr von im Einzelfall oder im Hinblick auf bestimmte Ereignisse allgemein bestehende Gefahren errichtet wurden und der Abgleich zur Abwehr einer solchen Gefahr erforderlich ist.

III. Rechtliche Betrachtung

a) „Erforderlichkeit zur Aufgabenerfüllung“ , die Mutter aller informationellen Eingriffstatbestände (besonders unschönes Beispiel wg. der zusätzlichen Vermutungskomponente: § 43 Abs. 1 S. 2 SOG MV „Personenbezogene Daten anderer Personen kann die Polizei abgleichen, wenn tatsächliche Anhaltspunkte dafür bestehen, daß dies *zur Erfüllung polizeilicher Aufgaben erforderlich* erscheint.“)

b) Zweckänderungskaskaden/ “Datenwäsche“ / Befugnisshopping

c) Datenschutzrechtliche Verantwortung in Verbunddateien (z.B. § 3 Abs. 7 BDSG, § 12 BKAG): Speichernde Stelle vs. Zuständigkeit für Auskunft u.a..

d) § 481 StPO: Übermittlungsgeneralklausel für die Verwendung von Strafverfolgungsdaten durch die Polizei „nach Maßgabe der Polizeigesetze“ (verdrängt § 477 Abs. 3 S. 4 StPO) bei Beachtung „besonderer Verwendungsregelungen“

e) Zweckänderung polizeilicher Daten ohne Übermittlung: Generalklauseln in Polizeigesetzen der Länder (§§ 42 Abs. 3 ASOG, 16 Abs. 2 HHPolDVG, 37 Abs. 2, Abs. 1 SOG MV) betrifft auch Nicht-Beschuldigte (Kontakt- und Begleitpersonen, ZeugInnen, potentielle Opfer usw.). TK-Daten: Zitiergebot in den Polizeigesetzen der Bundesländer (wird nicht beachtet). Verwendung rechtswidrig erhobener Daten nur teilweise ausgeschlossen (B,

Bbg, HB, Nds, NW, Thü, SOG); teils Geltungsanordnung für § 163 a Abs. 3 S. 2 StPO entspr. (etwa § 12 Abs. 4 HessSOG, SOG MV)

f) Übermittlung von Strafverfolgungsdaten an Nachrichtendienste: § 474 Abs. 2 StPO i.V.m. § 18 BVerfSchG (Abgrenzung von Akteneinsicht, Übermittlungspflicht vs. Übermittlungsermessen vs. Übermittlungsersuchen; Spezialregelungen in §§ 23 – 26 BVerfSchG; Harmonisierung mit TKÜ-Sondervorschriften in § 18 Abs. 6 BVerfSchG)

g) Übermittlung von präventiv-polizeilichen Daten zur Strafverfolgung: Teilweise Öffnungsklauseln in den Polizeigesetzen, i.Ü. § 161 StPO

h) Übermittlung von Präventivdaten an Nachrichtendienste? Kein Spezialgesetz, aber typischerweise Öffnungsklauseln für die Übermittlung „an andere öffentliche Stellen“ und § 18 Abs. 2., Abs. 1 BVerfSchG (z.B. § 41 Abs. 5 SOG MV), beachte aber besondere Vorschriften des Polizeirechts wie § 44 Abs. 4 ASOG: zum Teil Übermittlung von Nicht-Störern nur an Polizeibehörden (aber § 39 Abs. 1 SOG MV).

i) Übermittlungen durch die Nachrichtendienste: Trennungsgebot (Verbot der institutionellen Verzahnung von Vollzugspolizei und Nachrichtendiensten und Verbot des Vollzuges nachrichtendienstlicher Maßnahmen durch die Polizei; umstritten: Auftrag zu spezifischer informationeller Gewaltenteilung?) §§ 19, 20 BVerSchG (von Datenübermittlungen an Polizei und Staatsanwaltschaften, Übermittlungsermessen) § 20 Abs. 2 BVerfSchG und § 161 StPO: Ersuchensbefugnis der Polizei; keine Schwellenharmonisierung (etwa auch Übermittlung von Bildern aus Wohnung: §§ 8 Abs. 2, 9 Abs. 2 BVerfSchG) und keine Lösung für rechtswidrig erhobene Verfassungsschutzdaten. Sondervorschriften des Polizeirechts: etwa § 44 Abs. 7 ASOG.

j) Praktisches Problem: Veralterte Daten (trotz Nachberichtspflichten, etwa § 482 StPO u.a.).

k) Datenschutzrechtliche Sicherungen: Kennzeichnungen usw..

IV. Rechte der Betroffenen

1. Berichtigung/Sperrung/Löschung

a) Sachliche Richtigkeit, Erforderlichkeit und sonst. Speicherungsvoraussetzungen noch gegeben?; Prüf- statt Löschungsfristen. Sonderfall: Rechtmäßigkeit der Erhebung als Speicherungsvoraussetzung (z.B. § 45 Abs. 2 Nr. 1 SOG MV). Sonderproblem: Beweislast

für die Richtigkeit? (BVerwG: bei non liquet bzgl. der Richtigkeit kann nicht etwa die Löschung, sondern nur die Eintragung eines Widerspruchs gegen die Richtigkeit verlangt werden).

b) Datenschutzrechtliche Argumente: „Schutzwürdige Interessen“, „besondere Verwendungsregeln“ (z.B.: Verwendungs- und Verwertungsverbote; Sozialdatengeheimnis: §§ 35 SGB I, 67ff SGB X; Steuergeheimnis, § 30ff AO, …).

2. Auskunft und Auskunftssrechtsstreit

a) Grundregeln § 19 BDSG: „Dem Betroffenen ist auf Antrag Auskunft zu erteilen über … die zu seiner Person gespeicherten Daten, … Herkunft … Empfänger…Zweck der Speicherung (Abs. 1). Die Auskunfterteilung unterbleibt, soweit die Auskunft die ordnungsgemäße Erfüllung der … Aufgaben …. oder die öffentliche Sicherheit oder Ordnung gefährden würde (Abs. 4).“ Schutzwürdige Interessen Dritter; „ihrem Wesen nach geheim zu halten“; § 48 SOG MV, Nachrichtendienstrecht u.a.: „Besonderes Interesse“ an der Auskunftserteilung (typ.: Bewerbung für den öff. Dienst); Auskunftsanspruch vs. Auskunftsermessen. BVerfG: Methodenschutz jedenfalls bei schwerwiegenden Informationseingriffen kein Auskunftshindernis.

b) Rechtsstreit: Vorbeugender Rechtsschutz? (nur auf Sperrung). In- Camera- Verfahren (§ 99 VwGO). Regelstreitwert.

c) Flankierende Maßnahmen: Datenschutzbeauftragte u.a.; Beschwerden entspr. § 98 Abs. 2 StPO; Sonderproblem: Anordnungen des ErmittlungsRi beim BGH/ Anhörungsrüge? – nicht vergessen: G10- Anträge (während lfd. Maßnahme kann nur Prüfung erreicht werden).

d) Kosten(falle): Gegenstandswert im datenschutzrechtlichen Rechtsstreit bei den VGen regelm. € 5.000,-; ordentl. Gerichtsbarkeit im Einzelfall erheblich darunter.

V. Freitextfeld

Gemeinsame Dateien- Gesetz (ATD, „Projektdateien“; Übermittlungsreflexe,); INPOL- neu, das security data warehouse (objektrelationale Datenbanken, „Analysen“); SIS; Europol.