Big Data bei der Polizei

Sommerakademie 2014

Infobörse 5

Barbara Körffer

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Übersicht

1. Merkmale von Big Data
2. Einsatzmöglichkeiten für die Polizei
3. Grundsätze des Datenschutzes bei polizeilicher Datenverarbeitung
4. Zulässigkeit nach geltendem Recht
5. Herausforderung Big Data
6. Folgerungen de lege ferenda

Merkmale von Big Data

- Menge und Vielfalt von Daten
  - Strukturierte Datenbanken
  - Unstrukturierte Textdokumente
  - Bilder/Video/Audio etc.
- Vielfalt von Datenquellen
  - Polizeiliche Datenbanken/Vorgangsbearbeitungssysteme
  - Daten anderer Behörden und nicht öffentlicher Stellen
  - Allgemein zugängliche Daten, inbs. Soziale Netzwerke
- Verarbeitungsgeschwindigkeit
- Analysemöglichkeiten
  - Nach allen Merkmalen
  - Erkennung von Zusammenhängen und Mustern

Einsatzmöglichkeiten für die Polizei

- Strategische Analysen
- Operative Analysen
- Einschließlich Vorhersagen für künftige Entwicklungen („predictive policing“)

GRUNDSÄTZE DES DATENSCHUTZES

Grundsätze des Datenschutzes bei polizeilicher Datenverarbeitung

- Schutzrichtung des Datenschutzes bei polizeilicher Datenverarbeitung:
- Freiheit der Bürgerinnen und Bürger vor polizeilichen Maßnahmen sicherstellen
- Daher: Beschränkung polizeilicher Maßnahmen und polizeilicher Datenverarbeitung auf relevantes Verhalten

Weitere Grundsätze des Datenschutzes

- Verhältnismäßigkeit der Datenverarbeitung
  - Bestimmter Zweck
  - Geeignet für den Zweck
  - Erforderlichkeit für den Zweck
  - Angemessenheit des Eingriffs in Anbetracht des Zwecks
- Transparenz der Datenverarbeitung
  - Für den Betroffenen
  - Für die verantwortliche Stelle
  - Für externe Aufsicht und Kontrolle

GEWÄHRLEISTUNG DER FREIHEITSRECHTE DURCH GESETZ

Bei der Erhebung personenbezogener Daten

- Durch Beschränkung der Datenerhebung auf polizeilich relevantes Verhalten
  - Polizeirecht: Gefahr
  - Strafrecht: Anfangsverdacht für eine begangene Straftat
- Durchbrechungen dieses Grundsatzes
  - Datenerhebungen zur Verdachtsgewinnung
  - Ermittlungen im Vorfeld von Gefahren

Bei der weiteren Verarbeitung

- Sicherstellung durch Zweckbindung
- Zweckbindung gilt auch innerhalb polizeilicher Datenbanken und Systeme, d.h. auch dort Trennung nach unterschiedlichen Zwecken
- Genaue Festlegung von
  - Zwecken der weiteren Verarbeitung
  - Personenrollen und Datenkategorien
  - Austausch mit anderen Stellen
  - Aufbewahrungs- bzw. Prüffristen
- Durch Gesetze, Verordnungen (BKADV) und Errichtungsanordnungen

Bei der Nutzung personenbezogener Daten

- Ausgangslage:
  - Die für einen zuvor festgelegten Zweck gespeicherten Daten werden für diesen Zweck genutzt.
  - Grundsätzlich folgt aus der bestimmungsgemäßen Nutzung personenbezogener Daten keine besondere Gefährdung für Persönlichkeitsrechte, gleichwohl eigenständiger Grundrechtseingriff.
  - Allerdings abhängig von der Bestimmtheit der Zweckbeschreibung: Gefährdung steigt mit Unbestimmtheit der Verwendungszwecke, insbes. Vorbeugende Bekämpfung von Straftaten.
- Phase der Nutzung ist in den Datenschutzgesetzen wenig ausgeformt.

Durch technische und organisatorische Maßnahmen

- Gestaltung von Datenbanken
  - Unterscheidung nach Personenrollen (Beschuldigte, Geschädigte, Zeugen u.ä.)
  - Datenfelder
  - Recherchemöglichkeiten
  - Zugriffsrechte
  - Fristen für Prüfung/Löschung
- Verfahrensdokumentation
- Interne Kontrolle durch Datenschutzbeauftragte
- Externe Kontrolle
- Transparenz gegenüber Betroffenen

ZULÄSSIGKEIT VON BIG DATA AUSWERTUNGEN NACH GELTENDEM RECHT

Speicherung der Daten

- Eigenständige Datengrundlage für Big Data Auswertungen?
- Verbunden mit Zweckänderung; daher ist eigene Rechtsgrundlage für die Speicherung erforderlich.
  - § 8 BKAG, Polizeigesetze der Länder (§ 189 Abs. 1 Satz 4 LVwG SH), § 484 StPO: Speicherung polizeilicher Daten für die vorbeugende Bekämpfung von Straftaten

→ Nur Daten der Polizei/Staatsanwaltschaften dürfen gespeichert werden; keine Daten aus anderen Quellen.

→ Erforderlich ist eine besondere Relevanz für künftige Straftaten (Wiederholungsgefahr), diese muss vor der Speicherung geprüft werden.

→ Nur bestimmte Daten dürfen gespeichert werden, für Dateien des BKA in BKADV festgelegt.

Auswertung der Daten

- Auswertung/Nutzung ist ein eigenständiger Grundrechtseingriff; eigene Rechtsgrundlage erforderlich.
  - Vorschriften über den Datenabgleich
  - Vorschriften über die Rasterfahndung

Datenabgleich im Strafverfahren

§ 98c StPO

Zur Aufklärung einer Straftat oder zur Ermittlung des Aufenthaltsortes einer Person, nach der für Zwecke eines Strafverfahrens gefahndet wird, dürfen personenbezogene Daten aus einem Strafverfahren mit anderen zur Strafverfolgung oder Strafvollstreckung oder zur Gefahrenabwehr gespeicherten Daten maschinell abgeglichen werden. Entgegenstehende besondere bundesgesetzliche oder entsprechende landesgesetzliche Verwendungsregelungen bleiben unberührt.

Datenabgleich zur Gefahrenabwehr

§ 195 LVwG Schleswig-Holstein

(1) Die Polizei kann personenbezogene Daten der in den §§ 218, 219 sowie § 179 Abs. 2 Nr. 2 Buchst. a genannten Personen mit dem Inhalt polizeilicher Dateien im Rahmen der Zweckbindung dieser Dateien abgleichen. Personenbezogene Daten anderer Personen kann die Polizei abgleichen, wenn Tatsachen dafür sprechen, daß dies zur Erfüllung polizeilicher Aufgaben erforderlich erscheint. Die Polizei kann ferner im Rahmen ihrer Aufgabenerfüllung erlangte personenbezogene Daten mit dem Fahndungsbestand abgleichen. Ein Abgleich der nach § 179 Abs. 4 erlangten personenbezogenen Daten ist nur mit Zustimmung der betroffenen Person zulässig.

(2) Rechtsvorschriften über den Datenabgleich in anderen Fällen bleiben unberührt.

Voraussetzungen und Grenzen des Datenabgleichs

- Niedrige Eingriffsschwellen, da Gesetzgeber von geringfügigem Grundrechtseingriff ausging
- § 195 LVwG: 1:n-Abgleich – „Daten einer bestimmten Person mit einer Datei“
- § 98c StPO: Daten aus einem Strafverfahren mit anderen Daten, die zur Strafverfolgung oder Gefahrenabwehr gespeichert sind

Rasterfahndung im Strafverfahren

§ 98a StPO

(1) Liegen zureichende tatsächliche Anhaltspunkte dafür vor, daß eine Straftat von erheblicher Bedeutung [...] begangen worden ist, so dürfen [...] personenbezogene Daten von Personen, die bestimmte, auf den Täter vermutlich zutreffende Prüfungsmerkmale erfüllen, mit anderen Daten maschinell abgeglichen werden, um Nichtverdächtige auszuschließen oder Personen festzustellen, die weitere für die Ermittlungen bedeutsame Prüfungsmerkmale erfüllen. Die Maßnahme darf nur angeordnet werden, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre.

(2) Zu dem in Absatz 1 bezeichneten Zweck hat die speichernde Stelle die für den Abgleich erforderlichen Daten aus den Datenbeständen auszusondern und den Strafverfolgungsbehörden zu übermitteln.

(3) Soweit die zu übermittelnden Daten von anderen Daten nur mit unverhältnismäßigem Aufwand getrennt werden können, sind auf Anordnung auch die anderen Daten zu übermitteln. Ihre Nutzung ist nicht zulässig.

Rasterfahndung zur Gefahrenabwehr

- § 195a LVwG Schleswig-Holstein
- (1) Die Polizei kann von öffentlichen und nichtöffentlichen Stellen die Übermittlung von personenbezogenen Daten bestimmter Personengruppen aus Dateien zum Zwecke des automatisierten Abgleichs nach fahndungsspezifischen Suchkriterien mit anderen Datenbeständen verlangen, soweit dies erforderlich ist [...].
- (2) [...]
- (3) Das Übermittlungsersuchen ist auf Name, Anschrift, Tag und Ort der Geburt sowie andere für den Einzelfall benötigte Daten zu beschränken. Ist ein Aussondern der zu übermittelnden Daten nur mit unverhältnismäßigem Aufwand möglich, dürfen weitere, nicht vom Ermittlungsersuchen erfasste Daten ebenfalls übermittelt werden. Diese Daten dürfen von der Polizei nicht genutzt werden. [...]
- (4) Ist der Zweck der Maßnahme erreicht oder zeigt sich, daß er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten auf den Datenträgern zu löschen [...]

Wesensmerkmale der Rasterfahndung

- Schwerwiegender Grundrechtseingriff
  - Streubreite, Vielzahl von – auch anlasslos – Betroffenen
  - Unbegrenzt nach Umfang und Art der Daten, Verknüpfungsmöglichkeiten, Persönlichkeitsbilder möglich
  - Folgemaßnahmen, stigmatisierende Wirkung
- Festgelegtes Ziel
- Festgelegte Kriterien, nach denen gerastert wird
- strukturierte Datensätze, festgelegte Merkmale:
  - Merkmale für die Rasterung
  - Identifizierungsdaten der einbezogenen Personen

Auswertung der Daten - Ergebnis

- Auswertungen sind nach geltendem Recht nur in diesem Rahmen möglich.

- Big Data Auswertungen haben weit darüber hinausgehende Funktionalitäten

HERAUSFORDERUNG DURCH BIG DATA

Datenmenge

- Beliebig große Menge von Personen und von Daten kann verarbeitet werden.
  - Streubreite: Haben alle Personen, über die Daten verarbeitet werden, einen Anlass für die Verarbeitung gegeben?
  - Relevanz der Daten für den jeweiligen Zweck?

Vielfalt der Daten

- Auch unstrukturierte Daten einbezogen?
- Unstrukturierte Daten enthalten in der Regel mehr Informationen als erforderlich, z.B. Angaben über Zeugen, Geschädigte, Kontakt- und Begleitpersonen.
- Durch die Einbeziehung in die Auswertung können auch Informationen über nicht polizeilich relevantes Verhalten ausgewertet werden, die in einem anderen Zusammenhang eine neue Bedeutung und evtl. polizeiliche Relevanz gewinnen können.

Vielfalt der Quellen

- Zweckbindung: Durchbrechung der informationellen Gewaltenteilung.
- Zweckbindung: Daten sind bei anderen Stellen nicht für polizeiliche Zwecke gespeichert.
- Erforderlichkeit: Es können Informationen über Verhalten/Ereignisse etc. einbezogen werden, die selbst nicht polizeilich relevant sind.

Auswertemöglichkeiten

- Zweckbindung: Auswertung für neue, noch unbekannte Zwecke möglich.
- Erforderlichkeit: Big Data Auswertungen sind möglich ohne vorher festgelegte Auswertungsziele.
- Transparenz: Funktionsweise der Auswertungsalgorithmen bekannt? Ergebnisse nachvollziehbar?
- Richtigkeit, Verlässlichkeit: sowohl der Rohdaten als auch der Analyseergebnisse

Anwendung der Auswertungsergebnisse auf den Einzelfall-1

- Nicht personenbezogene Zuordnung des Ergebnisses (z.B. Gefährdungsanalyse für bestimmte Orte)
  - Trotz fehlendem Personenbezug gleichwohl oft Grundlage für spätere Grundrechtseingriffe, z.B. Grundlage für die Ausweisung von Gefahrengebieten oder gefährlichen Orten, an denen Personenkontrollen oder Identitätsfeststellungen vorgenommen werden können.
  - Daraus ergeben sich Anforderungen an die Zuverlässigkeit und Nachvollziehbarkeit der Ergebnisse

Anwendung der Auswertungsergebnisse auf den Einzelfall-2

- Personenbezogene Zuordnung des Ergebnisses
  - Keine automatisierte Einzelfallentscheidung
    - Erforderlich ist Entscheidung durch Polizeibeamte
    - Setzt eine Würdigung des Auswerteergebnisses und damit Nachvollziehbarkeit des Ergebnisses voraus.
  - Übertragung statistischer Erkenntnisse auf den Einzelfall und auf Einzelne:
    - Inwieweit können statistische Erfahrungswerte staatliche Eingriffsmaßnahmen gegen Personen begründen?
    - Problem bei Merkmalen nach Art. 3 Abs. 3 GG: Niemand darf wegen Geschlecht, Herkunft, Glauben etc. benachteiligt werden.

Anonymisierung oder Pseudonymisierung als Antwort auf die Herausforderungen?

- Ergebnis der Auswertung personenbezogen:
  - Nur geringfügiger „Gewinn“ für den Datenschutz
  - Risiko für den Einzelnen, in eine Auswertung einbezogen zu werden und auf Grund des Ergebnisses der Auswertung weiteren polizeilichen Maßnahmen unterzogen zu werden, bleibt in gleicher Weise bestehen wie bei von vornherein personenbezogener Auswertung
- Ergebnis der Auswertung nicht personenbezogen
  - Z.B. aggregierte statistische Daten
  - Als solche kein Eingriff in das Recht auf informationelle Selbstbestimmung

Auswirkungen auf die Transparenz für die Betroffenen

- Welche Daten bei welchen Stellen vorhanden?
- Welche Daten werden von welchen Stellen genutzt?
- Für welche Zwecke werden sie genutzt?
- Nach welchen Kriterien werden welche Informationen bewertet?
- Welche Folgen hat welches individuelle Verhalten?

FOLGERUNGEN DE LEGE FERENDA

Nutzung personenbezogener Daten

- Große Mengen von Daten sind für Jedermann verfügbar
- Rechnerkapazitäten und Programme zur Speicherung und Auswertung der Daten sind ebenfalls verfügbar
- Neben der Erhebung und Speicherung gewinnt die Nutzung personenbezogener Daten zunehmend an Bedeutung
- Präzisere Ausgestaltung dieser Phase der Datenverarbeitung durch den Gesetzgeber erforderlich

Regelungsbeispiel für komplexe Auswertungen

§ 7 RED-G Erweiterte Datennutzung

(1) Die beteiligten Behörden dürfen zur Erfüllung ihrer jeweiligen gesetzlichen Aufgaben die in der Datei nach § 3 gespeicherten Datenarten erweitert nutzen, soweit dies im Rahmen eines bestimmten Projekts zur Sammlung und Auswertung von Informationen über konkrete rechtsextremistische Bestrebungen, die darauf gerichtet sind, Gewalt anzuwenden oder Gewaltanwendung vorzubereiten, oder zur Verfolgung gewaltbezogener rechtsextremistischer Straftaten im Einzelfall erforderlich ist, um weitere Zusammenhänge aufzuklären. Satz 1 gilt entsprechend für Projekte zur Verhinderung gewaltbezogener rechtsextremistischer Straftaten, soweit Tatsachen die Annahme rechtfertigen, dass eine solche Straftat begangen werden soll. Projekte zur Verfolgung oder Verhinderung von Straftaten nach Satz 1 oder Satz 2 dürfen sich nur auf Straftaten nach den §§ 88 bis 89b, 91, 102, 105, 106, 108, 125a bis 129a, 211, 212, 224, 226, 227, 239a, 239b, 306 bis 306c, 308, 310 des Strafgesetzbuchs beziehen.

§ 7 RED-G

(2) Eine erweiterte Nutzung sind das Herstellen von Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen, der Ausschluss von unbedeutenden Informationen und Erkenntnissen, die Zuordnung eingehender Informationen zu bekannten Sachverhalten sowie die statistische Auswertung der gespeicherten Daten. Hierzu dürfen die beteiligten Behörden Daten auch mittels

- 1.phonetischer oder unvollständiger Daten,
- 2.der Suche über eine Mehrzahl von Datenfeldern,
- 3.der Verknüpfung von Personen, Institutionen, Organisationen, Sachen oder
- 4.der zeitlichen Eingrenzung der Suchkriterien

aus der Datei abfragen sowie räumliche und sonstige Beziehungen zwischen Personen und Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen darstellen sowie die Suchkriterien gewichten.

Bundesverfassungsgericht zur Antiterrordatei

Entscheidung d. BVerfG v. 24.4.2013, Rn. 194:

„Eine Grenze [d. Zugriffs auf die Daten] liegt insbesondere darin, dass § 5 ATDG lediglich Einzelabfragen, nicht aber auch eine Rasterung, Sammelabfragen oder die übergreifende Ermittlung von Zusammenhängen zwischen Personen durch Verknüpfung von Datenfeldern erlaubt. Die Vorschrift setzt damit einen konkreten Ermittlungsanlass voraus. Auch steht jede Abfrage unter der im Einzelfall sachhaltig zu prüfenden Voraussetzung der Erforderlichkeit.“

Grenzen einer gesetzlichen Regelung

- Grundsatz der Zweckbindung als Kernelement informationeller Selbstbestimmung kann nicht aufgegeben werden, daraus folgt:
  - Relevanzschwelle für die Einbeziehung von personenbezogenen Daten in Auswertungen
  - Keine beliebige Auswertung ohne Anlass und Zweckbestimmung
- Schutz der Betroffenen vor Anwendung statistischer Werte auf Einzelne als Grundlage für staatliche Eingriffe

Notwendige Garantien einer gesetzlichen Regelung

- Transparenz
  - Für Daten verarbeitende Stelle
  - Für Betroffene
  - Für Aufsicht und Kontrolle
- Kontrolle
  - Vorige Kontrolle, intern und extern, z.B. Richtervorbehalt
  - Nachträgliche Kontrolle, intern und extern (BVerfG zum ATDG)

Fragen?

Barbara Körffer
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein
uld5@datenschutzzentrum.de
0431 988-1216

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein