Datenverarbeitung zur Strafverfolgung und Gefahrenabwehr

Dr. Julia Victoria Pörschke
Unabhängiges Landeszentrum für Datenschutz

uld69@datenschutzzentrum.de

Gefahrenabwehr

- Gefahr
  - Sachverhalt, der bei ungehindertem Geschehensablauf in absehbarer Zeit mit hinreichender Wahrscheinlichkeit zu einem Schaden für die öffentliche Sicherheit führen könnte.
  - Schutzgut: Öffentliche Sicherheit
    - objektive Rechtsordnung
    - subjektive Rechte des einzelnen
    - Einrichtungen und Veranstaltungen des Staates
- Zuständige Behörden für die Gefahrenabwehr
  - Sonderordnungsbehörde (z.B. Umweltamt, Verkehrsbehörde)
  - Ordnungsbehörde (Ordnungsamt der Kommune)
  - Polizei
- Landesrecht (in Schleswig-Holstein: Landesverwaltungsgesetz - LVwG)

Strafverfolgung

- Aufklärung und Ahndung von Straftaten
- Bundesrecht (Strafprozessordnung - StPO)
- Voraussetzung: Anfangsverdacht für eine begangene Straftat

- Strafverfahren, verschiedene Stationen
  - Ermittlung der Tat (Ermittlungsverfahren)
  - Abschluss: Anklageerhebung oder Einstellung durch die StA
  - Gerichtsverfahren (Zwischen- und Hauptverfahren)
  - Abschluss: Urteil oder Einstellung
  - Vollstreckung (Freiheits- oder Geldstrafe)

- Zuständige Behörden im Ermittlungsverfahren
  - Staatsanwaltschaft als „Herrin des Ermittlungsverfahrens"
  - Polizei (entweder eigenständig oder im Auftrag der Staatsanwaltschaft - Ermittlungsbeamte)

Aufgaben und Befugnisse der Behörden

- 1. Schritt: Informationsgewinnung
  - Aufklärung der Gefahrensituation / Ermittlung von eventuellen Störern oder Personen, die die Gefahr abwehren können
  - Aufklärung der Straftat / Ermittlung des Täters

- 2. Schritt: bei Gefahrenabwehr
  - Ergreifen von Maßnahmen zur Abwehr der festgestellten Gefahr
  - z.B. Platzverweis, Sicherstellung von Sachen, Gewahrsam von Personen

- 2. Schritt: bei Strafverfolgung
  - Anklageerhebung oder Einstellung des Verfahrens
  - durch Gericht kann Strafe verhängt werden

Informationsquellen (1)

- Der Betroffene
  - bei Gefahrenabwehr: Störer
  - im Strafverfahren: Beschuldigter/Angeklagter
  - Maßnahmen: z.B. Befragung, erkennungsdienstliche Behandlung, Blutuntersuchung, DNA-Analyse
- Allgemein zugängliche Quellen
  - z.B. öffentliche Verzeichnisse (Telefonbuch)
  - Presse, Fernsehen, allgemein zugängliche Veröffentlichungen im Internet
  - frei zugängliche Register, z.B. Handelsregister
  - Soziale Netzwerke?
- Andere Polizeibehörden und Informationssysteme der Polizei
  - INPOL (u.a. mit Kriminalaktenhinweis, AFIS, Fahndungsdateien), Datenbanken der Landespolizei
  - Auf europäischer Ebene: Schengener Informationssystem, Eurodac, Europol, Prümer Beschluss
  - International: Interpol

Informationsquellen (2)

- von anderen Behörden geführte Register, z.B.
  - Melderegister
  - Bundeszentralregister
  - Gewerbezentralregister
  - Ausländerzentralregister
  - Verkehrszentralregister
  - Fahrzeugregister
  - Fahrerlaubnisregister
  - Zentrales staatsanwaltschaftliches Verfahrensregister (nur für Staatsanwaltschaften)

Informationsquellen (3)

- Andere Behörden, z.B.
  - Ausländerbehörde
  - Verkehrsbehörde
- Zeugen, z.B.
  - Dritte
  - Angehörige
  - Nachbarn, Freunde
  - P: Ärzte, Rechtsanwälte, Steuerberater, Geistliche
  - Arbeitgeber
- Unternehmen, z.B.
  - Banken
  - Telekommunikationsdiensteanbieter
  - Versicherungen

Informationsquellen (4)

- sonstige (offene) Maßnahmen, z.B.
  - Einsatz von Videoüberwachung auf öffentlichen Plätzen
  - Identitätsfeststellung von Personen im öffentlichen Raum
  - Kontrolle von Fahrzeugen im öffentlichen Verkehr
  - Kfz-Kennzeichenscanning (gibt es in Schleswig-Holstein nicht mehr)

Informationsquellen (5)

- Heimliche Ermittlungen: Verdeckte Ermittlungsmaßnahmen, z.B.
  - Telekommunikationsüberwachung
  - Wohnraumüberwachung
  - Observation mit technischen Mitteln
  - Einsatz von sog. IMSI-Catchern zur Ermittlung des Standorts von Mobilfunkgeräten
  - Einsatz verdeckter Ermittler
  - Online-Durchsuchung (nur für einzelne Behörden zulässig, z.B. BKA)

Rechtliche Voraussetzungen und Grenzen (1) Grundrechte

- Sämtliche Maßnahmen der Informationsgewinnung über Personen oder Sachverhalte, die mit einer Person verknüpft werden können, sind Grundrechtseingriffe
- Betroffene Grundrechte
  - Recht auf informationelle Selbstbestimmung (Art. 2, 1 GG)
  - Brief-, Post- und Fernmeldegeheimnis (Art. 10 GG)
  - Unverletzlichkeit der Wohnung (Art. 13 GG)
  - Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2, 1 GG)

Rechtliche Voraussetzungen und Grenzen (2) Funktionen der Grundrechte

- Grundrecht als Abwehrrecht gegenüber dem Staat
  - Grundrechte dienen in erster Linie dem Schutz der Bürger vor staatlichen Eingriffen
  - Staatliche Eingriffe dürfen nur innerhalb der Grundrechtsschranken vorgenommen werden
- Mittelbare Drittwirkung von Grundrechten zwischen Privaten
  - Grundrechte gelten unmittelbar nur zwischen Bürger und Staat, d.h. keine unmittelbare Geltung zwischen Privaten (also z.B. zwischen Verbraucher und Unternehmen)
  - Die Wertungen der Grundrechte fließen aber auch in das Privatrecht ein, so z.B. im Datenschutzrecht für den nichtöffentlichen Bereich
  - Die entsprechenden Regelungen sind daher so anzuwenden und auszulegen, dass die Wertungen der Grundrechte zum Tragen kommen, insofern kann man von einer mittelbaren Wirkung der Grundrechte im Privatrecht sprechen.

Rechtliche Voraussetzungen und Grenzen (3) Wann ist Eingriff in Grundrechte zulässig?

- Grundrechtsschranken
  - z.B. beim Recht auf informationelle Selbstbestimmung: Eingriff nur, soweit ein Gesetz diesen erlaubt. Das Gesetz muss hinreichend klar und bestimmt sein.
- Verhältnismäßigkeit **(„G-E-Z")**
  - Zweck des Eingriffs - dient der Eingriff einem legitimen Zweck?
  - **G**eeignetheit des Eingriffs - ist der Eingriff überhaupt geeignet, um den angestrebten Zweck zu erzielen?
  - **E**rforderlichkeit des Eingriffs - gibt es ein milderes, gleich geeignetes, Mittel?
  - **Z**umutbarkeit/Angemessenheit des Eingriffs - wie schwerwiegend ist der Eingriff? Wie gewichtig sind die mit dem Eingriff verfolgten Zwecke? Ist der beabsichtigte Eingriff für den angestrebten Zweck angemessen?

Rechtliche Voraussetzungen und Grenzen (4) Kriterien der Verhältnismäßigkeitsprüfung

- Legitimer Zweck
  - Strafverfolgung und Gefahrenabwehr sind Schutzaufgaben des Staates, stets legitime Zwecke
- Zumutbarkeit/Angemessenheit
  - für schweren Grundrechtseingriff sprechen z.B.
    - Heimlichkeit der Maßnahme für den Betroffenen
    - Intensität des Eindringens in die Privatsphäre, z.B. ist Wohnung stärker geschützt als Handlungen im öffentlichen Raum
    - Art der Daten, z.B. sensitive Daten
    - Streubreite von Maßnahmen (viele Betroffene, darunter vor allem „Unschuldige")
  - gewichtige Zwecke sind z.B.
    - Schutz gewichtiger Rechtsgüter: Leib, Leben, Freiheit
    - Verfolgung schwerer Straftaten (Katalogstraftaten des § 100a StPO)

Rechtliche Voraussetzungen und Grenzen (5) Grundlagen für die Informationsermittlung

- Ermittlung von personenbezogenen Informationen
  - für die ermittelnde Stelle: Erhebung
  - für die befragte Stelle: Übermittlung

- Eingriff in Grundrechte, erfordert
  - Gesetzliche Grundlage oder
  - Einwilligung

Rechtliche Voraussetzungen und Grenzen (6) Problem der Einwilligung

- Einwilligung muss vor allem eines sein: Eine freiwillige Entscheidung des Betroffenen
- D.h.: Dem Betroffenen muss eingeräumt werden, die Einwilligung nicht zu erteilen
- Was machen in diesem Fall die Sicherheitsbehörden?
  - Verzicht auf die Datenerhebung oder weitere Verarbeitung möglich, ohne dass Aufgabenerfüllung gefährdet wird?
    - falls nein, kann die Datenverarbeitung nicht zur Disposition des Betroffenen gestellt werden
    - falls ja, stellt sich die Frage, ob die Datenverarbeitung tatsächlich erforderlich ist (kann nur im Einzelfall beurteilt werden)

Rechtliche Voraussetzungen und Grenzen (7) Gesetzliche Grundlagen

- Allgemeine Befugnisnormen (so genannte Generalklauseln)
  - Gefahrenabwehr: § 179 LVwG
  - Strafverfolgung: §§ 161, 163 StPO
- Spezielle Befugnisnormen (für bestimmte Eingriffe)
  - Gefahrenabwehr: z.B. §§ 183, 185, 185a LVwG
  - Strafverfolgung: z.B. §§ 98a, 100a, 100c, 100g StPO
- Verhältnis allgemeiner zu speziellen Befugnissen
  - Die allgemeinen Befugnisnormen ermöglichen nur Eingriffe von geringer Intensität
  - Eingriffe mit höherer Intensität (Kriterien s. Folie 13) dürfen nur vorgenommen werden, wenn es hierfür eine spezielle Befugnis gibt und deren Voraussetzungen erfüllt sind
  - Beispiel: Die heimliche Überwachung von Telefongesprächen darf nur vorgenommen werden, wenn eine spezielle Regelung genau dies erlaubt. Gibt es eine solche Regelung nicht oder sind die Voraussetzungen einer bestehenden Regelung im Einzelfall nicht erfüllt, darf die Maßnahme nicht auf die Generalklausel gestützt werden.

Rechtliche Voraussetzungen und Grenzen (8) Gesetzliche Grundlagen

- Erhebung beim Betroffenen
  - Gefahrenabwehr: § 178, 179 LVwG - Grundsatz der offenen Erhebung direkt beim Betroffenen
  - Strafverfolgung: §§ 161, 163 StPO

- Es gilt der Grundsatz, dass sich niemand wegen einer Straftat selbst belasten muss. Daraus folgt das Recht zur Verweigerung der Aussage im Strafverfahren (§§ 136, 163a StPO). Der Grundsatz gilt allgemein, d.h. Aussageverweigerungsrecht immer dann, wenn der Betroffene sich dadurch einer Straftat verdächtig machen würde.

Rechtliche Voraussetzungen und Grenzen (9) Gesetzliche Grundlagen

- Polizeiliche Informationssysteme / Erhebung bei anderen Polizeibehörden
  - §§ 7, 8 Bundeskriminalamtgesetz (BKAG)
  - § 192 LVwG
- Andere Register
  - Melderegister: § 24 Landesmeldegesetz
  - Bundeszentralregister: § 30 Bundeszentralregistergesetz
  - Verkehrszentralregister: § 30 Straßenverkehrsgesetz
  - Fahrzeugregister: § 35 Straßenverkehrsgesetz
  - Fahrerlaubnisregister: § 52 Straßenverkehrsgesetz
  - Ausländerzentralregister: § 10 Ausländerzentralregistergesetz
  - Gewerbezentralregister: § 150a Gewerbeordnung
  - Zentrales staatsanwaltschaftliches Verfahrensregister: § 492 StPO

Rechtliche Voraussetzungen und Grenzen (10) Gesetzliche Grundlagen

- Behörden (allgemeine Befugnisnormen)
  - Gefahrenabwehr: § 179 LVwG
  - Strafverfolgung: § 161, 163 StPO
    - Unterschied zwischen Polizei und Staatsanwaltschaft:
      - Gegenüber der Staatsanwaltschaft besteht für Behörden grundsätzlich Auskunftspflicht
      - Gegenüber der Polizei besteht für Behörden in der Regel keine Auskunftspflicht, es sei denn die Polizei ist von der Staatsanwaltschaft mit den Ermittlungen beauftragt oder es besteht Gefahr im Verzug.
  - gelten nicht, wenn besondere Geheimhaltungsvorschriften entgegenstehen, z.B. das Steuergeheimnis oder das Sozialgeheimnis. Hierfür gibt es wiederum besondere Regelungen in der Abgabenordnung (§ 30 Abgabenordnung) und im Sozialrecht (z.B. § 68 Sozialgesetzbuch X)

Rechtliche Voraussetzungen und Grenzen (11) Gesetzliche Grundlagen

- Unternehmen
  - Gefahrenabwehr: § 179 LVwG
  - Strafverfolgung: §§ 160, 161, 161a, 163 StPO
  - Unternehmen werden als Zeugen vernommen
  - Auf Ladung der Staatsanwaltschaft sind Zeugen verpflichtet, zur Sache auszusagen (§ 161a StPO), gegenüber der Polizei ist die Auskunft dagegen freiwillig.
  - Korrespondierende Übermittlungsbefugnis für die Unternehmen:

    § 28 Abs. 2 Nr. 2b BDSG
    - Daten für Gefahrenabwehr oder Strafverfolgung erforderlich
    - kein Überwiegen schutzwürdiger Interessen des Betroffenen
    - nur Übermittlungsbefugnis, keine Pflicht
    - Pflicht kann entstehen, durch Maßnahmen der Staatsanwaltschaft /des Gerichts (Vorladung nach § 161a StPO oder Beschlagnahme von Unterlagen, § 95, 98 StPO)

Rechtliche Voraussetzungen und Grenzen (12) Gesetzliche Grundlagen

- Unternehmen
  - Sonderregelungen für Post und Telekommunikation
    - § 100j StPO für die Herausgabe von Bestandsdaten und Internet-protokoll-Adressen
    - § 99 StPO für die Postbeschlagnahme
    - § 100g StPO für die Herausgabe von Verkehrsdaten der Telekommunikation
  - Zeugnisverweigerungsrecht nach § 53 StPO für Berufsgeheimnisträger
    - Ärzte, Zahnärzte, Geistliche, Rechtsanwälte, Steuerberater, Journalisten etc.
    - korrespondierend dazu Strafvorschrift in § 203 Strafgesetzbuch für die unbefugte Offenbarung von Berufsgeheimnissen (auch gegenüber Sicherheitsbehörden)

Rechtliche Voraussetzungen und Grenzen (13)
Gesetzliche Grundlagen

- Andere Dritte (soziales Umfeld)
  - Gefahrenabwehr: § 179 LVwG
  - Strafverfolgung: § 161, 161a, 163 StPO
  - werden als Zeugen vernommen
  - Zeugnisverweigerungsrecht für Angehörige (§ 52 StPO)

Rechtliche Voraussetzungen und Grenzen (14) Gesetzliche Grundlagen

- Verdeckte Ermittlungsmaßnahmen, z.B.
  - Gefahrenabwehr
    - Observation: § 185 LVwG
    - Telekommunikationsüberwachung: § 185a LVwG
    - Online-Durchsuchung: § 20k Bundeskriminalamtgesetz (Befugnis gilt nur für das BKA, soweit es zur Abwehr terroristischer Gefahren tätig wird)
  - Strafverfolgung
    - Telekommunikationsüberwachung: § 100a StPO
    - Wohnraumüberwachung: § 100c StPO
    - Observation: § 100h StPO
    - Einsatz von IMSI-Catchern zur Ermittlung z.B. des Standorts eines Mobilfunkgeräts: § 100i StPO
    - Einsatz verdeckter Ermittler: § 110a StPO

Rechtliche Voraussetzungen und Grenzen (15) Gesetzliche Grundlagen

- Wichtig bei verdeckten Ermittlungsmaßnahmen
  - hohe Eingriffsschwellen, da stets schwerwiegender Grundrechtseingriff
    - z.B. mit sehr hoher Wahrscheinlichkeit unmittelbar bevorstehende Gefahr für ein gewichtiges Rechtsgut (Leib, Leben, Freiheit)
    - Aufgrund von Tatsachen erhärteter Verdacht des Vorliegens einer Straftat von erheblicher Bedeutung (siehe z.B. die in § 100a StPO aufgeführten Straftaten)
    - Formell: In der Regel Anordnung durch das Gericht erforderlich
  - absoluter Schutz des Kernbereichs privater Lebensgestaltung: Daten aus diesem Bereich (höchstpersönlicher Bereich) dürfen nicht erhoben werden. Falls sie versehentlich erhoben werden, müssen sie sofort gelöscht werden.
  - Nach Beendigung der verdeckten Maßnahme muss der Betroffene hiervon benachrichtigt werden (siehe im Einzelnen § 101 StPO).

Beispiele der „Zusammenarbeit" von Sicherheitsbehörden und Unternehmen

Passenger Name Records (Fluggastdaten)

- Abkommen zwischen EU und USA verpflichtet Luftfahrtunternehmen, Fluggastdaten an die USA (Department of Homeland Security) zu übermitteln. Insgesamt werden die Daten aus 19 Datenfeldern der Buchung übermittelt.
- Fluggastdaten werden in USA insgesamt 15 Jahre gespeichert und ausgewertet
- In der EU werden Überlegungen zur Einrichtung eines eigenen europaweiten PNR-Systems diskutiert.
- PNR-Daten für USA mittlerweile ergänzt durch ESTA: elektronisches Registriersystem für Flugreisende in die USA

Beispiele der „Zusammenarbeit" von Sicherheitsbehörden und Unternehmen

Finanztransaktionsdaten (SWIFT)

- US-Finanzministerium betreibt Terrorist Finance Tracking Programme (TFTP), eine Datenbank zum Aufspüren von Terrorismusfinanzierungen

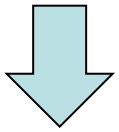
- Dafür wurden seit 2001 regelmäßig die Daten des europäischen Finanzdienstleisters SWIFT genutzt, der ein Spiegelrechenzentrum in den USA betrieb. 2009 Verlegung des Spiegelrechenzentrums in die Schweiz. Kein unmittelbarer Zugriff der US-Behörden mehr auf die SWIFT-Daten.

- Abkommen zwischen EU und USA zur Übermittlung von Finanz-transaktionsdaten seit Sommer 2010

Was ist nach der Datenerhebung zu beachten?

Schritte der Informationsverarbeitung sind:

1. Datenerhebung



2. Datenspeicherung, -veränderung und –nutzung

Datenverarbeitungsschritte – Datenspeicherung

- Gefahrenabwehr: § 188 LVwG

  „P.D. können gespeichert, verändert und genutzt werden, soweit dies zur Erfüllung der jeweiligen ordnungsbehördlichen oder polizeilichen Aufgabe oder hiermit im Zusammenhang stehender Aufgaben erforderlich ist. Die Speicherung, Veränderung oder Nutzung darf nur zu dem Zweck erfolgen, zu dem die personenbezogenen Daten erlangt worden sind."

- Strafverfolgung: §§ 481, 483 StPO

  „soweit für Zwecke des Strafverfahrens erforderlich"

  Daten aus Strafermittlungsverfahren können grds. auch zur Gefahrenabwehr genutzt werden

Datenverarbeitungsschritte – Datenveränderung und Datennutzung

- Verändern
  = inhaltliche Umgestaltung gespeicherter Daten
  - erfordert eine gesonderte Rechtsgrundlage

- Nutzen
  = Verwendung von personenbezogenen Daten
  - stellt selbst keine Datenerhebung dar

Was ist nach der Datenerhebung zu beachten?

Schritte der Informationsverarbeitung sind:

1. Datenerhebung

2. Datenspeicherung, -veränderung und –nutzung

3. Datenberichtigung und Datenlöschung

Datenverarbeitungsschritte – Datenberichtigung und Datenlöschung I

Strafverfolgung: § 489 StPO

Gefahrenabwehr: § 196 LVwG

- Berichtigungspflicht, wenn die Daten unrichtig sind
- zudem Dokumentationspflichten in welchem Zeitraum und aus welchem Grund die Daten unrichtig waren
- Pflicht zur Löschung nach Ablauf bestimmter Prüffristen oder wenn die Daten nicht mehr für die Aufgabenerfüllung der speichernden Stelle erforderlich sind

Datenverarbeitungsschritte – Datenberichtigung und Datenlöschung II

Prüffristen i.R. der Strafverfolgung

Erwachsene → 10 Jahre

Jugendliche → 5 Jahre

Kinder → 2 Jahre

bei rechtskräftigem Freispruch → 3 Jahre

Prüffristen i.R. der Gefahrenabwehr

Erwachsene → 5-10 Jahre

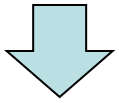
Erwachsene (über 70) und Jugendliche → 5 Jahre

Kinder → 2 Jahre

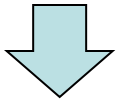
Was ist nach der Datenerhebung zu beachten?

Schritte der Informationsverarbeitung sind:

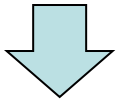
1. Datenerhebung



2. Datenspeicherung, -veränderung und –nutzung



3. Datenberichtigung und Datenlöschung



4. Betroffenenrechte

Betroffenenrechte I

- Gefahrenabwehr: Belehrungs- und Informationspflicht bei Erhebung, § 178 III LVwG
  - besteht Auskunftspflicht oder Angabe freiwillig?
  - Erhebungszweck
- Strafverfolgung: Informationspflicht bei Einstellung, § 170 II 2 StPO
- Benachrichtigungspflichten bei besonderen Mitteln zur Datenerhebung, z. B. bei verdeckten Maßnahmen

Betroffenenrechte II

- Auskunftsanspruch des Betroffenen
  - Strafverfahren: §§ 491 I, 495 I StPO
  - Gefahrenabwehr: § 198 LVwG

  über
  den zu ihm gespeicherten Daten,
  den Zweck und die Rechtsgrundlage der Speicherung,
  die Herkunft der personenbezogenen Daten,
  die Empfänger von Übermittlungen

Betroffenenrechte III

- Die Auskunftserteilung oder die Gewährung von Akteneinsicht entfällt, soweit eine Prüfung ergibt, dass
  - dadurch die Erfüllung ordnungsbehördlicher oder polizeilicher Aufgaben erheblich erschwert oder gefährdet werden würde,
  - die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder wegen der berechtigten Interessen einer dritten Person geheim gehalten werden müssen oder
  - durch die Auskunftserteilung oder die Gewährung von Akteneinsicht dem Wohl des Bundes oder eines Landes Nachteile entstehen würden.

Links

- Landesverwaltungsgesetz
  http://www.gesetze-rechtsprechung.sh.juris.de/jportal/portal/t/lpp/page/bsshoprod.psml?doc.hl=1&doc.id=jlr-VwGSHrahmen%3Ajuris-lr00&documentnumber=1&numberofresults=459&showdoccase=1&doc.part=R&paramfromHL=true#focuspoint
- Strafprozessordnung
  http://www.gesetze-im-internet.de/stpo/index.html
- andere Landesgesetze (z.B. Landesmeldegesetz):
  www.gesetze-rechtsprechung.sh.juris.de
- andere Bundesgesetze:
  www.gesetze-im-internet.de