Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 4. Übung im SoSe 2007:
Datenschutz bei Sicherheitsbehörden

4.1 Vergleich zur Daten- erhebung: LDSG vs. PolG (1)

- **Erforderlichkeitsprinzip** (§ 13 Abs. 1 LDSG)
- **Direkterhebung**, sofern Daten nicht allgemein zugänglich (§ 13 Abs. 2 LDSG)
- bei Betroffenheit eines Mehrpersonenkreises müssen diese **Kenntnis** darüber erlangen können (§ 13 Abs. 2 LDSG)
- Kenntnissetzung bei gesetzlicher Regelung entbehrlich (§ 13 Abs. 3 LDSG)
- **Direkterhebung**, sofern Daten nicht allgemein zugänglich (§ 19 Abs. 1 PolG)
- keine Kenntnissetzung, wenn dies die **Wahrnehmung polizeilicher Aufgaben** gefährden würde (§ 19 Abs. 1 PolG)
- Grundsatz der **offenen Erhebung** personenbezogener Daten (§ 19 Abs. 2 PolG)
- **verdeckte Datenerhebung** zulässig, wenn sonst die Wahrnehmung polizeilicher Aufgaben gefährdet oder nur mit unverhältnismäßig hohem Aufwand möglich wäre (§ 19 Abs. 2 PolG)

4.1 Vergleich zur Datenerhebung: LDSG vs. PolG (2)

- Direkterhebung insbesondere entbehrlich, wenn **andere Rechtsvorschrift** dies vorsieht (§ 13 Abs. 4 Nr. 1 LDSG i.V.m. § 15 Abs. 2 Nr. 1 LDSG), dies erforderlich ist zur **Abwehr erheblicher Nachteile für das Gemeinwohl**, einer sonst **unmittelbar drohenden Gefahr für die öffentliche Sicherheit** oder einer **schwerwiegenden Beeinträchtigung der Rechte** einer **anderen Person** (§ 13 Abs. 4 Nr. 1 LDSG i.V.m. § 15 Abs. 2 Nr. 5 LDSG) oder wenn dies erforderlich ist zur **Verfolgung von Straftaten oder Ordnungswidrigkeiten** (§ 13 Abs. 4 Nr. 1 LDSG i.V.m. § 15 Abs. 2 Nr. 8 LDSG)
- Betroffener ist auf Verlangen auf die **Rechtsgrundlage** seiner Auskunftspflicht bzw. der Freiwilligkeit der Auskunft hinzuweisen (§ 19 Abs. 3 PolG)
- keine Angabe der Rechtsgrundlage gegenüber **Dritten**, wenn erkennbar schutzwürdige Interessen beeinträchtigt werden können (§ 19 Abs. 3 PolG)
- Polizei darf jeden befragen, von dem angenommen werden kann, dass er erforderliche, sachdienliche Angaben zur **Wahrnehmung polizeilicher Aufgaben** liefern kann (§ 20 Abs. 1 PolG)

4.1 Vergleich zur Datenerhebung: LDSG vs. PolG (3)

- Befragte Personen **verpflichtet** zur **Angabe** von Name, Vorname, Tag & Ort der Geburt, Wohnanschrift und Staatsangehörigkeit (§ 20 Abs. 1 PolG)
- zur **vorbeugenden Bekämpfung von Straftaten** darf der Polizeivollzugsdienst Daten erheben zu Personen, bei denen tatsächliche Anhaltspunkte vorliegen, dass diese künftig Straftaten begehen oder Opfer von Straftaten werden, sowie zu Zeugen, Hinweisgeber oder sonstige Auskunftspersonen (§ 20 Abs. 2 PolG)

4.1 Vergleich zur Datenerhebung: LDSG vs. PolG (4)

- bei öffentlichen Veranstaltungen bzw. Ansammlungen (wider Versammlungsgesetz) darf der Polizeivollzugsdienst **Bild- und Tonaufzeichnungen** anfertigen, sofern Tatsachen die Annahme rechtfertigen, dass dabei Ordnungswidrigkeiten mit erheblicher Bedeutung bzw. Straftaten begangen werden (§ 21 Abs. 1 PolG)
- bei öffentlich zugänglichen Orten dürfen **Bildaufzeichnungen** angefertigt werden zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Beseitigung von Störungen der öffentlichen Sicherheit (§ 21 Abs. 3 PolG)

4.1 Vergleich zur Datenerhebung: LDSG vs. PolG (5)

- zur Abwehr einer erheblichen Gefahr auch der **verdeckte Einsatz technischer Mittel** zur Anfertigung von Lichtbildern und Bildaufzeichnungen zulässig bzw. wenn andernfalls Wahrnehmung des Polizeivollzugsdienstes gefährdet oder erheblich erschwert würde (§ 22 Abs. 2 PolG)
- zusätzlich **Einsatz verdeckter Ermittler** und **Aufzeichnung nicht-öffentlich gesprochener Worte** zur Abwehr einer Gefahr für den Bestand des Bundes oder des Landes oder für Leben, Gesundheit oder Freiheit einer Person oder für bedeutende Sach- und Vermögenswerte (§ 22 Abs. 3 PolG)

4.2 Vergleich zur Rasterfahndung: StPO vs. PolG (1)

StPO:

- Maschineller Datenabgleich zulässig bei **Straftaten von erheblicher Bedeutung**, wenn andere Ermittlungsmethoden erheblich weniger erfolgversprechend oder wesentlich erschwert wären (§ 98a Abs. 1 StPO)
- Die Aussonderung der erforderlichen Datenbestände erfolgt durch die speichernde Stelle (§ 98a Abs. 2 StPO)

PolG:

- Maschineller Datenabgleich zur vorbeugenden Bekämpfung von **Straftaten mit erheblicher Bedeutung** zulässig (§ 40 Abs. 1 PolG)
- Zu übermittelnde personenbezogene Daten sind Name, Anschrift, Tag und Ort der Geburt, sowie für den **Einzelfall** festzulegende Merkmale (§ 40 Abs. 2 PolG)

4.2 Vergleich zur Rasterfahndung: StPO vs. PolG (2)

StPO:

- Keine Aussonderung durch speichernde Stelle nötig, wenn dies nur mit unverhältnismäßigem Aufwand möglich wäre (§ 98a Abs. 3 StPO)
- Abgleich und Übermittlung der Daten nur durch **richterliche Anordnung**; bei Gefahr im Verzuge durch die Staatsanwaltschaft (§ 98b Abs. 1 StPO)
- Beschränkung auf Daten und Prüfungsmerkmale, die für den **Einzelfall** benötigt werden (§ 98b Abs. 1 StPO)

PolG:

- Keine Aussonderung nötig, wenn dies nur mit unverhältnismäßigem Aufwand möglich wäre (§ 40 Abs. 2 PolG)
- Abgleich und Übermittlung der Daten „nur“ durch **Anordnung** der Leitung von LKA, Wasserschutzpolizeidirektion, Landespolizeidirektion, Polizeipräsidium, Polizeidirektion oder eines Abschnitts **mit Zustimmung des Innenministeriums** (§ 40 Abs. 3 PolG)

4.2 Vergleich zur Rasterfahndung: StPO vs. PolG (3)

StPO:

- Übergebene Datenträger sind nach Beendigung des Abgleichs unverzüglich zurückzugeben (§ 98b Abs. 3 StPO)
- Auf andere Datenträger übertragene personenbezogene Daten sind unverzüglich zu löschen, sobald sie für das Strafverfahren nicht mehr benötigt werden (§ 98b Abs. 3 StPO)
- Bindung an Beweiszweck für Straftaten mit erheblicher Bedeutung (§ 98b Abs. 3 StPO)

PolG:

- LfD ist von der Anordnung der Maßnahme unverzüglich zu unterrichten (§ 40 Abs. 3 PolG)
- Nach Abschluss der Rasterfahndung bzw. nach Feststellung der Zweckunerreichbarkeit sind die übermittelten und zusätzlich angefallenen Daten zu löschen, soweit sie nicht zur Verfolgung von Straftaten [ohne Abgrenzung!] benötigt werden (§ 40 Abs. 4 PolG)

4.2 Vergleich zur Rasterfahndung: StPO vs. PolG (4)

StPO:

- Der zuständige Datenschutzbeauftragte wird nach Beendigung der Rasterfahndung informiert (§ 98b Abs. 4 StPO)
- Abgleich von Datensätzen aus verschiedenen Strafverfahren von erheblicher Bedeutung im Rahmen einer (weiteren!) Rasterfahndung zulässig (§ 98c StPO i.V.m. § 98b Abs. 3 StPO)
- Spezialrechtliche Verwendungsregelungen bleiben bestehen (§ 98b Abs. 1 StPO und § 98c StPO)

4.3 Überprüfung der Rasterfahndung nach § 40 PolG (1)

Überprüfung der Normenklarheit:

- **Regelungen** ausreichend **bereichsspezifisch** getroffen
- **verwendungsbezogene Zweckfestlegung** durch Verbindung der Anordnung auf Straftaten von erheblicher Bedeutung (Katalog aus § 22 Abs. 5 PolG) gegeben
- Gewährleistung der **informationellen Gewaltenteilung** insoweit erreicht, da Daten aus der Rasterfahndung nicht für straftatenunabhängige Belange verwendet werden dürfen, aber die Angabe der Anordnungsbefugten ist möglicherweise zu weit gefasst – Korrektiv nur durch Zustimmung des Innenministeriums gegeben

4.3 Überprüfung der Rasterfahndung nach § 40 PolG (2)

Fortsetzung zur Überprüfung der Normenklarheit:

- Die Regelungen zu den zu übermittelnden und abzugleichenden Daten sind dagegen klar **bestimmt**
  - **Transparenzgebot** erreicht, da LfD unverzüglich informiert wird und sich der Betroffene (unter Berücksichtigung von § 27 Abs. 2 LDSG) an den LfD wenden kann
- **Ergebnis:** Anforderungen an Normenklarheit weitgehend erfüllt!

4.3 Überprüfung der Rasterfahndung nach § 40 PolG (3)

Überprüfung der Verhältnismäßigkeit:

- **Eignung** der Rasterfahndung hängt maßgeblich von dem zugrunde liegenden Wirklichkeitsmodell und damit von dem konkreten Einzelfall ab; das Abstellen auf den Einzelfall bei den merkmalsbezogenen Daten (§ 40 Abs. 2 PolG) ist daher konsequent – eine Aussage über Prüfungsergebnis damit hierzu nicht möglich
- Rasterfahndung führte bisher in keinem Fall zu den gewünschten Ermittlungsergebnissen, so dass sogar die Eignung in Frage gestellt werden kann; allerdings kann Eignung auch nicht pauschal ausgeschlossen werden
- **Erforderlichkeitsprüfung** dem Innenministerium überantwortet, da nur mit dessen Zustimmung die Rasterfahndung durchgeführt werden darf

4.3 Überprüfung der Rasterfahndung nach § 40 PolG (4)

Fortsetzung zur Überprüfung der Verhältnismäßigkeit:

- **Zweckbindung** aufgrund von der fehlenden Beschränkung in § 40 Abs. 4 PolG auf die für die Anordnung grundlegenden Straftaten von erheblicher Bedeutung (Katalog aus § 22 Abs. 5 PolG) fraglich
- Ob **geringerer Eingriff** in das informationelle Selbstbestimmungsrecht möglich ist, hängt vom Einzelfall ab und lässt sich damit nicht allgemein beantworten
- Bindung der Rasterfahndung an Straftaten mit erheblicher Bedeutung erfolgt im überwiegenden Allgemeininteresse

4.3 Überprüfung der Rasterfahndung nach § 40 PolG (5)

2. Fortsetzung zur Überprüfung der Verhältnismäßigkeit:

- Gewährleistung des **Übermaßverbots** dennoch fraglich, da vorbeugende (!) Bekämpfung von Straftaten mit erheblicher Bedeutung nicht an das Vorliegen einer konkreten und gegenwärtigen Gefahr gebunden ist [siehe auch Beschluss des BVerfG vom 04.04.2006 zur Rasterfahndung] – bei StPO-Verfahren liegt dagegen bereits eine verübte Straftat vor
  - insofern mangelt es auch an der Bestimmtheit (Normenklarheit!)
  - Lösungsgebot und Beachtung der technischen und organisatorischen Maßnahmen nach § 9 LDSG als ausreichende Schutzvorkehrungen prinzipiell geeignet (hängt von konkreter Umsetzung ab, die pauschal nicht beurteilt werden kann)
- **Ergebnis:** Verhältnismäßigkeit nur eingeschränkt gewahrt!

4.4.1 Anforderungen zur Telekommunikationsüberwachung (1)

- Anordnung nur zulässig, wenn bestimmte Tatsachen den Verdacht begründen, dass schwerwiegende Straftaten (siehe Katalog aus § 100a StPO) durch den Zuüberwachenden begangen oder vorbereitet wurden bzw. eine entsprechende Beihilfe vorliegt, und eine andere Erforschung des Sachverhalts aussichtslos oder wesentlich erschwert wäre
- Richterliche Anordnung erforderlich; nur bei Gefahr im Verzug auch Anordnung durch Staatsanwaltschaft möglich, die aber einer richterlichen Bestätigung bedarf (§ 100b Abs. 1 StPO)
- Aufzeichnungsdaten sind auf entsprechende Anordnung (für 3 Monate nach § 100b Abs. 2 StPO) durch jeden zu ermöglichen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt (§ 100b Abs. 3 StPO mit Verweis auf § 110 TKG & TKÜV)

4.4.1 Anforderungen zur Telekommunikationsüberwachung (2)

- Aufzeichnung ist unverzüglich zu beenden, wenn die Voraussetzungen aus § 100a StPO nicht mehr vorliegen (§ 100b Abs. 4 StPO)
- Aufzeichnungsunterlagen sind unverzüglich zu vernichten, wenn die Unterlagen nicht (mehr) zur Strafverfolgung erforderlich sind (§ 100b Abs. 5 StPO)
- Auf Anordnung ist von den geschäftsmäßigen Erbringern oder Mitwirkenden von Telekommunikationsdiensten Auskunft über Telekommunikationsverbindungsdaten zu erteilen (§ 100g Abs. 1 StPO)
- Das Zeugnisverweigerungsrecht nach § 53 StPO verhindert eine entsprechende Verwertung von Aufzeichnungsdaten (§ 100h Abs. 2 StPO)

4.4.1 Anforderungen zur Telekommunikationsüberwachung (3)

- Betroffene sind über Telekommunikationsüberwachungsmaßnahmen erst zu unterrichten, sobald keine Gefährdung des Untersuchungszwecks, *der öffentlichen Sicherheit*, von Leib und Leben einer Person *sowie der Möglichkeit der weiteren Verwendung eines eingesetzten verdeckten Ermittlers* (mehr) gegeben ist (§ 101 Abs. 1 StPO) [kursive Formulierung voraussichtlich unwirksam analog zum BVerfG-Urteil zum Großen Lauschangriff!]

4.4.2 Anforderungen zur Wohnraumüberwachung (1)

- Anordnung nur zulässig, wenn bestimmte Tatsachen den Verdacht begründen, dass besonders schwere Straftaten (siehe Katalog aus § 100c Abs. 2 StPO) durch den Zuüberwachenden begangen oder vorbereitet wurden bzw. eine entsprechende Beihilfe vorliegt, und eine andere Erforschung des Sachverhalts aussichtslos oder unverhältnismäßig erschwert wäre (§ 100c Abs. 1 StPO)
- Äußerungen zum Kernbereich privater Lebensgestaltung dürfen nicht aufgezeichnet werden (§ 100c Abs. 4 und 5 StPO) [Umsetzung des BVerfG-Urteils vom 03.03.2004 zum Großen Lauschangriff]
- richterliche Anordnung nur auf Antrag der Staatsanwaltschaft zulässig und i.d.R. auf 1 Monat beschränkt (§ 100d Abs. 1 StPO)

4.4.2 Anforderungen zur Wohnraumüberwachung (2)

- Voraussetzungen für die Anordnung sind ausdrücklich unter Darlegung der wesentlichen Abwägungsgesichtspunkte (zu Erforderlichkeit und Verhältnismäßigkeit) zu benennen (§ 100d Abs. 3 StPO)
- Über den Verlauf und die Ergebnisse der Wohnraumüberwachung ist das anordnende Gericht zu unterrichten (§ 100d Abs. 4 StPO)
- Aufzeichnungsdaten sind unverzüglich zu vernichten, wenn sie nicht mehr zur Strafverfolgung erforderlich sind (§ 100d Abs. 5 StPO)
- Zweckänderung nur für ausdrücklich bestimmte Fälle zulässig (§ 100d Abs. 6 StPO)
- Herkunft der Daten ist zu kennzeichnen (§ 100d Abs. 7 StPO)

4.4.2 Anforderungen zur Wohnraumüberwachung (3)

- Betroffene sind über Wohnraumüberwachungsmaßnahmen durch die Staatsanwaltschaft zu unterrichten, sobald keine Gefährdung des Untersuchungszwecks oder von Leib, Leben oder Freiheit einer Person bzw. eines bedeutenden Vermögenswertes (mehr) gegeben ist (§ 100d Abs. 8 StPO)
- Das Zeugnisverweigerungsrecht nach § 53 StPO verhindert eine entsprechende Verwertung von Aufzeichnungsdaten (§ 100c Abs. 6 StPO)

4.5 Antiterrordatei und Trennungsgebot (1)

- Beim BKA werden sowohl von Polizeibehörden als auch von Nachrichtendiensten eine gemeinsame standardisierte zentrale Antiterrordatei zur Erfüllung ihrer jeweiligen gesetzlichen Aufgaben geführt (§ 1 Abs. 1 ATDG)
- Es dürfen nur Daten eingespielt werden, zu deren Erhebung die betroffene Behörde berechtigt ist (§ 2 ATDG)
- Kennzeichnungspflichten sind beizubehalten (§ 3 Abs. 2 ATDG)
- Einzelne Datenbestände werden für unbefugte Behörden auf Entscheidung des Behördenleiters der speichernden Stelle verdeckt gespeichert (§ 4 Abs. 1 ATDG)
- Ein Zugriff auf die Antiterrordatei ist nur zur Erfüllung der gesetzlichen Aufgaben zugunsten auf Aufklärung bzw. Bekämpfung internationalen Terrorismus zulässig (§ 5 Abs. 1 ATDG)

4.5 Antiterrordatei und Trennungsgebot (2)

- Über erweiterte Grunddaten (im Sinne von § 3 Abs. 1 Nr. 1 lit. b ATDG) erhält eine anfragende Behörde nur Zugriff, wenn eine Übermittlung zulässig wäre (§ 5 Abs. 1 ATDG)
- Im Eilfall darf auf die erweiterten Grunddaten durch die abfragende Behörde zugegriffen (und die Daten auch genutzt) werden, wenn dies aufgrund bestimmter Tatsachen erfolgt zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben, Gesundheit oder Freiheit einer Person bzw. einer Sache von erheblichem Wert, deren Erhalt im öffentlichen Interesse geboten ist, und die eingehende Behörde nicht nachträglich ihre Zustimmung verweigert (§ 5 Abs. 2 ATDG)
- Über die Abfragen sind jeweils Zweck und Dringlichkeit zu dokumentieren (§ 5 Abs. 4 ATDG)

4.5 Antiterrordatei und Trennungsgebot (3)

- Einsichtnahme und Verwendungsberechtigung hängt maßgeblich von den gesetzlich zugewiesenen Aufgaben der Behörde ab
- die Trennung zwischen Nachrichtendienst und Polizeibehörden betrifft organisatorische Regelungen und wird daher überwiegend formal-institutionell gefordert (wäre also gegeben)
- jede Behörde hat zu prüfen (und im Zweifel darzulegen), ob sie zur Datenerhebung berechtigt wäre und folglich entsprechende Daten empfangen darf (durch ATDG gewährleistet)
- die eingehende Behörde muss dem Abruf von erweiterten Grunddaten zustimmen, nicht aber dem Abruf von Grunddaten

4.5 Antiterrordatei und Trennungsgebot (4)

- In den Grunddaten befinden sich insbesondere Angaben zu besonderen körperlichen Merkmalen, die zu den besonderen Arten personenbezogener Daten nach § 3 Abs. 9 BDSG zu rechnen sind (Gesundheitsdaten!), sowie Angaben über Sprachen und Dialekte und Lichtbilder (ggf. Hinweis auf rassische oder ethnische Herkunft im Sinne von § 3 Abs. 9 BDSG)
- Für besondere Arten personenbezogener Daten sind besondere Schutzvorkehrungen zu treffen und eine Übermittlung nur zulässig, wenn dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist (§ 13 Abs. 2 Nr. 5 BDSG) oder zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist (§ 13 Abs. 2 Nr. 6 BDSG)

4.5 Antiterrordatei und Trennungsgebot (5)

- Die Vorgaben aus § 13 Abs. 2 Nr. 5 und Nr. 6 BDSG sind im ATDG nicht ausreichend berücksichtigt! [allerdings kann bestenfalls davon ausgegangen werden, dass diese Einschränkung zumindest von den Bundesbehörden dennoch subsidiär zu befolgen ist]
- Der für eine baden-württembergische Polizeibehörde vorrangige § 33 Abs. 3 LDSG berechtigt dagegen bereits die Verarbeitung besonderer Arten personenbezogener Daten zur Gefahrenabwehr (§ 33 Abs. 3 Nr. 1 LDSG) und zur Verfolgung von Straftaten oder Ordnungswidrigkeiten (§ 33 Abs. 3 Nr. 2 LDSG)
- Für Ordnungswidrigkeiten wiederum sind damit die Schwellen nicht hoch genug angesetzt!

4.5 Antiterrordatei und Trennungsgebot (6)

- Sicherheitsbehörden dürfen nur auf die Daten zugreifen, die für ihre Aufgabenbewältigung erforderlich sind (siehe auch § 16 Abs. 1 LDSG). Dies ist bei den aufgeführten besonderen Arten personenbezogener Daten zur Verfolgung von Ordnungswidrigkeiten nicht gegeben! [die entsprechende Regelung aus der EU-Datenschutz-RL gilt zwar nicht für die öffentliche Sicherheit und die Sicherheit des Staates, darunter fällt jedoch nicht die Verfolgung von Ordnungswidrigkeiten; in Anlehnung an den Rasterfahndungsbeschluss des BVerfG ist hierbei die Einschreitschwelle zu niedrig!]
- **Insofern wird auch die Trennung zwischen Nachrichtendiensten und Polizeibehörden aufgabenwidrig aufgehoben!**