

Welche Gefahren sind mit dem Einsatz von **IT-Systemen** verbunden?

1. Fehlerhafte Datenverarbeitung

- 1.1 Die abgespeicherten Daten sind mit dem Betroffenen mangels Kenntnis der speichernden Stelle oder mangels Auskunftsrecht (bes. im Sicherheitsbereich) unbekannt und können somit nicht auf ihre Richtigkeit oder Rechtmäßigkeit überprüft werden.

Teilweise werden die Daten aus Personalmangel nicht gepflegt. Gleiche Datensätze in unterschiedlichen Datenbanken haben häufig unterschiedliche Aktualität.

- 1.2 Daten werden versehentlich an falsche Endgeräte überspielt. Häufig herrscht Schlamperei bei der Datenlöschung oder bei der Beseitigung von alten Ausdruck (z.B. Datensammlung auf dem Müllberg).

Namensverwechslungen aufgrund fehlerhaften Daten oder gleicher Namen kommen vor. Folgen: Falsche Beschuldigungen, Kreditsperre etc.

Vortäuschen oder Verwechseln einer Datenempfangsberechtigung oder Insidervortäuschung durch fehlende Anruflegitimierung sind möglich.

Möglich sind „Freundschaftsdienste“ für vertrauenswürdige Personen oder Dienststellen, z.B. Amtshilfe (Werkschutz, Detektei oder andere Mittelsmänner).

2. Computerkriminalität

- 2.1 Je mehr Terminals, PCs und Modems bzw. ISDN-Anschlüsse vorhanden sind, desto mehr Mißbrauchsgefahren entstehen.

Absichtliches, kriminelles Unterlaufen von Gesetzen, Schutzbereichen etc. durch Überspielung der Daten an Schwachstellen der Speicherkette wird möglich.

- 2.2 Lukrativer Nebenerwerb für Zugriffsberechtigte.

Machtzuwachs durch Sammeln von Erpressungsmaterial (Vorstrafen, Schulden, Pfändungen, frühere Aktivitäten, medizinische Daten, Daten aus dem persönlichen oder Intimbereich etc.).

Durch immer umfangreichere, zentral geführte oder miteinander verknüpfte Dateien wächst das Interesse an den Daten (immer mehr „Hacker“). Der mögliche Schaden für die Betroffenen durch Raubkopien oder Datenverfälschungen steigt rapide.

- 2.3 Daten stammen aus dunklen Quellen oder „schwarzen Listen“. In diesen Bereich gehören alle Auswertungen ohne gesetzliche Grundlage oder ohne schriftliches Einverständnis des Betroffenen.

3. Ordnungsgemäße Datenverarbeitung

- 3.1 Verlust des persönlichen Kontakts zum Beurteilenden. Die Beurteilung erfolgt anhand von einzelnen Daten anstatt die Person zu befragen und kennenzulernen.. Verlust der Identität (Datensatz anstelle Mensch).

Die Beurteilung kann schon deshalb erfolgen, weil von einer Person ein paar Daten (evtl. sogar irrtümlich) in einer bestimmten Datei abgespeichert sind (bes. im Sicherheitsbereich). Rechtfertigung ist ausgeschlossen, da kein Kontakt zum Betroffenen hergestellt wird.

- 3.2 Daten sind verschlüsselte Kurzangaben (z.B. in sog. „Merkmalsleisten“. Fehlerinterpretationen sind daher nicht auszuschließen (Aussageverlust, z.B. Datenkrüppel „amtsbekannt“).

Wenn Verdachtsdaten abgespeichert werden – ohne Angabe des Verdachtsgrundes – wenn Daten aus sog. Lauschmaterial oder aus der sog. Lumpenverwertung stammen, also unzulässig sind, ist eine Überprüfung unmöglich. Gefahr des Werturteils und der Benachteiligung ohne Prozeß oder prozeßfähige Beweise.

Medienbedingte Informationsverkürzung (Buch, Zeitung, Fernsehen ...).

- 3.3 Löschen von Daten wird häufig „vergessen“, teilweise sogar systembedingt verhindert („Sicherheitsbereich), zumindest besteht psychologisch die Angst, Daten endgültig zu löschen. Die Vergangenheit wird wichtiger als die Zukunft.

- 3.4 Daten werden für andere Anwendungen zur Verfügung gestellt, als bei der Datenerhebung angegeben oder vermutet wurde. Die Daten werden je nach Interessenlage gezielt selektiert. Zweckoffene Systeme (Datensammlungen auf Vorrat zu unbestimmtem Zwecken) können zu nicht mehr nachvollziehbaren „Erkenntnissen“ führen.

- 3.5 Der Besitzer der Daten kann sich durch Simulationsauswertungen einen beachtlichen Informationsvorsprung verschaffen (Wissen ist Macht).

Durch Schaffung von sog. „Erfahrungsdatenbanken“ kann dieser Informationsvorsprung ständig überprüft und ausgebaut werden. Richtwerte, Rahmenbedingungen und dergleichen werden vom Datenlieferanten nicht als vorgegeben erkannt. Geplantes wird für Schicksal oder Zufall gehalten.

- 3.6 Verhaltensänderung durch tatsächliche oder mutmaßliche Kontrolle (z.B. kreisende Kamera im Supermarkt, Telefonüberwachung, Überwachung der Post und E-Mail...). Der Wunsch vieler, sich so zu verhalten, daß man nicht auffällt, führt zur Anpassung an die gesetzten Normen und erhöht den Anpassungsdruck für alle anderen.