Workshop der Alcatel SEL Stiftung für Kommunikationsforschung in Kooperation mit dem Hans-Bredow-Institut für Medienforschung „Next Generation E-Government für die innere Sicherheit - Erfahrungen Praxisberichte und Visionen“ am 10. August 2004 in Hamburg

Redebeitrag des Herrn BfD

„eGovernment bei Sicherheitsbehörden – virtueller Datenschutz?“

- Punktation -

I. Einleitung

- **Gesellschaftlicher Umbruch - Wandel zur Informations- und Wissensgesellschaft**

  Die Nutzung moderner Informations- und Kommunikationstechnologien ist von zentraler Bedeutung für die wirtschaftliche, gesellschaftliche und kulturelle Entwicklung Deutschlands (Beispiele: Anstieg der Internetnutzung (aktuell nutzen bereits mehr als die Hälfte aller Deutschen das Internet (Steigerung bis 2006 auf nahezu zwei Drittel)); Deutschland ist mit deutlichem Abstand der größte E-Commerce-Markt in Europa und hat weltweit die fünft höchste Internet-Nutzerdichte (hinter Kanada, Südkorea, USA und Japan - vor Großbritannien und Frankreich); Quelle: Aktuelle Studie im Auftrag des BMWA vom April 2004 (TNS infratest, Monitoring Informationswirtschaft, chart 21, 26, 30)). Vor diesem Hintergrund verdeutlicht sich die Notwendigkeit zur Modernisierung der Verwaltung mittels eGovernment.

- **Gestaltungspotential von eGovernment im Sicherheitsbereich?**

  Die Frage, welche Anwendungsmöglichkeiten eGovernment im Bereich der inneren Sicherheit bietet, welche Chancen und Risiken hieraus resultieren und welche datenschutzrechtlichen Garantien – auch zur Vermeidung potentieller Nachteile – unabdingbar zu gewährleisten sind, ist angesichts der besonderen Intensität des Eingriffs staatlicher Sicherheitsmaßnahmen in das Recht auf informationelle Selbstbestimmung datenschutzrechtlich von zentraler Bedeutung. Zur Beantwortung dieser Frage möchte ich zunächst die wesentlichen Aspekte des eGovernment (Ziele, Auswirkungen, (potentielle) Gefahren etc.) darlegen und - von dieser Grundlage ausgehend - die im Sicherheitsbereich bestehenden (spezifischen) Gefahrenlagen sowie die zu gewährleistenden (datenschutz-) rechtlichen Garantien aufzeigen und deren Relevanz anhand praktischer Beispielfälle verdeutlichen.

II. Modernisierung der Verwaltung mittels eGovernment

1. **Ziel**
   Optimierung des Verwaltungshandelns
   - schneller,
   - einfacher,
   - effektiver,
   - transparenter.

2. Umsetzungsschritte

- September 2000: Bundeskanzler initiiert Projekt **„BundOnline 2005“** – „größte eGovernment-Initiative Europas“ – so Bundesinnenminister Otto Schily (Quelle: „Government Computing“ Ausgabe 4/04). Ziel: Bis zum Jahre 2005 sollen die fast 450 internetfähigen Dienstleistungen der Bundesverwaltung online zur Verfügung stehen (Ende des Jahres 2003 bereits 260 Dienstleistungen online nutzbar).
- Juni 2003: Regierungschefs von Bund und Ländern beschließen auf der CeBIT gemeinsame eGovernment-Strategie „Deutschland-Online“. Ziel: Stufenweise Entwicklung einer vollständig integrierten eGovernment-Landschaft in Deutschland bis zum Jahre 2010.
  Strategie **„Deutschland-Online“** beruht auf fünf Säulen:
  - Portfolio prioritärer Dienstleistungen zur Bereitstellung der wichtigsten Online-Angebote,
  - Harmonisierung und Vernetzung der Internetportale,
  - Schaffung gemeinsamer Infrastrukturen zur Erleichterung des Datenaustauschs,
  - Entwicklung gemeinsamer Standards zum effizienten Datenaustausch sowie
  - Optimierung des Know-how-Transfers zur eGovernment-Koordinierung.

3. eGovernment

a) Definition

Durchführung von Prozessen der öffentlichen Willensbildung, der Entscheidung sowie der Leistungserstellung und –abwicklung in Politik, Regierung und Verwaltung unter Nutzung der modernen Informations- und Kommunikationstechniken (IT), insbesondere des Internet, in Bezug auf den gesamten öffentlichen Sektor.

b) Bedeutung für Bürger, Wirtschaft und Verwaltung

- Verbesserte Einbeziehung von Bürgern und Unternehmen in das Verwaltungshandeln (staatliche Verwaltungsakte und Dienstleistungen).
- Effizientere Ausgestaltung von Verwaltungsabläufen durch zielbewusste und konsequente Nutzung moderner IT.
- Internet (world wide web (www)) als wichtigster Informationsweg zwischen Bürgern, Unternehmen und Verwaltung.
- Anwendungserstreckung auf alle **Interaktionsformen** – Beispiele:

  - **eInformation**
    Unaufgeforderte Bereitstellung von (klassischen) Informationsangeboten, insbesondere im Rahmen zentraler Portale der öffentlichen Verwaltung; Abholung durch unbekannten Nutzerkreis ohne darüber hinausgehende Kontaktaufnahme.

  - **eKommunikation**
    Aufbau und Durchführung reiner auf den Austausch von Informationen gerichteter Kommunikationsprozesse (z.B. Online-Verbindungen, Videokonferenzen, Internetchats, eMail).

  - **eTransaktion**
    Für beide Seiten verbindliche und möglichst vollständige Abwicklung von Verwaltungsaufgaben unter Einschluss der abschließenden Entscheidung

und deren Bekanntgabe auf elektronischem Wege. Elektronische Signatur insoweit von zentraler Bedeutung.

- **eVerwaltungsverfahren**
  Unterfall der eTransaktion. Umfasst das über die eigentliche Transaktion hinausgehende Vor- und Umfeld von Verwaltungsentscheidungen – den gesamten Workflow innerhalb der Verwaltung, d.h. elektronische Vorgangsbearbeitung, Akteneinsicht, Erteilung rechtlich verbindlicher Auskünfte etc.

- **eArchiv**
  Kernpunkt: Elektronische Archivierung abgeschlossener Verfahren. Folge: Dauerhafte Nutzbarkeit archivierter elektronischer Dokumente. Datenschutzrechtlich besonders bedeutsam hinsichtlich Datenlöschung (separate Löschbarkeit einzelner Verfahren oder Arbeitsschritte).

c) Erscheinungsformen / Beziehungsgeflechte bzw. Schnittstellen

- Verwaltung – Bürger (**Government to Citizen, G2C**):
  Öffentliche Leistungserbringung durch Bundes-, Landes- oder Kommunalverwaltung unmittelbar zugunsten des Bürgers; Partizipation der Bürger an politischen Entscheidungsprozessen.

- Verwaltung – Wirtschaft (**Government to Business, G2B**):
  Inanspruchnahme öffentlicher Leistungen durch Unternehmen oder Nutzung von Leistungen der Privatwirtschaft durch die Verwaltung.

- Verwaltung – Verwaltung/Partner **(Government to Government, G2G)**:
  Informations- und Leistungsaustausch unter eigenständigen Verwaltungseinheiten oder anderen Leistungspartnern (kooperierende Verwaltung).

- Verwaltung – Beschäftigte **(Government to Employee, G2E)**:
  Unterstützung der Beschäftigten bei der effizienten Verrichtung ihrer Tätigkeit durch interne Informationen und Leistungen.

III. (Neue) Herausforderungen für Datenschutz und Datensicherheit

1. Sicherheitsbedenken in der Bevölkerung

81 Prozent aller deutschen Internet-Nutzer haben noch erhebliche Sicherheitsbedenken im Hinblick auf die Nutzung des Internets (s.o. aktuelle Studie im Auftrag des BMWA vom April 2004, 7. Faktenbericht 2004, S. LIX.)

2. (Potentielle) Gefahren

a) Generelle Bedrohungen

- **Unsichtbarkeit elektronischer Informationen**
  - Lesbarkeit elektronisch gespeicherter/übertragener Informationen nur mittels technischer Hilfsmittel (Soft-/Hardware);

- Kopie und Original digitaler Dokumente nicht mehr unterscheidbar.

➢ **Flüchtigkeit elektronischer Informationen**
- Prinzipielle Verlustgefahr – ohne Verbleib irgendwelcher Spuren;
  mögliche Ursachen: Entmagnetisierung durch Alterung des Datenträgers, Temperatur, Luftfeuchte, äußere Magnetfelder, versehentliches/vorsätzliches Löschen/Überschreiben, technisches Versagen von Festplatten.

➢ **Veränderung räumlicher Relation**
- Aufgrund ständig zunehmender Vernetzung Zugriff auf elektronisch gespeicherte Daten unabhängig vom Ort (weltweit) und vom Endgerät (Großrechner, PC etc.) möglich.

➢ **Lediglich elektronische Protokollierung**
- Elektronisch gespeicherte Protokolle unterliegen gleichen Gefährdungen wie die verarbeiteten Daten selbst (Flüchtigkeit etc.).

b) Spezifische Bedrohungen

➢ **Zunahme personenbezogener Daten**
Systembedingt offenbart das Internet eine Vielzahl personenbezogener Informationen über seine Nutzer. So fallen im Rahmen des eGovernment neben vorgangsbezogenen Daten der Bürger weitere personenbezogene Daten an. Zu unterscheiden sind folgende Datentypen:

- **Bestandsdaten**
  Notwendig zur Nutzung von eGovernment; dem Betroffenen auf Dauer zugeordnet z.B.
  - Name,
  - Anschrift,
  - E-Mail-Adresse,
  - Telefon- oder Faxnummer,
  - Geburtsdatum,
  - Bankverbindung,
  - Kreditkartennummer,
  - Öffentlicher Schlüssel,
  - User-ID,
  - Statische IP-Adressen.

- **Nutzungsdaten**
  Notwendig für Inanspruchnahme von Tele- und Mediendiensten, insbesondere:
  - Merkmale zur Identifikation des Nutzers,
  - Angaben über Beginn und Ende sowie Umfang der jeweiligen Nutzung und
  - Angaben über die von den Nutzenden in Anspruch genommenen Tele- oder Mediendienste.

- **Verbindungsdaten**
  Beispiel: E-Mail
  - E-Mail-Adresse,

- Zeitpunkt der Sendung bzw. Zustellung,
- Routing-Informationen (Angaben über diejenigen Rechner, die eine E-Mail durchgeleitet haben).

- **Inhaltsdaten**
  Beispiel: E-Mail
  - Angaben über den Betreff,
  - Bezeichnungen von Datei-Anlagen.

➢ **Zusammenführung von Daten an Kommunikationsstellen**
- Die Kommunikationsstellen zwischen Verwaltung und Nutzern (z.B. Internet-Portal, virtuelle Poststelle etc.) sind die wichtigsten Schaltstellen von eGovernment. Da an diesen Schnittstellen die Kommunikationsvorgänge zusammenlaufen, entstehen umfangreiche Datensammlungen und damit neuartige Bedrohungen für die Privatsphäre – konkret:
  - Erfassung und Analyse der gesamten Kommunikation Einzelner mit Behörden (G2C, G2B),
  - Zusammenführung und Verdichtung der Daten zu (teilweisen) Persönlichkeitsprofilen,
  - Durchbrechung der Zweckbindung elektronisch übertragener Daten.

➢ **Zentrale Datenbestände**
- Schaffung zentraler, bereichsübergreifender Datenbestände, um Bürgern und Unternehmen Verwaltungsdienstleistungen unterschiedlicher Behörden oder Behördenbereiche an einer zentralen Stelle oder mit einem elektronischen Verfahren **(One-Stop-Government)** anbieten zu können. Daraus resultieren folgende Bedrohungen:
  - Durchbrechung der Zweckbindung gespeicherter Datenbestände,
  - Durchbrechung der „informationellen Gewaltenteilung“,
  - mangelnde Transparenz für die Betroffenen (wer greift zu welchem Zweck auf welche Daten zu),
  - unzulässiges Aufspüren unbekannter Zusammenhänge mit Data Mining.

➢ **Organisatorische Veränderung bestehender Arbeitsabläufe, Tätigkeitsfelder, Datenschutzmaßnahmen**
Gewährleistung der bisherigen Mitwirkung aller maßgeblichen Stellen (z.B. behördlicher/betrieblicher Datenschutzbeauftragter, Personalvertretung etc.).

➢ **Elektronische Archivierbarkeit (eArchiv) / Recherchierbarkeit**
Dauerhafte Nutzbarkeit und - vergleichsweise einfache und schnelle - Recherchierbarkeit elektronisch archivierter Daten;
Beispiele:
- www.archiv.org (Funktion „take me back“; z.B. detaillierte, chronologische Darstellung der inhaltlichen Entwicklung der Homepage des BfD, der TELEKOM etc.);
- www.google.de (Funktion „Group-Suche“ am Beispiel „Peter Schaar“; chronologische Auflistung aller Beiträge in allen Groups von bzw. über Herrn Peter Schaar).

- **Authentifizierungserfordernis**
  Gewährleistung der Authentizität und Integrität durch entsprechende Sicherungsmaßnahmen (elektronische Signatur). Wichtig: Strikte Wahrung der Vertraulichkeit des Signaturschlüssels.

c) Bedrohungen bei der Daten verarbeitenden Stelle

- **Angriffe auf sicherheitstechnische Einrichtungen, z.B. aufgrund**
  - fehlender regelmäßiger Softwareaktualisierung,
  - veralteter, unsicherer Verschlüsselungs- oder Signaturverfahren,
  - unsachgemäßem Umgang mit Zertifikaten oder geheimen Schlüsseln.

- **Unzulässiger Umgang mit elektronisch gespeicherten Daten**
  Gefährdung der Zweckbindung, Verfügbarkeit und Integrität z.B. aufgrund
  - unzulässiger Datenübermittlung an Dritte,
  - versehentlicher Löschung oder Veränderung bei der Verarbeitung,
  - unzureichender Benutzer- und Rechteverwaltung,
  - fehlender Zuständigkeitsregelungen für die Pflege zentraler Datenbestände.

d) Bedrohungen beim Transport

Eigenschaften des Transportwegs über öffentliche Netze sind dem Absender und dem Empfänger regelmäßig weder bekannt noch durch sie beeinflussbar. Dies gilt sowohl für den Leitungsweg als auch für die Anzahl und Lokation der passierten Vermittlungsrechner. Kommunikation über öffentliche Leitungen beinhaltet beispielsweise folgende Gefährdungen:

- Manipulation der Daten durch gezielte Angriffe / technische Fehlfunktionen,
- Vortäuschen einer falschen Identität oder Verschleierung der Herkunft von Daten durch unzureichende Authentifizierung,
- Übernahme von Verbindungen, wenn etwa Zeitstempel, kryptographisch erzeugte Prüfsummen oder elektronische Signaturen fehlen,
- Angriffe auf Protokolle und Dienste durch Manipulation des HTML-Codes oder infolge artfremder Nutzung des HTTP-Protokolls bzw. des HTTP-Ports 80.

e) Bedrohungen beim Nutzer von eGovernment-Anwendungen

Fehlendes / nicht ausreichendes Datenschutz- und IT-Sicherheitsniveau – Folge:

- Fehlerhafte Datenverarbeitung durch
  - veraltete / fehlerhafte Software (Viren, Trojanische Pferde, aktive Inhalte, fehlerhafte Einstellungen, Programmfehler etc.),
  - fehlerhafte Hardware (falsch installiert, unzureichend gewartet, ungenügend geprüft etc.),
- Analyse des Nutzungsverhaltens durch unzulässige Auswertung von Protokolldaten,
- Durchbrechung der Zweckbindung (Nutzung für andere als die vom Empfänger definierten Zwecke).

IV. Gestaltungspotential des eGovernments im Sicherheitsbereich

1. **Spezifische Situation / Gefahrenlagen**
   Im Vergleich zu sonstigen Verwaltungsbehörden nehmen die Sicherheitsbehörden eine „Sonderstellung“ ein, die sich im Bereich der Polizei und Nachrichtendienste beispielsweise wie folgt konkretisiert:

   - **Sicherheitsbehörden – unterschiedliche Aufgaben und Befugnisse**
     Im Gegensatz zur Polizei dürfen Nachrichtendienste personenbezogene Daten bereits bei Vorliegen „tatsächlicher Anhaltspunkte“ (niedrigste Eingriffsschwelle) erheben. Das Bundesverfassungsgericht hat diese Schwelle im Urteil zum Artikel 10-Gesetz wie folgt definiert: Das Tatbestandsmerkmal „tatsächlicher Anhaltspunkt“ kann den verfassungsrechtlichen Anforderungen im Ansatz nur genügen, wenn eine einengende Auslegung sicherstellt, dass nicht im wesentlichen Vermutungen, sondern konkrete und in gewissem Umfang verdichtete Umstände als Tatsachenbasis für den Verdacht vorliegen.

   - **Zunehmende informationelle Kooperation - Beachtung des Trennungsgebotes**
     In zunehmendem Maße soll eine engere informationelle Kooperation zwischen Polizei und Nachrichtendiensten erfolgen (elektronischer Datenaustausch, Vernetzung vorhandener Datenbestände, Aufbau gemeinsamer Dateien, Errichtung eines gemeinsamen Lage- und Analysezentrums).
     Eine uneingeschränkte informationelle Kooperation von Polizei und Nachrichtendiensten (G3G) ist aufgrund der unterschiedlichen Aufgaben und Befugnisse dieser Behörden mit dem verfassungsrechtlichen Trennungsgebot nicht zu vereinbaren.
     Folge:
     - Unzulässigkeit eines elektronischen Vollverbunds (z.B. Zusammenführung aller polizeilichen und nachrichtendienstlichen Informationen in einer „gemeinsamen Datei“ bzw. Einrichtung unbeschränkter wechselseitiger Online-Direktzugriffsrechte auf bestehende Dateien).
     - Beachtung der als Ausprägung des Trennungsgebotes normierten Regelungen zur Übermittlung personenbezogener Daten zwischen Polizei und Nachrichtendiensten.

   - **Zulässigkeit „verdeckter“ Datenerhebung**
     Aufgrund überragender Gemeinwohlbelange (Schutz der Verfassung, Gefahrenabwehr, Strafverfolgung) genießen die Sicherheitsbehörden gegenüber sonstigen Behörden eine vergleichsweise weitreichende Befugnis zur Verarbeitung personenbezogener Informationen. Sie sind berechtigt, personenbezogene Daten nicht nur „offen“, sondern auch durch „besondere Mittel“ (§ 23 BKAG), d.h. durch verdeckte Maßnahmen“ (heimliche Observation, Einsatz technischer Mittel, V-Leute etc.) und damit ohne Kenntnis des Betroffenen zu erheben.

   - **Befugnis zur Verarbeitung auch „weicher“ personenbezogener Daten**
     Aufgrund ihrer „Sonderstellung“ dürfen Sicherheitsbehörden nicht nur „harte“, sondern auch „weiche“ personenbezogene Daten verarbeiten. Während erstere in der Regel das Resultat von polizeilichen Ermittlungen oder von Verwaltungsverfahren sind, handelt es sich bei den sogenannten „**weichen**“ Informationen um teilweise hochsensible, noch nicht ausermittelte, d.h. ungesicherte Daten, deren Wahrheitsgehalt zum Zeitpunkt ihrer Speicherung noch offen ist und die einer Bewertung bedürfen, um sie für die polizeiliche/nachrichtendienstliche Arbeit nutzbar zu machen.

- **Erstellbarkeit von Charakter-/Verhaltens- oder Persönlichkeitsprofilen**
  Die elektronische Verarbeitung insbesondere „weicher" personenbezogener Daten ermöglicht de facto die Erstellung von verdachtsdatengestützten Verhaltens-, Persönlichkeits- und Risikoprofilen der Betroffenen (in der analogen Welt der Papierakten war dies wegen des relativ großen Aufwandes nur ein vergleichsweise geringes Risiko). (Groß-)Rechner sind heute beispielsweise in der Lage, Datenbanken in Sekundenbruchteilen nach beliebig vielen Stichworten zu durchsuchen, die gefundenen Merkmale miteinander zu verknüpfen und das Ergebnis grafisch aufbereitet darzustellen.

- **Fehlende justizielle Kontrolle der Nachrichtendienste / Quellenschutz**
  Im Gegensatz zur polizeilichen Tätigkeit unterliegt die Tätigkeit der Nachrichtendienste keiner justiziellen Kontrolle. Hervorzuheben ist auch der im Bereich der Nachrichtendienste bestehende weitreichende Quellenschutz.

2. **Verfassungsrechtliche Vorgaben / Gewährleistungen**
   Ausgehend von der „Sonderstellung" der Sicherheitsbehörden und den damit verbundenen spezifischen Gefahrenlagen im Bereich der inneren Sicherheit für das Recht auf informationelle Selbstbestimmung stellt sich die Frage, welche datenschutzrechtlichen Anforderungen eGovernment im Sicherheitsbereich - auch unter Berücksichtigung zukünftiger technischer Entwicklungen – gewährleisten muss, d.h. welche Rechtsfolgen bzw. Vorgaben aus dem verfassungsgerichtlich entwickelten Recht auf informationelle Selbstbestimmung abzuleiten sind.

   - **Recht auf informationelle Selbstbestimmung – Rechtsfolgen (Grundlagen: „Volkszählungsurteil"; Urteil zum „Großen Lauschangriff")**
     Nach der Rechtsprechung des Bundesverfassungsgerichts („Volkszählungsurteil") ist jede Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ein Eingriff in das durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz (GG) geschützte Recht auf informationelle Selbstbestimmung. Nach Auffassung des Gerichts bedarf die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, auch unter den heutigen – und zukünftigen – Bedingungen der automatisierten Datenverarbeitung insbesondere des Schutzes. Diese Befugnis des Einzelnen ist vor allem deshalb gefährdet, weil bei Entscheidungsprozessen nicht mehr wie früher auf manuell zusammengetragene Karteien oder Akten zurückgegriffen werden muss, sondern mit Hilfe automatisierter Datenverarbeitung bereits heute Einzelangaben über persönliche und sachliche Verhältnisse einer Person, d.h. personenbezogene Daten, technisch unbegrenzt gespeichert und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abgerufen werden können. Die Immaterialisierung und Globalisierung von Informationsströmen durch das Internet hat diese Entwicklung maßgeblich befördert.

   - **Fortgeltung – auch unter den Bedingungen der modernen Informationstechnologien?**
     Damit stellt sich die Frage: Hat die rasante technische Entwicklung zur Folge, dass der Staat das Grundrecht auf informationelle Selbstbestimmung, nicht mehr so effektiv schützen kann bzw. muss wie bisher, so dass sich die bisherige Vollzugsverantwortung des Staates in eine Gewährleistungs- und Infrastrukturverantwortung gewandelt hat?

Zur Beantwortung dieser Frage darf ich auf das Urteil des Bundesverfassungsgerichts verweisen. Es hat – die rasant fortschreitende technische Entwicklung voraussehend – eindeutig festgelegt, dass die individuelle Selbstbestimmung auch unter den Bedingungen moderner Informationsverarbeitungstechnologien gewahrt werden muss.

In seinem aktuellen Urteil zum „Großen Lauschangriff" vom 3. März 2004 hat das Gericht nochmals betont, dass die verfassungsrechtliche Beurteilung der Informationserhebung auch davon abhängt, in welchen Verwendungszusammenhängen die gewonnenen Informationen genutzt werden können und welche Schutzvorkehrungen, insbesondere welche datenschutzrechtlichen Regelungen, getroffen worden sind. Ist eine weitere Verwendung der Daten ohne verfassungsrechtlich hinreichende Sicherungen möglich, ist auch die Datenerhebung nach Auffassung des Gerichts verfassungswidrig.

Fazit: Die verfassungsgerichtlichen Vorgaben sind – auch im Hinblick auf zukünftige technische Entwicklungen – im Sicherheitsbereich strikt zu beachten. Diese Notwendigkeit verdeutlichen auch die folgenden praktischen Beispiele.

V. Praxisrelevante Beispiele

1. Verhältnis Bürger – Sicherheitsbehörde (G2C)

- **Geltendmachung datenschutzrechtlicher Ansprüche**
  Die elektronische Abwicklung datenschutzrechtlicher Ansprüche der Betroffenen, z.B. auf Auskunft der zu ihrer Person gespeicherten Daten, hat zur Folge, dass insbesondere im Sicherheitsbereich teilweise hochsensible personenbezogene Daten elektronisch übermittelt werden. Hinsichtlich der damit verbundenen Gefahren darf ich auf meine vorherigen Äußerungen verweisen.
  Folge: Notwendigkeit zur Abwehr (potentieller) Bedrohungen (s.o. III, 2) durch Gewährleistung sicherer Authentifizierungsverfahren (elektronische Signatur (s.o. III, 2)) und Implementierung technisch sicherer Kommunikationsstrukturen.

- **Virtuelle Polizei(-dienststelle)**
  Jede elektronische Kontaktaufnahme, z.B. mit einer virtuellen Polizeidienststelle anlässlich einer Anzeigeerstattung, kann die Registrierung aller elektronischen Spuren des Absenders zur Folge haben (hinsichtlich Art und Umfang dieser personenbezogenen Daten - s.o. III, 2 b)).

- **Virtuelle Zentralstelle zur Korruptionsbekämpfung**
  Beispiel: Business Keeper Monitoring System (BKMS) des LKA-Niedersachsen. Erfassung per Internet anonym übermittelter Hinweise aus der Bevölkerung über (vermeintlich) illegales Geschäftsgebaren. Projektbeginn: Oktober 2003. Bis Mitte Juli 2004 bereits 336 Meldungen eingegangen.
  (Potentielle) Gefahren:
  - Missbrauch (Übermittlung nicht korruptionsbezogener personenbezogener Informationen),
  - falsche Verdächtigung (Straftat gemäß § 164 Strafgesetzbuch (StGB)),
  - Vortäuschen einer Straftat (Straftat gemäß § 145 d StGB),

- **Polizeiliche Internetfahndung nach Beschuldigten / Zeugen**

  Die polizeiliche Internetfahndung als eine besondere Form der Öffentlichkeitsfahndung nach Beschuldigten und Zeugen verdeutlicht in besonderer Weise die im Bereich der inneren Sicherheit bestehenden spezifischen Gefahren für das Recht der Betroffenen auf informationelle Selbstbestimmung. Auch nach Schaffung entsprechender Rechtsgrundlagen in der Strafprozessordnung (§§ 131 ff. StPO) durch das Strafverfahrensänderungsgesetz 1999 (v. 02/08/2000) wird die Zulässigkeit der Öffentlichkeitsfahndung, d.h. die Zulässigkeit der Fahndung nach Beschuldigten und Zeugen in Publikationsorganen (z.B. Presse, Rundfunk, Fernsehen und Internet – vgl. Richtlinie über die Inanspruchnahme von Publikationsorganen zur Fahndung nach Personen bei der Strafverfolgung (Anlage B der Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV)), teilweise immer noch konträr beurteilt.

  Die Öffentlichkeitsfahndung ist nur unter **Einschränkungen** zulässig:
  - Zwecke:
    - Aufenthaltsermittlung oder
    - Identitätsfeststellung.
  - Ultima ratio (strenge gesetzliche Subsidiaritätsklausel, d.h. Fahndung auf andere Weise muss ausgeschlossen oder zumindest wesentlich erschwert sein).
  - Veröffentlichung von Abbildungen (Lichtbildern) der Betroffenen zulässig.
  - Zeugenstellung, d.h. die Tatsache, dass es sich nicht um einen Beschuldigten, sondern einen Zeugen handelt, muss deutlich erkennbar gemacht werden.

  (**Potentielle) Nachteile** öffentlicher Zeugenfahndung für den Betroffenen:
  - Verwechslung mit dem Beschuldigten,
  - Nähe zur Straftat.

  Besondere Eingriffsintensität der Zeugenfahndung im **Internet**

  Die Zeugenfahndung im Internet ist für den Betroffenen im Vergleich zur Fahndung in sonstigen öffentlichen Publikationsorganen (potentiell) eingriffs-intensiver.

  Begründung: Personenbezogene Daten sind im Internet leichter
  - recherchierbar,
  - archivierbar (vgl. III. 2. b)) und
  - manipulierbar.

  Zudem können auch nach dem Zeitpunkt der Löschung der ursprünglich eingestellten Daten digitale Kopien dieser Informationen, beispielsweise durch Übernahme auf andere Internetseiten (Sekundärverwertung), weltweit in unbekannter Anzahl dauerhaft recherchierbar vorhanden bleiben. Vorhalte- und Verwertungsverbote sind de facto nicht kontrollierbar.

  Konsequenz: Einstellung personenbezogener Daten ins Internet bedarf in jedem Einzelfall einer besonders sorgfältigen Verhältnismäßigkeitsprüfung.

- **Verfassungsschutzberichte im Internet – fortlaufende Veröffentlichung personenbezogener Daten**
  - **Problematik**

    Beispiel:

    In einer Eingabe hatte ein Petent vorgetragen, in mindestens zwei Fällen negative berufliche Nachteile erlitten zu haben, da potentielle Arbeitgeber aufgrund der Speicherung seiner personenbezogenen Daten in zeitlich

zurückliegenden Verfassungsschutzberichten von einer Einstellung abgesehen hätten. Sie hätten im Internet mittels einer Suchmaschine zu seiner Vergangenheit recherchiert und wären dabei in „alten" Verfassungsschutzberichten auf seinen Namen und den zu seiner Person geschilderten Sachverhalt „gestoßen". Bei der geschilderten Tat, für die er rechtskräftig verurteilt worden sei, habe es sich um „eine Jugendsünde" gehandelt. Er könne nicht verstehen, dass er wegen dieser Tat lebenslang Nachteile erleiden solle, obgleich seine Verurteilung im Bundeszentralregister (BZR) bereits vor „geraumer Zeit" getilgt worden sei. Die Löschung im BZR habe zur Folge, dass ihn das im Rahmen einer Bewerbung vorzulegende polizeiliche Führungszeugnis als nicht vorbestraft ausweise. Dieser gesetzlich intendierte Schutz werde durch die - extrem leichte und schnelle - Recherchierbarkeit seiner personenbezogenen Daten im Internet „unterlaufen".

- **Kollidierende Rechtsgüter**
  - Recht am eigenen Bild und Namen sowie „Recht auf Vergessen" (als besondere Ausprägungen des Allgemeinen Persönlichkeitsrechts) einerseits und
  - öffentliches Informationsinteresse andererseits.

- **Rechtsfolge(n) – ableitbar aus dem LEBACH-Urteil (**BVerfG 1 BvR 1087/91 vom 16.05.1995)

  Feststellungen/Vorgaben des Bundesverfassungsgerichts

  Publikation personenbezogener Daten im Fernsehen verursacht in der Regel einen weitaus stärkeren Eingriff in die private Sphäre als eine Wort- oder Schriftberichterstattung in Hörfunk oder Presse. Dies folgt zunächst aus der stärkeren Intensität des optischen Eindrucks und der Kombination von Wort und Bild, vor allem aber aus der ungleich größeren Reichweite, die dem Fernsehen auch im Verhältnis zu Film und Theater eine Sonderstellung einräumt. Es besteht daher besonderer Anlass, auf eine Wahrung der vom Recht gesetzten Schranken zu achten und einem Missbrauch des leichter verletzbar gewordenen Persönlichkeitsrechts vorzubeugen. Das Recht darf sich in diesem Punk der technischen Entwicklung nicht beugen.

  Die Ausstrahlwirkung des verfassungsrechtlichen Schutzes der Persönlichkeit lässt es nicht zu, dass sich die Kommunikationsmedien über die aktuelle Berichterstattung hinaus zeitlich unbeschränkt mit der Person eines Straftäters und seiner Privatsphäre befassen. Vielmehr gewinnt nach Befriedigung des aktuellen Informationsinteresses grundsätzlich sein **Recht**, **„allein gelassen zu werden"** zunehmende Bedeutung. Dieses Recht hat auch ein Täter, der durch eine schwere Straftat in das Blickfeld der Öffentlichkeit getreten ist und die allgemeine Mißachtung erweckt hat, denn er bleibt dennoch ein Glied der Gemeinschaft mit dem verfassungsrechtlichen Anspruch auf Schutz seiner Individualität.

  Abwägung der widerstreitenden Interessen

  Im Konfliktfall müssen beide Verfassungswerte gemäß dem Grundsatz der **praktischen Konkordanz** nach Möglichkeit zu einem schonenden Ausgleich gebracht werden. Lässt sich dies nicht erreichen, ist unter Berücksichtigung der typischen Fallgestaltung und der besonderen Umstände des Einzelfalls zu entscheiden, welches Interesse zurückzutreten hat.

- **Konsequenz**:
  - Publikation personenbezogener Daten im Internet nur nach strikter Beachtung des Grundsatzes der Verhältnismäßigkeit (adäquate Abwägung im vorstehend genannten Sinne),
  - möglichst weitgehende Anonymisierung,
  - zeitliche Limitierung (Löschung der Berichte nach 5 Jahren).
    Auch insoweit ist zu berücksichtigen, dass zum gegenwärtigen Zeitpunkt auch nach diesem Zeitablauf weltweit zeitlich unbegrenzte Recherche- und sonstige Nutzungsmöglichkeiten bestehen und unkontrollierbar bleiben, beispielsweise infolge von Sekundärverwertungen etc. (s.o. polizeiliche Internetfahndung). Auch dieses Beispiel verdeutlicht: Publikation personenbezogener Daten im Internet hat eine erheblich größere Eingriffsintensität.

2. Verhältnis Sicherheitsbehörde - Unternehmen (G2B)

- **Sicherheitserklärung online**
  Unter Federführung des Bundesministeriums für Wirtschaft und Arbeit (BMWA) wird aktuell geprüft, ob diejenigen Beschäftigten, die in Unternehmen der Privatwirtschaft im Rahmen staatlicher Auftragsabwicklungen Zugang zu vertraulich bzw. geheim eingestuften Unterlagen erhalten sollen und sich aus diesem Grunde vor der Aufnahme ihrer Tätigkeit einer Sicherheitsüberprüfung durch die deutschen Sicherheitsbehörden unterziehen müssen, die zur Einleitung dieser Überprüfung notwendige Sicherheitserklärung in elektronischer Form ausfüllen und über die verantwortlichen Unternehmensstellen an das zuständige BMWA übermitteln dürfen.
  Die Sicherheitserklärung enthält zum Teil hochsensible Daten der Betroffenen, die von den Sicherheitsbehörden überprüft werden. Die Konsequenzen dieser Überprüfung können für den Betroffenen gravierend sein. Bestehen staatliche Sicherheitsbedenken, ist ihm die Ausübung der gewünschten Tätigkeit verwehrt. Im Extremfall kann dies den Verlust des Arbeitsplatzes bedeuten.
  Angesichts der Sensibilität der Daten und der weitreichenden Konsequenzen für den Betroffenen besteht insbesondere die Notwendigkeit zur Gewährleistung sicherer Kommunikationswege sowie einer zweifelsfreien Authentifizierung sowohl des Betroffenen als auch der Behörde, die das Ergebnis der Sicherheitsüberprüfung dem Unternehmen als Arbeitgeber des Antragstellers mitteilt.

3. Verhältnis Sicherheitsbehörde - Sicherheitsbehörde (G2G)

- **Vollständige elektronische Schriftguterfassung (elektronische Akte)**
  Ziel: Modernes „Wissensmanagement“ zwecks optimaler Auswertung und Analyse des vorhandenen Gesamtdatenbestands.
  Folge:
  - Vollständige elektronische Erfassung und Speicherung aller Informationen (auch des vorhandenen Schriftgutes).
  - Umfassende digitale Recherchierbarkeit sämtlicher Informationen.
  - De facto bestehende Möglichkeit zur Erstellung umfassender (Teil-)Persönlichkeitsprofile.

- **Gemeinsame Dateien / gemeinsames Analysezentrum der Sicherheitsbehörden zur Terrorismusbekämpfung**
  In der letzten IMK-Sitzung wurden entsprechende Beschlüsse gefasst. Eine Zusammenführung aller Informationen wäre mit dem informationellen Trennungsgebot nicht vereinbar (s.o. V 1). Das Trennungsgebot prägt die inhaltliche Ausgestaltung der geltenden Übermittlungsschranken.
  Folge: Kooperation auch in Form von Teilverbünden zulässig, aber nur im Rahmen der geltenden Übermittlungsbefugnisse (s.o. V 1).

VI. Fazit / Ausblick

EGovernment ist grundsätzlich notwendig und wünschenswert.

Im Bereich der inneren Sicherheit ist der Gestaltungsspielraum von eGovernment aufgrund der besonderen Eingriffsintensität staatlicher Maßnahmen sorgfältig zu prüfen. Aus der Tätigkeit der Sicherheitsbehörden (Polizei und Nachrichtendienste) resultieren im Vergleich zur sonstigen Verwaltungstätigkeit öffentlicher Stellen besondere Gefahren für das Recht der Betroffenen auf informationelle Selbstbestimmung.

Auch im Sicherheitsbereich sind die vom Bundesverfassungsgericht seit dem Volkszählungsurteil entwickelten Vorgaben zum Datenschutz und zur Datensicherheit strikt zu beachten. So darf der Einzelne auch unter den Bedingungen einer automatischen Erhebung und Verarbeitung seiner personenbezogenen Daten nicht zum bloßen Informationsobjekt werden. Er muss alleinig befugt sein, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu entscheiden. Zudem muss er mit hinreichender Sicherheit überschauen können, welche seine Person betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind. Dies ist durch entsprechende Verarbeitungsvoraussetzungen zu gewährleisten.

Folglich ist der Staat - auch beim eGovernment im Sicherheitsbereich - verpflichtet,

- sichere Kommunikations- und Informationsstrukturen zu schaffen,
- die den Betroffenen unabdingbar zustehenden Datenschutzrechte (Auskunft, Löschung, Berichtigung, Sperrung) effektiv zu gewährleisten,
- die Grundsätze der
  - Verhältnismäßigkeit
  - Zweckbindung und
  - Unzulässigkeit multifunktionaler Verwendungen zu beachten,
- keine Persönlichkeits(-teil)profile der Betroffenen zu erstellen und
- das Trennungsgebot, d.h. die verfassungsrechtlich vorgegebenen Grenzen der informationellen Kooperation der Sicherheitsbehörden, zu respektieren.

Diese verfassungsgerichtlichen Vorgaben sind auch im Rahmen zukünftiger technischer Entwicklungen zu gewährleisten. Angesichts des rasanten Wandels der Informations- und Kommunikationstechnologie, dem damit verbundenen Wegfall zeitlicher und räumlicher Kommunikationsgrenzen und der stetigen Perfektionierung interaktiver Kommunikationsprozesse hängen die Geltungschancen des Datenschutzes, wie vor allem das Internet exemplarisch verdeutlicht, „von der Fähigkeit ab, den Konsequenzen der Technologie durch die Technologie selbst zu begegnen, ohne Rücksicht darauf, ob es um den Zugang zu Daten, ihre Verbreitung, die Integrität der Texte, die Wahrung der

Anonymität oder der Bestätigung der Identität geht.“ (Simitis, in: NJW 1998, S. 2473 (2478)).