Videoüberwachung & die Modernisierung des Datenschutzrechts

Informatik & Gesellschaft
7. Vorlesung

#7 - Aus dem Inhalt

- Newsticker: VÜ nun auch in Berlin!
- Alles Gute kommt von oben?
  - Videoüberwachung
  - Kunst der Gegenwehr - Gegenwehr der Kunst
- Zur Modernisierung des Datenschutzrechts
  - Selbstbestimmung & Selbstregulierung
  - Erforderlichkeit & Zweckbindung
  - Organisatorische Unterstützung & Datenschutz durch Technik
  - Stärkung der Betroffenenrechte
  - Effektive Kontrolle

Videoüberwachung in Berlin!

- Pressemitteilung der HUMANISTISCHEN UNION, Landesverband Berlin - Sperrfrist: 13. Juni 2002, 0:00 Uhr -
  Rot-Rote Polizeigesetznovelle führt zu uferloser Ausbreitung der Videoüberwachung

- Zu der heute im Berliner Abgeordnetenhaus eingebrachten Senatsvorlage zur Änderung des „Allgemeinen Sicherheits- und Ordnungsgesetzes" (ASOG) erklärt Nils Leopold, Datenschutzexperte der Bürgerrechtsorganisation Humanistische Union:
- „Rot-Rot verliert seine bürgerrechtliche Unschuld: Entgegen anderslautender Beteuerungen beider Regierungsparteien droht nun auch in Berlin die Videoüberwachung des öffentlichen Raumes.
- Die geplante Regelung ermöglicht es der Berliner Polizei, gefährdete Objekte und die anliegenden öffentlichen Straßen- und Grünflächen mit Videoüberwachung zu erfassen und aufzuzeichnen.

Videoüberwachung in Berlin! (II)

- Die Einstufung als ‚gefährdetes' Objekt, bleibt dabei allein der Einschätzung der Polizei überlassen. Laut Senatsvorlage kommen als ‚Bauwerke von öffentlichem Interesse' sogar ‚natürliche Trinkwasserspeicher' in Betracht. Mit solchen uferlosen Formulierungen ließe sich im Prinzip die totale Überwachung der Berliner Seenlandschaft legitimieren.
- Die Humanistische Union lehnt die weitere Ausbreitung der Videoüberwachung ab. Keine Kamera wird Anschläge verhindern können. Vermummte Täter werden sich auch im nachhinein nicht identifizieren lassen. Stattdessen werden unbescholtene Bürgerinnen und Bürger tagtäglich erfasst und gefilmt.
- Die Privatisierung öffentlicher Räume hat bereits zu einem exzessiven Anstieg der Kameraüberwachung geführt. Privat betriebene Örtlichkeiten wie Bahnhöfe oder das Sony Center am Potsdamer Platz werden extensiv mit Kameras überwacht, ohne dass hier ein wirksamer Grundrechtsschutz, insbesondere ein Schutz der Privatsphäre gewährleistet ist.

Videoüberwachung in Berlin! (III)

- Die nunmehr geplante Regelung der rot-roten Koalition öffnet mit ihren windelweichen Formulierungen die Tür zur polizeilichen Überwachung aller verbliebenen öffentlichen Bereiche. In den Wind geschlagen werden offenbar die Warnungen zahlreicher Bürgerrechtsvereinigungen und Datenschützer, die vor einer schleichenden Entwicklung zu einer Video-Totalüberwachung warnen.
- Die Koalition verfehlt mit der jetzigen Vorlage auch ihr eigenes Ziel, die Videoüberwachung zu begrenzen. Daher ist es unverständlich und verantwortungslos, wenn die Regierungsparteien im Abgeordnetenhaus drängen, das Gesetz noch vor der Sommerpause zu beschließen.
- Die Humanistische Union appelliert an alle Parteien, die Vorlage sorgsam zu prüfen und steht für bürgerrechtliche Expertisen gern zur Verfügung."

Alles Gute kommt von oben!

Washington D.C.
Smithsonian Institution Castle
1000 Jefferson Drive SW

24 mm Linse

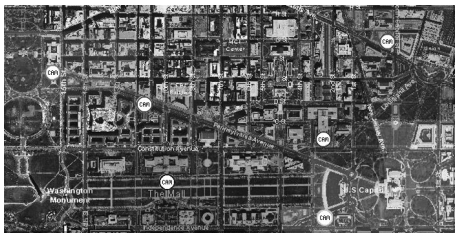
Washington D.C.
Smithsonian Institution Castle
1000 Jefferson Drive SW
(II)

90 mm Linse 180 mm Linse 400 mm Linse

Washington D.C.
Smithsonian Institution Castle
1000 Jefferson Drive SW
(III)

600 mm Linse

Washington D.C.
Smithsonian Institution Castle
1000 Jefferson Drive SW (IV)



The different color CAM-icons and corresponding color-shaded areas indicate the location of DC Metropolitan Police Department surveillance cameras and their proposed areas of coverage as noted in the *Washington Post* on March 23, 2002.

Kennzeichen D

- Historischer Rückblick der Kameraüberwachung in der BRD
  - In München wurden ab 1958 siebzehn Verkehrsschwerpunkte mit Kameras überwacht.
  - Für die Industrie- und Luftfahrtmesse in Hannover kam 1959 eine Fernsehanlage zur Verkehrsüberwachung zum Einsatz.
  - 1960 kamen die ersten mobilen (an Hubschraubern installierten) Kameras zum Einsatz.
  - 1964 wurde der Münchner Polizei die erste mobile Fernsehaufnahme-Anlage übergeben. Sie sollte Beobachtungen bei "größeren Menschenansammlungen", Aufmärschen, Versammlungen, Streiks, Krawallen u. Ä. machen.

Kennzeichen D (II)

- 1976 war Hannover ebenfalls die erste Stadt, in der 25 Kameras, schwenkbar und mit Zoom ausgestattet, im Dauereinsatz waren.
- In der zweiten Hälfte der 70er Jahre, während der Fahndung nach der RAF, wurden in 30-km Umkreis des NATO-Hauptquartiers bei Heidelberg versteckte Hochleistungskameras aufgebaut.
- Anfang der 80er Jahre wurden am "eisernen Vorhang" automatische Kameras in Grenzkontrollbereichen installiert.
- Ende der 80er Jahre wurden an der nach Osten verlagerten Grenze ein neuer elektronischer Vorhang bzw. Schutzwall errichtet. An der Grenze zu Polen und Tschechien sollen Lichtschranken, Bewegungsmelder - und vor allem - Infrarot- und Videokameras illegale Grenzübertritte anzeigen.

Kennzeichen D (III)

- 1996 führte die Stadt Leipzig einen Modellversuch zur "Videoüberwachung von Kriminalitätsschwerpunkten" durch, der mittlerweile feste Einrichtung geworden ist!

- Quelle und mehr Info:
  Augen der Macht - Teil 1: Ein allgemeiner Überblick über Videoüberwachung in der Bundesrepublik
  von Thomas Brunst und Tilman Boller, (Juni 1999) bei www.safercity.de

Wichtige Funktionselemente

- Managementsystem:
  - Integration der Bedien- und Steuerelemente; Verknüpfung von Video-, Gefahrenmelde-, Brandmelde- und Zutrittskontrollanlagen
  - Weitere Integration von Löschmittelanlagen & Gebäudeleittechnik
  - Einbindung von Telefon- und Notrufanlagen
  - ATM schafft Bandbreite nach Bedarf, zeichnet sich durch skalierbare Übertragungskanäle aus, hat eine Broadcast-Funktion und ist hochgradig auslastbar.

Wichtige Funktionselemente (II)

- Aufnahme:
  - CCD-Kameras/Dome-Kameras
  - Manuell oder Auto-Tracking
  - Verknüpfung von Farbbild/Ton & Alarm
  - Aufnahme nur im Falle ungewöhnlicher Aktionen

- Bildanalyse:
  - Objekterkennung, -klassifikation
  - Bewegungserkennung; auch charakteristischer Bewegungen
  - Objektverfolgung in einer Szene (Tracking)

Wichtige Funktionselemente (III)

- Biometrie:
  - Marktreife Verifikationssysteme werden derzeit nur von deutschen und amerikanischen Unternehmen angeboten (Gesichtserkennung):
  - Plettac electronics, ZN-Bochum, DCS, Visionics
- Fernwirken:
  - Steuernde Eingriffe durch Mensch und/oder System

Einschätzungen (I)

- Videoüberwachung ist alltäglich präsent: zum Gebäudeschutz, zur Verkehrskontrolle und -Regelung, zur Absicherung von Einkaufspassagen …
- Die Videoüberwachung wird als „Wundermittel" gegen Kriminalität, „Vandalismus" und andere Regelverstöße propagiert.
- Zunehmend finden die diffusen Ängste der Bevölkerung ihren Niederschlag in sicherheitspolitischen Überlegungen: „Um neue Polizeipraktiken, härtere Kontrollmaßnahmen sowie Strafverschärfungen zu fordern oder zu legitimieren, wird nicht mehr auf ein wie auch immer begründetes objektives Problem rekurriert, sondern auf subjektive Befindlichkeiten." (Ronneberger u.a.)

Einschätzungen (II)

- Diese Vorgehensweise fällt auf einen fruchtbaren Boden: Längst befindet sich die Videoüberwachung nicht mehr nur in den Händen des Staates sondern stellt auch einen florierenden Wirtschaftszweig dar.
- Dazu kommen kulturelle Veränderungen wie der „universellen Voyeurismus" (P. Virilio) der Webcams und BigBrother Container, ganz zu schweigen von den neuen technischen Möglichkeiten.

Einschätzungen (III)

- Eigentlich geht es darum, dass die Videoüberwachung ein wichtiges Element bei der „Umformatierung" der Stadt zu einem idealen Wirtschafts- und Tourismusstandort darstellt. Armut und jedwede Form von „Fehlverhalten" sollen als „Vebrechen gegen die Lebensqualität" an die Stadtränder gedrängt werden, denn wie der Hauptverband des deutschen Einzelhandels feststellte: „Für die Geschäftsleute in den betroffenen Innenstädten stellt die Massierung solcher Verhaltensweisen eine wirtschaftliche Bedrohung dar."
- Aus dieser Perspektive ist die Privatisierung innenstädtischer Bereiche eine effektive Antwort, denn mit der Privatisierung gilt das Hausrecht des Besitzers. Dieser kann seinen Besitz auf ihm genehme Art kontrollieren. Dabei sind die Übergänge zwischen öffentlichen Plätzen und Privateigentum nicht immer klar ersichtlich siehe z.B. den Katharinenhof in Bremen.

Einschätzungen (IV)

- Die Videoüberwachung entzieht sich durch ihre entpersonalisierte Form einer direkten Konfrontation und vielleicht auch der Wahrnehmung. Sie ermöglicht durch ihre „unsichtbare" Kontrolle den Abbau von sichtbaren Sperren, Zäunen und Mauern, wodurch sie der kontrollierten Stadt ein vermeintlich „freiheitliches Aussehen" (G. Deleuze) gibt.
- Die Beobachtung des öffentlichen Raumes wird sich vermehrt auf dessen Zugänglichkeit bzw. Ausschlussmechanismen auswirken, nicht nur durch die erweiterten Möglichkeiten der verwendeten Technologie sondern auch durch die Interpretation der Beobachter: durch eine allgegenwärtige Beobachtung wird jede, auf den Video-Monitoren dargestellten Bewegung zu einem potentiellen Regelverstoß.

Einschätzungen (V)

- Da jeder Mensch in der Öffentlichkeit Objekt dieser Überwachung ist, kann er nur durch unauffälliges, konformes Verhalten - also einer Kontrolle seiner selbst - einer möglichen Verdächtigung entgegenwirken.
- Die dauerhafte und flächendecke Videoüberwachung ist nur eine von vielen möglichen technischen Kontrollformen. Die stetige Verbesserung von Informations- und Kommunikationstechnologien, deren Einsatz zudem immer weniger kostet, stellt auch ein enormes Entwicklungspotential für die Möglichkeiten der Kontrolle und Überwachung dar.
- Ob und wie diese Technologien zukünftig eingesetzt werden ist jedoch weder eine Frage des Schicksals, noch der Sachzwänge, sondern eine politische Entscheidung auf die in vielfältiger Form Einfluss genommen werden kann und muss.

Rechtliche Einhegung

- Die bisherige Überwachung ist ohne gesetzliche Regelung entstanden und erst spät als besonderes verfassungs- und datenschutzrechtliches Problem wahrgenommen worden.
- Für das Versammlungsrecht sind 1989 mit den §§ 12a, 19a VersG erste Befugnisnormen geschaffen worden.
- Im Mai 2001 folgte mit § 6b BDSG eine Vorschrift, die die Beobachtung und Aufzeichnung im öffentlichen Raum einer sehr knappen und wenig aussagefähigen Regelung zugeführt hat. Die Vorschrift ist für Bundesbehörden und Private anwendbar.
- Daneben bestehen Überwachungsbefugnisse des Bundesgrenzschutzes nach den § 26 Abs. 1, 2 und § 27 Abs. 1 i. V. m. §§ 23 Abs. 1 Nr. 2, 28 Abs. 2 Nr. 2 BGSG in Luftverkehrs- und Eisenbahneinrichtungen, an Amtssitzen von Verfassungsorganen und Bundesministerien, an Grenzschutzeinrichtungen, Grenzübergangstellen und Ansammlungen.

Rechtliche Einhegung (II)

- Die Länder haben eigenständige Regelungen getroffen, die fast ausnahmslos im Polizei- und Ordnungsrecht zu finden sind. Präventivpolizeiliche gesetzliche Regelungen finden sich u.a. in den Ländern Baden-Württemberg, Bayern, Berlin, Hessen, Mecklenburg-Vorpommern, Niedersachsen und Schleswig-Holstein.
- In jüngerer Zeit machen vor allem die Städte von den neu geschaffenen Ermächtigungen Gebrauch.
- Größere Vorhaben laufen in Hannover, Hamburg, München, Leipzig und Berlin.

Rechtliche Einhegung (III)

- Im Rahmen der Strafverfolgung gehört die Bild- und Videoüberwachung seit langem zu den Standardinstrumenten.
- Dieser Einsatz beruht auf den §§ 81b und 100c StPO. § 81b StPO sieht offene, mit Kenntnis der betroffenen Personen hergestellte Aufzeichnungen vor, § 100c StPO eine verdeckte Vorgehensweise gegen ausgewählte Zielpersonen, gegen die ein Anfangsverdacht vorliegt.
- Nur ausnahmsweise dürfen andere Personen einbezogen werden. Soweit Aufzeichnungen erkennungsdienstlichen Zwecken dienen, sind sie auch präventiv verwendbar (§ 491 StPO).

§ 6b BDSG

- An dies Stelle kann ich leider nicht auf die gesetzlichen Regelungen im Einzelnen eingehen. Eine herausragende Übersichtsdarstellung stammt vom Hessischen Datenschutzbeauftragten Prof. Dr. Friedrich von Zezschwitz unter http://www.datenschutz.hessen.de/o-hilfen/VideoverfassFragen.pdf
- Hier wollen wir speziell die Neuregelung der Videoüberwachung im BDSG (Mai 2001) im § 6b unter die Lupe nehmen.

§6b BDSG (II)

- Das neue BDSG trat am 23.05.2001 mit einer Videoregelung in § 6b in Kraft.
- Sie zwingt zu einer Totalrevision der bisherigen Überwachungspraxis. Die Überwachungszwecke müssen präzise festgelegt werden. Es muss ein Hinweis in der Öffentlichkeit erfolgen. Nur in begründeten Sicherheitsfällen ist eine Zweckänderung zulässig.
- Im Fall der Identifizierung von Einzelpersonen sind diese zu benachrichtigen.
- Eine frühestmögliche Löschung wurde zur Pflicht. Dessen ungeachtet hat sich kurzfristig keine wesentliche Veränderung in der Praxis feststellen lassen.
- Dies gilt v.a. für die Pflicht zum Kenntlichmachen (§ 6b Abs. 2 BDSG). Dieses Vollzugsdefizit liegt nicht nur an der mangelnden Bekanntgabe des neuen BDSG allgemein und dessen § 6b im Speziellen.

§6b BDSG (III)

Vollzugsdefizit: Hinweispflicht

- Das feststellbare Vollzugsdefizit ist wohl zu erklären mit bisher ungenügenden Kontrollen durch die Datenschutz-Aufsichtsbehörden.
- Eine Ursache mangelnden Respekts vor der Hinweispflicht liegt aber sicher auch daran, dass die Betreiber bei einem Verstoß keine spürbaren Sanktionen befürchten müssen.
- Tatsächlich hat der Gesetzgeber vergessen, den Verstoß gegen § 6b Abs. 2 BDSG in den Bußgeldkatalog des § 43 BDSG aufzunehmen. Dies ist angesichts der späten Einfügung der Regelung nicht verwunderlich und angesichts der überkomplexen Gesetzestechnik beileibe nicht der einzige handwerkliche Fehler im neuen BDSG.

§6b BDSG (IV)

- Die Aufsichtsbehörden können lediglich das Anbringen von Hinweisen auf die Videoüberwachung als eine technisch-organisatorische Maßnahme nach § 9 BDSG, um „den besonderen Anforderungen des Datenschutzes gerecht" zu werden, nach § 38 Abs. 5 BDSG anordnen.
- Fehlen also Schilder mit den gesetzlich geforderten Hinweisen auf Videoüberwachung, so kann deren Installation per Verwaltungsakt durchgesetzt werden.
- Nicht nur der Vollzug des § 6b BDSG ist ein Problem, sondern auch die Regelung selbst. Diese weist insbesondere folgende zwei Defizite auf:
  - 1. die uferlose Weite der Erlaubnistatbestände und
  - 2. der Verzicht auf die Meldepflicht.

§6b BDSG (V)

Die Legitimation durch mehr als Sicherheit

- Nach § 6b Abs. 1 legitimieren die „Aufgabenerfüllung", das „Hausrecht" oder „berechtigte Interessen für konkret festgelegte Zwecke" den Kameraeinsatz.
- Insbesondere die beiden letztgenannten Begriffe sind derart weit, dass mit ihnen keine vernünftige rechtsstaatliche Begrenzung vorgenommen werden kann. Als zusätzliche Anforderung muss daher verlangt werden, dass die Videoüberwachung der „Gewährleistung von Sicherheit" dient.
- Bis heute konnte niemand ein Beispiel für eine legitime Videoüberwachung vortragen, das nicht auf den Schutz von subjektiven Rechten, also v.a. den Schutz von Personen und Sachen ausgerichtet wäre.

§6b BDSG (VI)

- Egal, wer für die Maßnahme verantwortlich ist: Polizei, öffentliche Stellen, private Sicherheitsdienste, Bahnabfertigungsdienste, Ladenbesitzer - in jedem Fall ist Voraussetzung für die Videoüberwachung, dass gesetzlich geschützte Güter vor Schaden bewahrt oder eine erfolgte Schädigung verfolgt und sanktioniert werden sollen.
- Notwendige und zugleich hinreichende Voraussetzung ist schon heute, dass als Zweck „Sicherheit" angestrebt wird. Die Regelung des § 6b fordert für jeden einzelnen Kameraeinsatz eine Abwägung mit den schutzwürdigen Belangen der Betroffenen.
- Im Rahmen einer grundrechtskonformen Auslegung dieser Norm reduziert sich die Zulässigkeit auf diesen Zweck. Dass dies nicht so im Gesetz steht, hat die ärgerliche Folge, dass weitergehende Gelüste bei den Videosystem-Produzenten und -Betreibern geweckt werden, die diese auch in ihren Hochglanzbroschüren offen präsentieren. Derartige Wünsche können aber bei einer datenschutzgerechten Auslegung des § 6b Abs. 1 BDSG nicht befriedigt werden dürfen.

§6b BDSG (VII)

- Kontrollfragen können dies verdeutlichen: Soll die „Aufgabenerfüllung" z.B. der Bundeswehr es legitimieren, à la „Cityserver" die gesamte Bundesrepublik zu videokartieren?
- Soll der Umstand, dass das „Hausrecht" in einer öffentlichen Ladenpassage bei einem privaten Unternehmer zur Kamerakontrolle genügt, die Aufnahme von Passanten per Webcam und die Übertragung dieser Bilder über das Internet für Werbezwecke legitimieren?
- Den buntesten Vogel schoss der Gesetzgeber mit dem Versuch der Eingrenzung der erkanntermaßen weiten „berechtigten Interessen" ab durch die Forderung nach deren „konkreten Festlegung".
- Wo wird der Zweck „festgelegt"? Jedenfalls nicht bei einer Meldung gegenüber der Datenschutz-Aufsichtsbehörde, denn diese hat der Gesetzgeber unterschlagen!

§6b BDSG (VIII)

- „Werbung" ist ebenso ein berechtigtes Interesse wie z.B. „Spaß haben". Die Betreiber sind die einzigen, die zunächst die Abwägung vornehmen müssen. Diesen werden noch viele andere „berechtigte Interessen" einfallen, die sie dann konkret im Geheimen „festlegen"!
- Videoüberwachung erfolgt nicht gezielt personenbezogen, sondern raumbezogen. Sie ist aber - deshalb ist sie grundrechtsrelevant - mit mehr oder weniger großem Aufwand personenbeziehbar. Die Zwecke bleiben vage.
- Dies hat zur Folge, dass in einer noch nicht direkt personenbezogenen Form massenhaft Daten auf Vorrat erhoben und oft genug auch gespeichert werden. Diese durch Technikeinsatz verursachte Gefährdungslage für das Persönlichkeitsrecht bedarf der Rechtfertigung durch eine Gefährdungslage für andere Rechte. Und präzise diese Gefährdungslage kann mit dem Terminus „Gewährleistung von Sicherheit" eingegrenzt werden.

§6b BDSG (IX)

<u>Für eine Meldepflicht</u>

- Eine noch größere Sünde als bei der materiellen Regelung in Absatz 1 beging der Gesetzgeber mit seinem Verzicht auf die Meldepflicht. Selbst die Datenschutzbeauftragten des Bundes und der Länder verwarfen diesen Vorschlag als nicht praktikabel. Dem gegenüber müssten eigentlich die Gründe für eine Meldepflicht überzeugen:
- Es sollte doch ein generelles Datenschutz-Anliegen sein, flächendeckende Videoüberwachung öffentlicher Räume schon im Ansatz zu verhindern. Dies lässt sich allein mit materiell-rechtlichen Regelungen nur unzureichend bewirken.
- In Anknüpfung an das Transparenzgebot der EU-DSRL kann hier der demokratische Meinungsbildungsprozess wirksam gemacht werden. Um diesen in Gang zu setzen, müssen die BürgerInnen die Möglichkeit erhalten, sich auf dem Weg über die Nachfrage bei der verantwortlichen Stelle oder bei der zuständigen Datenschutzkontrollinstanz genauere Informationen über die Überwachung zu beschaffen.

§6b BDSG (X)

- Die besondere gesamtgesellschaftliche Gefahr von Überwachung liegt darin, dass es durch deren technische Qualität und Vernetzung sowie durch deren quantitative Zunahme zumindest in den besonders von Menschen frequentierten Ballungsräumen immer weniger unbeobachtete Räume gibt.
- Dies kann bis zu einer allgegenwärtigen technischen Beobachtung führen. Eine solche Überwachungsinfrastruktur wäre nach der geltenden Rechtsprechung des Bundesverfassungsgerichtes verfassungswidrig. Unabhängig davon, dass es für die jeweiligen einzelnen Kameraeinsätze eine gute Begründung geben kann, muss eine Gesamtbewertung vorgenommen werden können.
- Als übergreifendes Frühwarnsystem und zur Überprüfung der Normeffizienz der Befugnisregelung könnte mit Hilfe der Meldepflicht ein Überblick über das gesamte Ausmaß der Überwachung hergestellt werden.

§6b BDSG (XI)

- Dieser Überblick kann den Parlamenten als Entscheidungslage zur Verfügung gestellt werden. Zugleich könnten damit Anfragen von besorgten BürgerInnen oder Beschwerden kurzfristig und kompetent beschieden werden.
- Die Datenschutzkontrollinstanzen sind zumeist gesetzlich verpflichtet, regelmäßig Tätigkeitsberichte zu veröffentlichen (z.B. § 26 Abs. 1 BDSG) sowie zu Fragen des Datenschutzes zu beraten (z.B. § 26 Abs. 2, 3 BDSG). Das Rohmaterial hierfür kann aus den Meldungen erlangt werden.
- Durch eine Anzeigepflicht wird der Betreiber einer Videoanlage dazu angehalten, im Einzelfall eine Interessenabwägung durchzuführen.

§6b BDSG (XII)

- Die Vorabkontrolle (Art. 20 EU-DSRL; § 4d Abs. 5 BDSG) sowie Anzeige- und Veröffentlichungspflichten (Art. 21 EU-DSRL) zwingen den Betreiber vor Einrichten eines Überwachungssystems zu einer rationalen Begründung der konkreten Erforderlichkeit.
- Im Rahmen der Vorabkontrolle muss ein Sicherheitskonzept erstellt werden. Wird dies unterlassen und erscheint die Anzeige der Datenschutzbehörde aus datenschutzrechtlichen Gründen problematisch, so kann und wird diese den Einsatz überprüfen und u.U. beanstanden.
- Dem Vorschlag einer Meldepflicht wird nun entgegengehalten, der dadurch verursachte Aufwand sei übermäßig und die bürgerrechtlich positiven Wirkungen seien nicht einschätzbar. Tatsächlich hat die notorische personelle Unterbesetzung und die Mittelknappheit bei den Datenschutz-Aufsichtsbehörden zur Folge, dass diese mit ihren Ressourcen so effektiv wie möglich haushalten.

§6b BDSG (XIII)

- Zugegeben ist auch, dass datenschutzrechtliche Registrier- und Meldepflichten bisher hohen Aufwand und wenig bürgerrechtlichen Nutzen brachten. Dieser hohe Aufwand bei ungenügendem Nutzen sämtlicher bisherigen Meldepflichten basierte u.a. darauf, dass nicht die technischen Möglichkeiten genutzt wurden, die im Interesse von Transparenz und Bürgerrechtsschutz möglich wären.
- Wer den Aufwand und die Kosten der Installierung einer Videokamera nicht scheut, den dürfte der Zusatzaufwand des Ausfüllens und des Versendens eines Formulars nicht schrecken, in dem lediglich folgende Angaben gemacht werden müssen: Name und Adresse des Betreibers der Stelle und bzw. des Verantwortlichen, Standort, Zweck, Schwenk- und Zoombarkeit, Vernetzung (Datenempfänger), automatisierte Auswertungsformen, Dauer der Bildaufbewahrung.

Video-Ausblick

Ausblick und Überblick

- Der wesentliche rechtliche Aspekt bei der normativen Einhegung von Videoüberwachung muss darin gesehen werden, dass Videoüberwachung das Pilotprojekt für die anlasslose technische Überwachung potenziell der gesamten Bevölkerung ist.

Shooting back ...

The Institute for Applied Autonomy

Shooting back (II)

Thesen zur Modernisierung des Datenschutzrechts

Für eine Modernisierung ...

- In ihrem Gutachten (Auftrag vom BMI) beschreiben Alexander Roßnagel, Andreas Pfitzmann und Hanjürgen Garstka eine auf die
  4. (grundlegende) Novelle ausgerichtete *Modernisierung des Datenschutzrechtes*.
- Das Gutachten (09/2001) ist beim Bundesministerium des Innern erhältlich unter:
  - http://www.bmi.bund.de/downloadde/11659/Download.pdf

Allgemeine Grundsätze

- Datenschutz ist *Grundrechtsschutz* und *Funktionsbedingung eines demokratischen Gemeinwesens*. Er ist notwendiger Bestandteil einer *freiheitlichen Kommunikationsordnung*.
- Teilhabe und Teilnahme an demokratischer Willensbildung und einem freien Wirtschaftsverkehr sind nur zu erwarten, wenn jeder Teilnehmer sein Handeln auf freier Willensbildung gründen kann. Diese ist nur möglich, wenn die Erhebung und Verwendung von Daten über ihn grundsätzlich seiner freien Selbstbestimmung unterliegt.
- Datenschutz ist ein wichtiger Akzeptanzfaktor der Informationsgesellschaft. Seine rechtliche Gestaltung beeinflusst die Entwicklung einer modernen Wirtschaft. Er ist der entscheidende Vertrauensfaktor, der es ermöglicht, in der Informationsgesellschaft personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen.

Allgemeine Grundsätze (II)

- Diesen Grundsätzen trägt das bisherige Datenschutzrecht in Deutschland nur bedingt Rechnung. Es ist immer noch zu sehr auf das Konzept der räumlich abgegrenzten Datenverarbeitung fixiert, nimmt neue Formen personenbezogener Daten und deren Verarbeitung nur ungenügend auf und berücksichtigt unzureichend die Gefahren und Chancen neuer Techniken der Datenverarbeitung.
- Darüber hinaus ist es in seinen Formulierungen häufig widersprüchlich und durch seine Normierung in hunderten von speziellen (vorrangigen) Gesetzen unübersichtlich und schwer zu handhaben.

Allgemeine Grundsätze (III)

- Die positiven Erwartungen an das Datenschutzrecht und die Unzulänglichkeit der bisherigen Regelungen aufnehmend, soll ein modernes Datenschutzrecht geschaffen werden, das zum Einen einfacher und verständlicher und zum Anderen angesichts neuer Formen der Datenverarbeitung risikoadäquat ist.
- Um das erste Ziel zu erreichen, müssen die Selbstbestimmung der betroffenen Person gestärkt und die Selbstregulierung und Selbstkontrolle der Datenverarbeiter ermöglicht und verbessert werden.
- Um das zweite Ziel zu erreichen, müssen vor allem Konzepte des Selbstdatenschutzes und des Systemdatenschutzes umgesetzt werden.

Weniger Spezialregelungen!

- Ein modernes Datenschutzrecht sollte auf einem allgemeinen Gesetz gründen, das bereichsspezifischen Regelungen vorgeht. Dieses enthält grundsätzliche und präzise Regelungen der Verarbeitung personenbezogener Daten und vermeidet möglichst offene Abwägungsklauseln.
- Das Gesetz soll darüber hinaus auch allgemeine Regelungen zur Technikgestaltung, zur Datensicherung, zur Datenschutzorganisation, zur Datenschutzkontrolle und zur Selbstregulierung enthalten.
- Wird die Vorrangregelung im Verhältnis zwischen BDSG und bereichsspezifischen Regelungen umgedreht, können die bisherige Normenflut und Rechtszersplitterung verringert und Widersprüche vermieden werden.

Weniger Spezialregelungen! (II)

- Spezialregelungen in bereichsspezifischen Gesetzen sollten nur Ausnahmen von den allgemeinen Regelungen enthalten und nur für bestimmte riskante Datenverarbeitungen die Anforderungen verschärfen oder bei unterdurchschnittlich riskanten Datenverarbeitungen
- Erleichterungen bieten. Auch könnten Ausnahmen vorgesehen werden, wenn Aufgaben im Allgemeininteresse ansonsten nicht erfüllt werden können.
- Alle Ausnahmen sind als explizite Durchbrechungen der allgemeinen Prinzipien durch Formulierungen wie „... in Abweichung von § X BDSG ..." kenntlich zu machen.

Weniger Spezialregelungen! (III)

- Das Telekommunikations- (§§ 85 und 89 TKG und TDSV) und Teledienstedatenschutzrecht (TDDSG) sollten in das BDSG integriert werden.
- Dies entspricht der Bedeutung der Telekommunikation für die Verarbeitung personenbezogener Daten. Dadurch könnten Wertungswidersprüche und Überschneidungen der Anwendungsbereiche beseitigt und eine Vereinheitlichung auf hohem Niveau erreicht werden.
- *Schutzgut* des Datenschutzrechts ist die informationelle Selbstbestimmung, die das Bundesverfassungsgericht als risikoorientierte Ausprägung der Grundrechte in der Informationsgesellschaft entwickelt hat.

Weniger Spezialregelungen! (IV)

- Die allgemeinen Datenschutzgrundsätze sollten gleichermaßen für den öffentlichen und für den nicht öffentlichen Bereich gelten. In beiden Bereichen ist – risiko- und nicht bereichsabhängig – das gleiche Datenschutzniveau zu gewährleisten. Unterschiede sind insoweit zu berücksichtigen, als im nicht öffentlichen Bereich die Regelungsadressaten Grundrechtsträger sind und im öffentlichen Bereich Allgemeininteressen verfolgt werden müssen.
- Die Grundsätze sollten nicht zwischen manueller und automatischer Datenverarbeitung unterscheiden. Die Unterscheidung zwischen Dateien und Akten beschreibt nicht die Grenze zwischen erforderlichem Schutz und irrelevanten Verhaltens-weisen und führt zu unsachlichen Abgrenzungen. Soweit zweckmäßig können einzelne Pflichten auf Dateien oder die automatisierte Datenverarbeitung beschränkt werden.

Weniger Spezialregelungen! (V)

- Juristische Personen sollten in den Schutzbereich des Datenschutzrechts einbezogen werden. Das Grundrecht auf informationelle Selbstbestimmung gilt, soweit nicht gerade sein persönlichkeitsrechtlicher Kern betroffen ist, nach Art. 19 Abs. 3 GG auch für juristische Personen. Auch das Telekommunikations-geheimnis des Art. 10 Abs. 1 GG gilt nach Art. 19 Abs. 3 GG für juristische Personen.
- Daher erstreckt das Telekommunikations-Datenschutzrecht bereits heute seinen Schutz auch auf juristische Personen. Wenn künftig Telekommunikation ein Regelbestandteil der Datenverarbeitung wird und das Telekommunikations-Datenschutzrecht in das BDSG integriert werden soll, können dessen Regelungen weder auf natürliche Personen beschränkt werden, noch kann der personelle Schutzbereich für die Datenverarbeitung in und außerhalb der Telekommunikation unterschiedlich bestimmt werden.

Weniger Spezialregelungen! (VI)

- Darüber hinaus ist die Abgrenzung zwischen Daten natürlicher und juristischer Personen in der Aufsichtstätigkeit ohnehin häufig schwierig oder unmöglich.
- Dateien über juristische Personen enthalten in der Regel auch Daten zu natürlichen Personen. Daher werden die Daten in der Praxis grundsätzlich ohne weitere Differenzierung dem höheren Schutzniveau unterstellt. Die Einbeziehung juristischer Personen wäre somit auch praxisadäquat.

Grundsätze der DV

- Datenschutz soll künftig vorrangig durch Grundsätze der Datenverarbeitung erfolgen, die einerseits ein Mindestschutzniveau beschreiben und andererseits der betroffenen Person Kontroll- und Mitwirkungsmöglichkeiten bieten.
- Daneben kann aber aus europa- und verfassungsrechtlichen Gründen auf gesetzliche Erlaubnisse der Datenverarbeitung nicht verzichtet werden. Diese sollen jedoch erheblich vereinfacht werden.
- Jeder Umgang mit personenbezogenen Daten sollte unter einer *einheitlichen* Bezeichnung erfasst werden. Entsprechend der Europäischen Datenschutzrichtlinie bietet sich die Bezeichnung der *„Verarbeitung"* an.

Grundsätze der DV (II)

- Nicht alle Formen der Datenverarbeitung werden künftig jedoch nach den gleichen Regeln behandelt werden können. Um insbesondere die Datenverarbeitung für das Erbringen technischer Leistungen adäquat regeln zu können, sollte das künftige Datenschutzrecht zwischen *zwei Kategorien der Datenverarbeitung* unterscheiden:
  - Verarbeitung mit *gezieltem Personenbezug* zum Zweck der personenbezogenen oder personenbeziehbaren Verwendung (z.B. Personalakten, Vertragsdaten, Bestandsdaten) und
  - Verarbeitung ohne gezielten Personenbezug zu anderen Zwecken als dem Zweck der personenbezogenen oder personenbeziehbaren Verwendung (z.B. Erbringen technischer Dienstleistungen, Kommunikation von Maschine zu Maschine, „Überschussdaten" bei Suchprozessen)

Grundsätze der DV (III)

- Die Datenverarbeitung *ohne gezielten Personenbezug* betrifft die bereits heute gewaltige Menge von Daten, die für technische Dienstleistungen der Telekommunikation verarbeitet werden muss. Diese wird vervielfacht durch das technische Ermöglichen, im Cyberspace zu handeln. Sie wird potenziert, wenn die unübersehbare Vielfalt des Ubiquitous Computing in der Alltagswelt hinzu kommt.
- Die Anforderungen für die Verarbeitung ohne gezielten Personenbezug sollten risikoadäquat und effizienzsteigernd spezifiziert werden. Sie werden insofern verschärft, als die Daten auf das erforderliche Minimum begrenzt, während ihrer Verarbeitung gegen Zweckentfremdung geschützt und nach der Verarbeitung sofort gelöscht werden müssen. Die Daten sollten außerdem einer strengen Zweckbindung (wie nach § 31 BDSG) unterliegen und durch ein Verwertungsverbot geschützt sein.

Grundsätze der DV (IV)

- Werden diese Anforderungen nicht erfüllt, wird vor allem ein weitergehender Zweck mit diesen Daten verfolgt, gelten für sie von Anfang an alle Anforderungen für die Datenverarbeitung mit gezieltem Personenbezug. Erleichterungen sollten insoweit vorgesehen werden, als auf eine vorherige Unterrichtung der betroffenen Personen verzichtet wird und ein Anspruch auf Auskunft über einzelne Daten für die kurze Zeit ihrer Speicherung nicht besteht.
- Ein solcher Anspruch erscheint kontraproduktiv. Er hätte den unerwünschten Effekt, dass Protokollverfahren oder Data-Mining-Techniken nur deshalb angewendet werden müssten, um die personenbezogenen Daten ausfindig zu machen und zusammenzuführen.
- Die notwendige Transparenz soll durch eine öffentliche und allgemeine Datenschutzerklärung des Datenverarbeiters über die Struktur seines Datenverarbeitungsverfahrens hergestellt werden.

Hohe Transparenz der DV

- Wenn das Datenschutzrecht entlastet und die Regelung des Datenverarbeitungsverhältnisses stärker seinen beiden Parteien überlassen werden soll, muss die Transparenz der Datenverarbeitung gegenüber der betroffenen Person erhöht werden.
- Zielsetzung eines modernen Datenschutzrechts muss es sein, ausreichende Informationen über die Erhebung personenbezogener Daten, über die Umstände und Verfahren ihrer Verarbeitung und die Zwecke ihrer Nutzung für die betroffenen Personen und die Kontrollstellen sicherzustellen.
- Wer geschäftsmäßig personenbezogene Daten automatisiert verarbeitet, sollte verpflichtet sein, die Struktur der Datenverarbeitung in verständlicher Form zu veröffentlichen, soweit dies ohne Offenlegung von schützenswerten Geheimnissen möglich ist.
- Mit angemessenem Aufwand muss überdies durchschaubar sein, was das System einschließlich aller Betriebs- und Anwendungssoftware genau tut.

Stärkung der Selbstbestimmung

- Obwohl in die Informationsgesellschaft kein formelles Verbot der Datenverarbeitung passt, muss dennoch aus verfassungs- und europarechtlichen Gründen die Datenverarbeitung jeweils spezifisch erlaubt werden. Um Datenschutz zu vereinfachen und absurde Ergebnisse zu vermeiden, sollte ein *genereller Erlaubnistatbestand* die Datenverarbeitung immer dann für zulässig erklären, wenn offenkundig keine Beeinträchtigung der betroffenen Person zu erwarten ist.
- Soweit die Datenverarbeitung Interessen der betroffenen Person beeinträchtigen könnte, soll die Entscheidung über diese vorrangig der *Selbstbestimmung der betroffenen Person* überlassen werden.
- Im Einzelfall muss die Datenverarbeitung grundsätzlich durch *Einwilligung* oder Einwilligungssurrogate wie Vertrag und vertragsähnliches Vertrauensverhältnis oder Antrag gegenüber einer Behörde erlaubt werden können.

Stärkung der Selbstbestimmung (II)

- Die Einwilligung ist der genuine Ausdruck des Rechts auf informationelle Selbstbestimmung. Da aber zwischen den betroffenen Personen und den verantwortlichen Stellen in der Regel ein erhebliches Machtgefälle besteht, muss die Selbstbestimmung gestärkt werden.
- Ziel eines modernen Datenschutzrechts muss es daher sein, einerseits die Zulässigkeit der Datenverarbeitung im vertretbaren Umfang durch Rahmenregelungen abzusichern.

Stärkung der Selbstbestimmung (III)

- Grundsätzlich sollte im *nicht öffentlichen Bereich* eine „Opt-in-Lösung" gewählt werden: Die Datenverarbeitung setzt die vorherige Einwilligung der betroffenen Person voraus. Allerdings muss eine Datenverarbeitung auch ohne Einwilligung der betroffenen Person möglich sein.
- Zur Umschreibung dieser Ausnahmefälle ist der bisher die Datenverarbeitung steuernde Begriff des „berechtigten Interesses" zu weit. Ausnahmen sollten nur erlaubt sein, wenn dies zum Schutz oder zur Verfolgung eigener Rechte oder Rechte Dritter notwendig ist, oder wenn es erforderlich ist, um eine Gefahr für Leben, Gesundheit oder sonstige bedeutende Rechtsgüter der betroffenen Person zu beseitigen, und die betroffene Person ihre Zustimmung nicht geben kann, oder wenn die Datenverarbeitung erforderlich ist, um Verpflichtungen zu erfüllen,die durch Rechtsvorschriften der verantwortlichen Stelle auferlegt wurden.

Stärkung der Selbstbestimmung (IV)

- Im öffentlichen Bereich sollte die Datenverarbeitung zulässig sein, wenn sie „zur Erfüllung einer gesetzlich zugewiesenen und in der Zuständigkeit der öffentlichen Stelle liegenden bestimmten Aufgabe erforderlich" ist.
- Soweit es allerdings um Verarbeitungszwecke und -formen geht, die gegen den Willen der betroffenen Person durchgesetzt werden müssen und deren Interessen stark beeinträchtigen können, sollen bereichsspezifische Regelungen die Zwecke und Formen risikoadäquat regeln.
- Die Einwilligung kann im öffentlichen Bereich die Datenverarbeitung im Wesentlichen nur im nicht gesetzlich gebundenen Bereich legitimieren.

Erforderlichkeit der DV & Vermeidung des Personenbezugs

- Soweit für die Zwecke der Datenverarbeitung ein Personenbezug nicht erforderlich ist, muss dieser von Anfang an vermieden oder nachträglich durch Löschung der Daten, ihre Anonymisierung oder Pseudonymisierung beseitigt werden.
- Darüber hinaus sind die verantwortlichen Stellen zu verpflichten, soweit dies technisch möglich und verhältnismäßig ist, ihre Datenverarbeitungsverfahren so zu gestalten, dass sie möglichst keinen Personenbezug und auch keine Personenbeziehbarkeit aufweisen.
- Dieses Ziel kann durch Anonymität oder Pseudonymität der betroffenen Person erreicht werden. Anonymität und anonymitätsnahen Arten von Pseudonymen sollte grundsätzlich Vorrang gegeben werden.

Erforderlichkeit der DV & Vermeidung des Personenbezugs (II)

- Die vorgenannten Grundsätze der Transparenz und der Vermeidung des Personenbezugs können nur durch die betroffenen Personen selbst durchgesetzt werden (Selbstdatenschutz).
- Sie müssen in die Lage versetzt werden, die Nutzung von technischen und organisatorischen Schutzinstrumenten selbst zu bestimmen. Dies sind Instrumente für Inhaltsschutz (Konzelation, Steganographie), Anonymität, Pseudonymität und Identitätsmanagement.
- Programme, die Schlüssel, Identitäten und Pseudonyme verwalten und den Nutzer bei der Verwendung von Selbstschutztechniken unterstützen, müssen gefördert werden.
- Eine Bildungsoffensive zum Umgang mit Instrumenten des Selbstdatenschutzes wäre zu erwägen.

Zweckbegrenzung & Zweckbindung der DV

- Die Zweckbindung bestimmt Ziel und Umfang zulässiger Datenverarbeitung und begrenzt sie zugleich auf diese.
- Eine Verarbeitung personenbezogener Daten darf nur zu bestimmten, in der Einwilligung oder der gesetzlichen Erlaubnis ausdrücklich genannten Zwecken erfolgen.
- Systemdatenschutz kann die technisch-organisatorische Sicherung der Zweckbindung unterstützen: Grundsätzlich sollten die verwendeten Produkte und die eingerichteten Datenverarbeitungsprozesse für die verarbeitenden Personen nur die Maßnahmen zulassen, die dem Zweck der Datenverarbeitung entsprechen.

Zweckbegrenzung & Zweckbindung der DV (II)

- Profilbildungen sind eine besondere Gefahr für die informationelle Selbstbestimmung.
- Gleichwohl sollten sie nicht generell verboten werden. Eine Kombination von Anforderungen könnte den erforderlichen Schutz bieten, wenn dadurch vor allem Transparenz und Einflussnahme für die betroffene Person gewährleistet sind.
- So ist die beabsichtigte Profilbildung als spezifische Form der Datenverarbeitung in der Datenschutzerklärung mit einem Hinweis auf ihre Struktur und ihren Zweck darzustellen. Grundsätzlich muss die Profilbildung von einer ausdrückliche Einwilligung gedeckt sein und die betroffene Person jederzeit die Möglichkeit haben, ihre Einwilligung für die Zukunft zu widerrufen.
- Nur in Ausnahmefällen sollte die Profilbildung durch einen Erlaubnistatbestand legitimiert werden, was allerdings die Unterrichtung und ein Widerspruchsrecht der betroffenen Person voraussetzt.

Organisatorische Unterstützung

- Viele bereits bestehende organisatorische Verpflichtungen der verantwortlichen Stellen sollten zu einem integrierten Datenschutzmanagementsystem zusammengefasst und fortentwickelt werden, um Verantwortlichkeit sicher zu stellen, das Datenschutzbewusstsein zu stärken und eine datenschutzfreundliche Betriebsorganisation zu erreichen.
- Die Bestellung eines Datenschutzbeauftragten, die Erarbeitung eines Plans der Datenschutzorganisation und die Erstellung eines Datenschutz- und Datensicherungskonzepts sind die wesentlichen Bestandteile.

Organisatorische Unterstützung (II)

- Zur Stärkung der Akzeptanz des Datenschutzes und um eine ständige Fortentwicklung entsprechend den sich verändernden und zunehmenden Risiken zu ermöglichen, muss ein modernes Datenschutzrecht auch Anreize für einen effektiven und sich fortentwickelnden Schutz bieten.
- Daher wird den verantwortlichen Stellen die Möglichkeit geboten, mit ihren Anstrengungen zur Implementierung eines effektiven Datenschutzes zu werben. Hierzu gehören insbesondere die vertrauenswürdige Auditierung von Datenschutzmanagementsystemen, die mit Erleichterungen rechtlicher Anforderungen belohnt werden sollte.
- Verantwortliche Stellen, die am Datenschutzaudit teilnehmen, sollten von öffentlichen Stellen außerdem bevorzugt berücksichtigt werden, wenn es um Aufträge zur Verarbeitung personenbezogener Daten geht.
- Mit dem Datenschutzaudit könnte unabhängig von der Novellierung des BDSG noch in dieser Legislaturperiode ein erster Schritt der zweiten Novellierungsstufe realisiert werden.

Datenschutz durch Technik

- Datenschutz muss künftig durch, nicht gegen Technik erreicht werden. Datenschutzrecht muss versuchen, die Entwicklung von Verfahren und die Gestaltung von Hard- und Software am Ziel des Datenschutzes auszurichten und die Diffusion und Nutzung datenschutzgerechter oder -fördernder Technik zu fördern.
- Datenschutz sollte so weit wie möglich in Produkte, Dienste und Verfahren integriert sein. Adressaten des Datenschutzrechts können daher nicht mehr nur die für die Datenverarbeitung verantwortlichen Stellen sein.
- Das Datenschutzrecht muss bereits bei der Entwicklung der Technik Einfluss auf deren Gestaltung nehmen. Es muss datenschutzgerechte Technik fordern und fördern. Zu diesem Zweck sollten zumindest drei Regelungen vorgesehen werden. Die Hersteller sollten verpflichtetet werden, für die Gestaltung ihrer Produkte zumindest die Erfüllung einiger zentraler Produktanforderungen zu überprüfen.

Datenschutz durch Technik (II)

- Wer datenschutzgerechte Produkte herstellt, sollte die Möglichkeit erhalten, diese zertifizieren zu lassen und mit dem Zertifikat werben zu können.
- Schließlich sollten die verantwortlichen Stellen aufgefordert werden, datenschutzgerechte Produkte zu verwenden. Zumindest für öffentliche Stellen sollte dies zu einer gesetzlichen Pflicht erhoben werden.

Gesellschaftliche Selbstregulierung

- Konkretisierungen der gesetzlichen Grundsätze können durch branchen- oder unternehmensspezifische Selbstregulierung erfolgen.
- Um in dieser ein faires Verfahren, einen angemessenen Interessen-ausgleich, die Berücksichtigung von Gemeinwohlinteressen und eine gewisse demokratische Legitimation zu gewährleisten, muss der Gesetzgeber auch für diese Regelsetzung einen gesetzlichen Rahmen vorgeben.
- Selbstregulierung ermöglicht es der Wirtschaft, relativ schnell passgerechte branchen- oder unternehmensbezogene verbindliche Regelungen zu entwickeln, die die schnelle Entwicklung der Technik, die Komplexität ihrer Systeme und die Vielfalt ihrer Anwendungen berücksichtigen.
- Der entscheidende Anreiz für Branchen, Verbände oder Unternehmen, eigene, durch Kontrollstellen anerkannte Verhaltensregeln zu erstellen, besteht in der Möglichkeit, die zu konkretisierenden Gesetzesvorgaben selbständig und auch für die Kontrollstellen verbindlich auszugestalten.

Gesellschaftliche Selbstregulierung (II)

- Die Selbstregulierung könnte beispielsweise Konkretisierungen der Erlaubnistatbestände „Verfolgung und Schutz eigener Rechte oder Rechte Dritter“ sowie der Erforderlichkeit bestimmter Daten für bestimmte Zwecke zum Inhalt haben.
- Andere Beispiele wären die brancheneinheitliche Festlegung notwendiger Vertragsdaten, von Grundsätzen für die branchenspezifische Unterrichtung betroffener Personen oder von branchenspezifischen Datenschutzerklärungen.
- Ebenso könnten Verfahren anonymen und pseudonymen Handelns festgelegt oder die Einrichtung branchenspezifischer Schlichtungsverfahren vorgesehen werden.
- Schließlich wäre an die Erarbeitung einheitlicher Einwilligungserklärungen zu denken.
- Die Selbstregulierung sollte auf einen gesellschaftlichen Konsens, nicht auf die einseitige Durchsetzung der Interessen eines Verbands zielen. Daher sollten sich anerkannte Datenschutz- und Verbraucherverbände an der Selbstregulierung beteiligen können.

Gesellschaftliche Selbstregulierung (III)

- In diesem Zusammenhang sollte das Gesetz der Bundesregierung die Möglichkeit bieten, für die freiwillige Erfüllung von Anforderungen zur Vorsorge gegen Risiken für die informationelle Selbstbestimmung formell Zielfestlegungen zu treffen, die innerhalb einer bestimmten Frist erreicht werden sollen.
- Diese ermöglichen es, Prioritäten zu setzen und die Richtung der Politik zu bestimmen. Die Zielfestlegung wirkt entweder normvermeidend, wenn die Ziele freiwillig erfüllt werden oder sie wirkt normvorbereitend, indem sie die künftigen Regelungsadressaten bereits auf die Regelung „einstimmt“.
- Nach Ablauf der vorgegebenen Frist wäre zu prüfen, ob und welche gesetzgeberischen Maßnahmen zu ergreifen sind.

Stärkung der Betroffenenrechte

Betroffenenrechte bieten eine wesentliche Stütze für einen effektiven Datenschutz nur, wenn sie von den Betroffenen auch tatsächlich wahrgenommen werden und wahrgenommen werden können.

- Die betroffenen Personen müssen ihre Rechte frei und unbehindert sowie unentgeltlich ausüben können, ohne Zwang, dies zu tun oder nicht zu tun.
- Betroffenenrechte sollten wenn möglich nur im allgemeinen Datenschutzgesetz geregelt und möglichst knapp und einfach formuliert werden, damit auch die Betroffenen selbst sie verstehen. Sie sind ausdrücklich für unabdingbar zu erklären und dürfen nicht durch Rechtsgeschäft ausgeschlossen werden können.
- Die Unterscheidung zwischen öffentlichen und nicht öffentlichen Stellen ist auch bezüglich der Betroffenenrechte aufzugeben. Im Rahmen der Online-Kommunikation sollten die betroffenen Personen ihre Rechte auch telekommunikativ wahrnehmen können.
- Die betroffene Person sollte bereits vor der Datenerhebung über ihre Rechte informiert werden. Die Informations- und Unterrichtungspflichten sind daher entsprechend auszuweiten.

Stärkung der Betroffenenrechte (II)

- Die Auskunft sollte umfassend erfolgen und sich je nach Anforderung der betroffenen Person auf alle Aspekte der Datenverarbeitung erstrecken. Insbesondere gehören hierzu Angaben
  - zu den gespeicherten Daten selbst,
  - zu deren Herkunft,
  - zu den Empfängern der Daten und Teilnehmern eines automatisierten Abrufverfahrens,
  - zum Zweck der Datenverarbeitung,
  - Zum Auftragnehmer bei Datenverarbeitung im Auftrag und
  - zum Dienstleister bei Outsourcing,
  - Wie auch Angaben über die erfolgte Berichtigung, Löschung oder Sperrung von Daten,
  - über den Aufbau, die Struktur und den Ablauf der automatisierten Datenverarbeitung, insbesondere
  - über Profilbildungen und deren Struktur.
- Ausnahmen von der Auskunftspflicht sollten auf wenige unabdingbaren Fallkonstellationen reduziert werden.

Stärkung der Betroffenenrechte (III)

- Jede betroffene Person kann den betrieblichen oder behördlichen Datenschutzbeauftragten als Beschwerdeinstanz anrufen. Er soll auf eine gütliche Lösung zwischen der verantwortlichen Stelle und der betroffenen Person hinwirken und innerhalb eines Monats eine schriftliche und mit Gründen versehene Antwort auf die Beschwerde abgeben.
- Der betroffenen Person sollte ein Recht zum Widerspruch, wie es auch von Art. 14 a) DSRL gefordert wird, eingeräumt werden.
- In Abgrenzung zum Widerspruch nach § 69 VwGO sollte es „Einwand" genannt werden. Es bietet der betroffenen Person die Möglichkeit, gegen eine auf der Basis eines Erlaubnistatbestands an sich rechtmäßige Datenverarbeitung ihren abweichenden Willen geltend zu machen.

Stärkung der Betroffenenrechte (IV)

- Nicht nur für öffentliche, sondern auch für nicht öffentliche Stellen, die geschäftsmäßig automatisiert Daten verarbeiten, sollte aufgrund des vergleichbaren Risikopotenzials ebenfalls eine Gefährdungshaftung vorgesehen werden.
- Um den Vollzug der Datenschutzregelungen zu unterstützen, sollte jedoch die *Gefährdungshaftung* entfallen und an ihre Stelle die allgemeine Haftungsregelung treten, wenn die verantwortliche Stelle nachweist, dass sie für den Zeitraum, in dem die Regelverletzung erfolgt sein kann, alle Anforderungen des Datenschutzmanagements erfüllt hat, oder am Datenschutzaudit teilnimmt.
- Neben materiellen Schäden sollten auch immaterielle Schäden anerkannt werden, wenn sie auf schweren Verletzungen des Persönlichkeitsrechts beruhen. Sie sind bei einer Verarbeitung personenbezogener Daten das eigentliche Risiko.

Stärkung der Betroffenenrechte (V)

- Ebenso sollte der Kausalitätsnachweis erleichtert werden. Wenn die betroffene Person die Rechtswidrigkeit oder Unrichtigkeit der Datenverarbeitung sowie Umstände des Einzelfalls belegt, die eine ganz überwiegende Wahrscheinlichkeit für die Ursächlichkeit des entstandenen Schaden begründen, soll die verantwortliche Stelle nachweisen müssen, dass ihr Fehler den Schaden nicht verursacht haben kann.
- Diese Beweismaßreduzierung trägt den Besonderheiten durch Datenverarbeitung verursachter Schäden Rechnung, bei denen eine vollständige Überzeugung des Gerichts hinsichtlich des Vorliegens der haftungsbegründenden Kausalität typischerweise nicht erreicht werden kann.
- Die Ursachenvermutung wird regelmäßig dann nicht eingreifen, wenn die verantwortliche Stelle nachweist, dass sie alle Anforderungen an ihr Datenschutzmanagement erfüllt hat. Der Nachweis kann auch durch die erfolgreiche Teilnahme am Datenschutzaudit erfolgen.

Effektive Datenschutzkontrolle

- Die Datenschutzkontrolle sollte für den öffentlichen und nicht öffentlichen Bereich einschließlich der Telekommunikation, Mediendienste und Rundfunkanstalten zusammengeführt werden.
- Hierfür bieten sich der Bundes- und die Landesbeauftragten an. Eine solche Vereinheitlichung der Kontrollstellen entspricht der Europäischen Datenschutzrichtlinie und führt zu wünschenswerten Synergieeffekten.
- Überdies erleichtert eine Vereinheitlichung es den Betroffenen, ihre Anrufungsrechte wahrzunehmen.

Effektive Datenschutzkontrolle (II)

- Im Sinn einer völligen Unabhängigkeit der Kontrollstellen nach Art. 28 DSRL sollte die Rechtsaufsicht über die Kontrollstellen sowohl für den öffentlichen wie auch für den nicht öffentlichen Bereich neu überdacht werden.
- Rechtsaufsicht ist immer mit einer Einflussnahme auf die Amtsführung der beaufsichtigten Stelle verbunden. Die Einführung der Initiativkontrolle auch im nicht öffentlichen Bereich führt überdies zu einem weitergehenden Eingriff in die Privatsphäre von Unternehmen und legt eine Kontrolle über diese durch unabhängige,nicht in die Ministerialverwaltung eingebundene und von ihr kontrollierte Stellen nahe.
- Die notwendige demokratische Legitimation der Kontrollstellen erfolgt – wie auch heute schon – durch die Wahl der Amtsinhaber durch die Parlamente und ihre Berichtspflicht gegenüber diesen.
- Zur Klarstellung der Unabhängigkeit wäre eine Einrichtung des Bundesbeauftragten als oberste Bundesbehörde wünschenswert.

Effektive Datenschutzkontrolle (III)

- Die Durchsetzungskompetenzen der Kontrollstellen müssen gestärkt werden. Ihnen müssen wirksame Einwirkungsbefugnisse in die Hand gegeben werden.
- Bei Nichtbeachtung von Beanstandungen gegenüber öffentlichen Stellen sollte den Datenschutzbeauftragten der Verwaltungsrechtsweg eröffnet werden.
- Gegenüber nicht öffentlichen Stellen müssen die Kontrollstellen mit der Befugnis ausgestattet werden, die Sperrung, Löschung oder Vernichtung von Daten, die widerrechtlich verarbeitet wurden, durch Verwaltungsakt anzuordnen. Sie sollten darüber hinaus über eine umfassende Strafantragsbefugnis verfügen.
- Eine Erziehungsfunktion gegenüber Personen, die durch die Nichtbeachtung datenschutzrechtlicher Vorschriften eine Ordnungswidrigkeit oder Straftat begangen haben, könnte ein verpflichtender Datenschutzunterricht erfüllen, in dem Kenntnisse im Datenschutz vermittelt werden.

Effektive Datenschutzkontrolle (IV)

- Die in Art. 28 Abs. 2 DSRL vorgesehene Anhörung der Kontrollstellen bei der Ausarbeitung von Rechtsverordnungen oder Verwaltungsvorschriften, die die Verarbeitung personenbezogener Daten betreffen, sollte als Verpflichtung der entsprechenden Stellen zur Konsultation des Bundesbeauftragten ausgestaltet werden.
- Die Stellung der *betrieblichen und behördlichen* Datenschutzbeauftragten muss gestärkt werden. Ihre Weisungsfreiheit und Unabhängigkeit sollte durch einen verstärkten Kündigungsschutz unterstützt werden, der sich an dem für Mitglieder der Mitarbeitervertretung orientiert.
- Lediglich natürliche Personen sollten als Datenschutzbeaftragte bestellt werden können. Externe Datenschutzbeauftragte sollten nur noch für einen Mindestzeitrahmen von fünf Jahren bestellt werden dürfen, um eine Umgehung des Kündigungsschutzes zu verhindern.

Effektive Datenschutzkontrolle (V)

- Die Anforderungen an Fachkunde und Qualifikation sowie die sachliche und personelle Ausstattung der Beauftragten sollten näher beschrieben werden. Das Verhältnis zwischen Datenschutzbeauftragtem und Mitarbeitervertretung muss geklärt werden.
- Ein neues BDSG sollte auch die Funktion eines Konzerndatenschutzbeauftragten aufnehmen. Dies würde zu wünschenswerten Synergieeffekten führen und die Rolle des Datenschutzes im gesamten Konzernverbund stärken.
- Einem vom deutschen Datenschutzrecht sanktionierten Konzerndatenschutzbeauftragten wird es darüber hinaus in weltweit tätigen Konzernen leichter fallen, Datenschutzgrundsätze im gesamten Konzern durchzusetzen.

Effektive Datenschutzkontrolle (VI)

- Datenschutz könnte künftig auch durch eine gesellschaftliche Kontrolle unterstützt werden.
- So sollten im Rahmen des unlauteren Wettbewerbs Konkurrentenklagen bei Datenschutzverstößen ermöglicht werden.
- Ebenso sollte anerkannten Verbänden des Verbraucher- und Datenschutzes ein Verbandsklagerecht eröffnet werden.

Informationelle Selbstbestimmung als Grundrecht stärken

- Die Modernisierung des Datenschutzrechts würde unterstützt, wenn flankierend die informationelle Selbstbestimmung als Grundrecht der Informationsgesellschaft in das Grundgesetz (explizit) aufgenommen würde.
- Das Grundrecht sollte nicht allein persönlichkeitsrechtlich gefasst, sondern als Kommunikationsgrundrecht ausgestaltet werden, das als Querschnittsgrundrecht den kommunikativen Gehalt aller Grundrechte zum Ausdruck bringt.

Zur Information: № 7

- Themennahe Veranstaltungen in Berlin:
  - http://waste.informatik.hu-berlin.de/peter/lehre/i+g_ss2002/i+g_ss2002.html#events

Zur Einstimmung auf die nächste Vorlesung

Thema Arbeitswelt/New Economy:

- Wie empfinden Sie ihren Bildschirmarbeitsplatz?
- Glauben Sie, dass der Einsatz von IT die Produktivität steigert?