Datenschutzbericht 1995/96

Die Landesbeauftragte
für den Datenschutz
Nordrhein-Westfalen

Dreizehnter Datenschutzbericht

der

Landesbeauftragten für den Datenschutz

Nordrhein-Westfalen

Bettina Sokol

für die Zeit vom 1. Januar 1995
bis zum 31. Dezember 1996

Herausgeberin: Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen
Postfach 20 04 44, 40102 Düsseldorf,
Telefon: (0211) 38 42 4-0,Telefax: (0211) 38 42 41 0,
E-Mail: mailbox@lfd.nrw.de
ISSN: 0179-2431
Druck: Neusser Druckerei und Verlag GmbH
Düsseldorf 1997

Gedruckt auf chlorfrei gebleichtem Recyclingpapier

13. Datenschutzbericht

Inhaltsverzeichnis

Anhang

Stichwortverzeichnis

Vorbemerkung

In den Berichtszeitraum fällt ein personeller Wechsel. Am 30. Juni 1995 ist mein Vorgänger im Amt, Hans Maier-Bode, mit Erreichen der gesetzlichen Altersgrenze in den Ruhestand getreten. Die Landesregierung sprach ihm zur Verabschiedung ihren Dank aus und hob anerkennend hervor, daß er in seiner Amtsführung große Sachkenntnis sowie Sachlichkeit bewiesen habe und das Bemühen, möglichst zufriedenstellende Lösungen für die Bürgerinnen und Bürger zu erreichen. Auch Vertreter der Landtagsfraktionen betonten, daß er ein immer wieder gern gesehener Gesprächspartner gewesen sei. Er hat die Belange des Datenschutzes mit Beharrlichkeit vertreten und einen wesentlichen Beitrag dazu geleistet, das Datenschutzbewußtsein in Nordrhein-Westfalen nachhaltig zu stärken.

Nach der Wahl durch den Landtag habe ich das Amt der Landesbeauftragten für den Datenschutz am 1. April 1996 angetreten. Ich möchte nicht versäumen, meinem Amtsvorgänger Dank dafür zu sagen, daß er mir eine wohlgeordnete Dienststelle überlassen hat. Sachkundige und motivierte Mitarbeiterinnen und Mitarbeiter ermöglichten mir ohne große Übergangsprobleme die Aufnahme der neuen Tätigkeit. Dafür sei ihnen an dieser Stelle besonders gedankt, zumal sie mit unerschöpflicher Geduld und Freundlichkeit meine - nicht selten von einem gewissen Befremden begleiteten - Fragen zu Arbeitsweisen und Gepflogenheiten in der "Welt der Verwaltung" beantwortet haben. Sehr angenehm ist auch die Zusammenarbeit mit den Datenschutzbeauftragten des Bundes und der Länder. In diesem Kreis habe ich nicht nur eine freundliche Aufnahme gefunden, sondern auch wertvolle Anregungen und Unterstützung erhalten, für die ich mich an dieser Stelle nochmals bedanken möchte.

Der nun vorliegende Datenschutzbericht umfaßt einen Zeitraum, der mit einem halben Jahr noch in die Amtszeit meines Vorgängers fällt und für weitere neun Monate eine Interimszeit darstellt, in der die Dienststelle stellvertretend von Dr. Guntram Spitzl geleitet wurde, dem dafür hier ebenfalls Dank zu sagen ist. In den neun Monaten meiner bisherigen Amtstätigkeit sind für mich gewisse Entwicklungstendenzen erkennbar geworden. Abgesehen von den vielen Anfragen, die die Dienststelle täglich telefonisch erreichen, ist auch die Zahl der schriftlichen Beschwerden und Informationswünsche gestiegen. Dabei zeichnen sich Schwerpunktverlagerungen ab, die der zunehmenden Technisierung geschuldet sind. Seien es beispielsweise Fragen von Bürgerinnen und Bürgern zum staatlichen Umgang mit ihren Daten, sei es datenschutzrechtlicher Beratungsbedarf bei der Planung und Durchführung von Automationsprojekten in der öffentlichen Verwaltung oder seien es Stellungnahmen zu Landes- oder Bundesgesetzgebungsvorhaben, die mittlerweile selbstverständlich von einer

informations- und kommunikationstechnisch unterstützten Verarbeitung personenbezogener Daten ausgehen: Allein mit juristischem Sachverstand lassen sich die damit verbundenen Probleme nur in seltenen Fällen noch lösen. In immer größerem Umfang ist in allen Fachreferaten der Dienststelle technisches Verständnis und Hintergrundwissen erforderlich, um praxisgerechte Antworten auf die im Schnittfeld von Technik und Recht liegenden Datenschutzfragen geben zu können.

Zu meiner Freude enden etliche Fälle datenschutzrechtlicher Überprüfungen mit dem Ergebnis, daß die betroffene öffentliche Stelle nicht gegen den Datenschutz verstoßen hat. Werden Datenschutzmängel festgestellt, gelingt es aber auch häufig, gemeinsam mit den ins Blickfeld geratenen Stellen datenschutzgerechte Lösungen zu finden, ohne daß es einer förmlichen Beanstandung bedarf. Um Datenschutzverstöße von vornherein zu vermeiden, wäre es allerdings wünschenswert, wenn die Beschäftigten im öffentlichen Dienst bei ihrer Arbeit den Datenschutzgedanken frühzeitig noch stärker im Bewußtsein hätten und die Einhaltung der datenschutzrechtlichen Bestimmungen gewährleisten würden. In Zweifelsfragen steht meine Dienststelle gerne mit Rat und Tat zur Seite. Die frühzeitige Information über und Beteiligung an datenschutzrelevanten Vorhaben oder Rechtsetzungsverfahren findet zu meinem Bedauern noch nicht immer in zufriedenstellender Weise statt.

Der 13. Datenschutzbericht hat ein neues Design und versucht auch inhaltlich gewisse Akzentverschiebungen vorzunehmen. So ist beispielsweise darauf verzichtet worden, Gesetzesänderungen auf Bundes- und auf Landesebene in einem eigenen Abschnitt umfassend zu beschreiben. Soweit sie von allgemeinem Interesse sind, finden sich Änderungen des gesetzlichen Rahmens sowohl in der Skizze "Zur Situation im Datenschutz" als auch in den Einleitungsabschnitten zu den jeweiligen Sachgebieten. In den Sachgebieten selbst wurde versucht, deren datenschutzrelevante Entwicklung kurz zu beleuchten sowie nur noch ausgewählte Einzelfälle knapp darzustellen. Nicht einmal sämtliche Fälle, in denen eine förmliche Beanstandung ausgesprochen werden mußte, sind aufgenommen worden. Auch sind einige Bereiche aus Gründen der Entschlackung des Berichts dieses Mal ganz herausgenommen worden, obwohl sie erhebliche Arbeitskapazitäten in der Dienststelle beansprucht haben.

Verzichtet wurde ebenfalls auf die Auflistung der durchgeführten Beratungsgespräche, der Informations- und Kontrollbesuche, der abgegebenen Stellungnahmen zu Entwürfen von Gesetzen, Verordnungen und Verwaltungsvorschriften auf Bundes- und Landesebene sowie der Vorlagen an den Landtag. Eine bloße Aufzählung dieser Aktivitäten, zu denen auch die intensivierte Öffentlichkeitsarbeit zählt, besitzt keinen über die Quantitätsdokumentation hinausgehenden Informationsgehalt. Gleiches gilt für die Fortbildungen, die

meine Mitarbeiterinnen und Mitarbeiter zum Datenschutz durchgeführt haben sowie für die Teilnahme an Podiumsdiskussionen, an sonstigen Veranstaltungen und nicht zuletzt an den Arbeitskreisen und Konferenzen der Datenschutzbeauftragten, wobei ein Großteil der von den Datenschutzbeauftragten des Bundes und der Länder gefaßten Entschließungen im Anhang abgedruckt ist. Zudem erscheint es wenig sinnvoll, manche Punkte, die bereits in früheren Tätigkeitsberichten ausführlich abgehandelt worden sind und für die die dortigen Ausführungen auch heute noch im wesentlichen Geltung beanspruchen können, immer wieder mit demselben Inhalt zu wiederholen. Dies ist von Fall zu Fall entschieden worden und bedeutet nicht, daß in allen unerwähnten Bereichen mit dem Datenschutz etwa alles zum Besten stünde.

Die Leitlinie der Überlegungen zur Entschlackung des Berichts war die Frage, für wen der Datenschutzbericht geschrieben wird. Die Adressatinnen und Adressaten des Berichts sind zu allererst die Mitglieder des Landtags, aber auch die interessierte Öffentlichkeit und nicht zuletzt die öffentlichen Stellen des Landes, die ich bei der Einhaltung des Datenschutzes unterstützen möchte, freilich auch zu kontrollieren habe. Die Informationsansprüche und Erwartungen dieses Adressatenkreises sind notwendigerweise unterschiedlicher Art. Sie bewegen sich zwischen umfassender Rechenschaftslegung und der Konzentration auf das Wesentliche, zwischen juristisch-fachlicher Ausführlichkeit und Allgemeinverständlichkeit in Sprache und Sachaussage. Es wäre allerdings vermessen zu glauben, daß der Datenschutzbericht all diesen sich zum Teil gegenseitig ausschließenden Ansprüchen uneingeschränkt gerecht werden könnte, zumal das Zeitbudget der meisten Leserinnen und Leser begrenzt sein dürfte. Es war also ein Kompromiß zu schließen, der zugleich ein Experiment darstellt. Das Ergebnis liegt Ihnen nun vor.

1. Zur Situation im Datenschutz - eine Skizze

Personenbezogene Datenverarbeitung begegnet den Bürgerinnen und Bürgern heutzutage auf Schritt und Tritt. Die Pflicht, dem Staat bestimmte Daten zur Speicherung zu überlassen, wird ergänzt durch den faktischen Zwang zur Datenpreisgabe für den Abschluß mancher Rechtsgeschäfte im privaten Wirtschaftsverkehr und angereichert durch die vielfältigen Verlockungen des bequemen Lebens, die uns Tag für Tag veranlassen, unsere Daten ganz freiwillig zu offenbaren. Angefangen bei der Speicherung der Bestands- und Verbindungsdaten beim Gebrauch des Telefons, dessen mobile Variante zugleich die Überwachung des örtlichen Aufenthalts ermöglicht, über die Vielzahl der täglich eingesetzten personenbezogenen Karten, mit denen gekauft und gemietet wird, Arztbesuche bestritten und Zugangsberechtigungen nachgewiesen werden, bis hin zur Kommunikation per Internet, deren Spuren und Inhalte lückenlos verfolgt werden können, sind wir auf dem Weg zur gläsernen Bürgerin und zum gläsernen Bürger schon viel zu weit vorangekommen.

Chipkarten sollen im übrigen schon bald die Rechenleistung heutiger PCs besitzen und den Alltag revolutionieren. Visionen einer verchipten Umwelt entstehen, in der der einzelne Mensch durch die allgegenwärtigen Kleincomputer gleichsam in einen Informationskokon eingesponnen ist. Chips an Gegenständen im Haushalt, im Auto, am Arbeitsplatz und im Kaufhaus sollen bei der Bewältigung des Alltags behilflich sein - um den Preis der vollständigen Überwachbarkeit durch die Vielzahl der im Datennetz vorhandenen Informationen.

Die technischen Voraussetzungen für die Erstellung von Nutzungs-, Konsum-, Bewegungs-, Kommunikations- und letztlich **Persönlichkeitsprofilen** sind vorhanden. Ob das technisch Mögliche jedoch auch seine tatsächliche Umsetzung ungehindert in großem Umfang erfährt, ist noch nicht völlig ausgemacht. In seinem Volkszählungsurteil aus dem Jahre 1983 (BVerfGE 65, 1/43) hat das Bundesverfassungsgericht es für verfassungsrechtlich geboten erachtet, daß jede Bürgerin und jeder Bürger, um sich mündig und frei bewegen zu können, wissen können muß, wer was wann und bei welcher Gelegenheit über sie oder ihn weiß, also gespeichert hat. Diese zuvorderst an die staatlichen Stellen gerichtete Aussage muß auch für die Bürgerinnen und Bürger untereinander Geltung beanspruchen können, denn der Eingriff in das grundrechtlich gesicherte Fernmeldegeheimnis beispielsweise, den die Speicherung von Verbindungsdaten darstellt, verliert für die Betroffenen nichts von seiner Qualität, wenn er durch eine private Telefongesellschaft vorgenommen wird. Daher verpflichtet das Telekommunikationsgesetz (§ 85 Abs. 2 TKG) alle, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, auf

die Einhaltung des Fernmeldegeheimnisses. Dies gilt für die Diensteanbieter ebenso wie für die Betreiberinnen und Betreiber von Telekommunikationsanlagen. Im übrigen ist der **staatliche Zugriff** auf Datensammlungen privater Unternehmen auch nicht ausgeschlossen, sondern beispielsweise im Bereich der Telekommunikation bereits jetzt ausdrücklich vorgesehen.

Anders als in manchen anderen Bundesländern unterliegen in Nordrhein-Westfalen allerdings nur die **öffentlichen Stellen** nach Maßgabe des Landesdatenschutzgesetzes meiner Datenschutzkontrolle. Die fehlende Zuständigkeit für eine Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften außerhalb des öffentlichen Bereichs führt dazu, daß auch in diesem Datenschutzbericht eine ganze Reihe von Datenschutzproblemen nicht thematisiert werden können. Kommerzielle Adressenweitergabe, Direktmarketing, Datenschutz und Datensicherheit in privaten Krankenhäusern und bei Versicherungsgesellschaften sind zum Beispiel immer wieder Gegenstände von Beschwerden, ohne daß von meinen Mitarbeiterinnen und Mitarbeitern mehr getan werden könnte, als Verständnis für die Betroffenen zu zeigen und sie an die zuständige Stelle zu verweisen. Dies ist wenig erfreulich, zumal es für Außenstehende kaum nachvollziehbar ist, daß die Videoüberwachung an Geldautomaten oder das Telebanking meiner Kontrolle unterliegt, wenn das Geldinstitut eine Sparkasse ist, nicht aber, wenn es sich um eine private Bank handelt.

Die rasant fortschreitende technische Entwicklung und die inzwischen enorme Verbreitung, die die elektronische Datenverarbeitung gefunden hat - PCs, Multimedia, Netze seien nur als Stichworte genannt -, stellen den effektiven Schutz der informationellen Selbstbestimmung vor eine Reihe **neuer Herausforderungen**. Daß Wissen Macht bedeuten kann, wird nirgends so sehr gelten wie in der derzeit entstehenden Informationsgesellschaft. Einen zusätzlichen Anlaß, sich Gedanken über neue Ansätze und Konzepte für einen wirksamen Datenschutz zu machen, bietet die Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, die 1995 verabschiedet worden ist (ABl EG, L 281/31). Da die Mitgliedstaaten diese **EU-Datenschutzrichtlinie** innerhalb von 3 Jahren in nationales Recht umzusetzen haben, ist eine Anpassung des Bundesdatenschutzgesetzes und der Landesdatenschutzgesetze notwendig.

Die **Richtlinie** will die Verwirklichung eines hohen Datenschutzniveaus erreichen, muß in ihren Anforderungen jedoch ebenfalls den unterschiedlichen datenschutzrechtlichen Entwicklungen und Bedingungen in den einzelnen Mitgliedstaaten Rechnung tragen. Sie unterscheidet nicht zwischen Datenschutzanforderungen an den öffentlichen und den privaten Bereich und ver-

langt beispielsweise die Festlegung eindeutiger Zweckbindungen für die Datenerhebung und weitere Verarbeitung. Zudem dürfen die Daten grundsätzlich nicht über den Zeitraum hinaus aufbewahrt werden, in dem sie zur Verwirklichung der festgelegten Zwecke benötigt werden. Für die Bundesrepublik Deutschland, die im Vergleich mit einigen anderen Mitgliedstaaten über ein recht weit entwickeltes Datenschutzrecht verfügt, sollten die europarechtlichen Vorgaben gerade als **Anstoß für weitere Verbesserungen** verstanden sowie Anstrengungen dafür unternommen werden, die Verarbeitung personenbezogener Daten auf das Unerläßliche zu reduzieren und den Betroffenen ein Höchstmaß an Transparenz bei der Verarbeitung ihrer Daten zu gewähren. Auch insoweit sieht die Richtlinie Informationspflichten und Auskunftsrechte vor.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich auf ihrer 51. Konferenz am 14./15. März 1996 für eine umfassende Modernisierung des Datenschutzrechts ausgesprochen und folgende Punkte als dabei wichtigste Ziele benannt:

- weitgehende **Vereinheitlichung** der Vorschriften für den öffentlichen und privaten Bereich mit dem Ziel eines hohen, gleichwertigen Schutzes der Betroffenen, beispielsweise bei der Datenerhebung und bei der Zweckbindung bis hin zur Verarbeitung in Akten,
- Erweiterung der Rechte der Betroffenen auf **Information** durch die datenverarbeitenden Stellen über die Verwendung der Daten, auf Auskunft, auf Widerspruch und im Bereich der Einwilligung,
- Verpflichtung zu Risikoanalyse, Vorabkontrolle, Technikfolgenabschätzung und zur **Beteiligung** der Datenschutzbeauftragten bei der Vorbereitung von Regelungen mit Auswirkungen auf den Datenschutz,
- Verbesserung der Organisation und Stärkung der Befugnisse der **Datenschutzkontrolle** unter den Gesichtspunkten der Unabhängigkeit und der Effektivität,
- Einrichtung und effiziente Ausgestaltung des Amtes eines oder einer **internen Datenschutzbeauftragten** in öffentlichen Stellen und
- Weiterentwicklung der Vorschriften zur **Datensicherheit**, insbesondere im Hinblick auf Miniaturisierung und Vernetzung.

Darüber hinaus haben sie unter anderem vorgeschlagen, den Schutz gegenüber Adressenhandel und Direktmarketing zu verstärken sowie besondere Regelungen für Chipkarten-Anwendungen zu erlassen, um die datenschutzrechtliche Verantwortung aller Beteiligten festzulegen und die Einzelnen vor einer un-

freiwilligen Preisgabe ihrer Daten zu schützen. Der Wortlaut der Entschließung ist im Anhang abgedruckt.

Der inzwischen vom Bundesinnenministerium vorgelegte Referentenentwurf zur Änderung des Bundesdatenschutzgesetzes läßt die Chance einer umfassenden Modernisierung des Datenschutzes bedauerlicherweise ungenutzt verstreichen. Er enthält lediglich solche Änderungen, die zur Anpassung des Bundesdatenschutzgesetzes an die Europäische Richtlinie unumgänglich sind und bleibt in einigen Punkten sogar noch hinter den Anforderungen der Richtlinie zurück. Die Anliegen der Datenschutzbeauftragten sind daher nach wie vor aktuell.

An der bisherigen Fassung des Referentenentwurfs zur Novelle des Bundesdatenschutzgesetzes läßt sich die Tendenz ablesen, den Datenschutz nicht zeitgemäß fortentwickeln zu wollen. Diese Tendenz ist auch an etlichen anderen Beispielen im Berichtszeitraum erkennbar geworden, auf manchen Feldern sind sogar **datenschutzrechtliche Rückschritte** zu konstatieren. Im Sicherheitsbereich gibt es unter Hinweis auf das Anwachsen und die sich ändernden Strukturen der Kriminalität Bestrebungen, den Datenschutz zurückzudrängen. Beispielsweise werden im Sozialbereich und im Ausländerbereich vermehrt neue Überwachungsverfahren eingeführt, so daß auch in Rechte Unverdächtiger und korrekt Handelnder eingegriffen werden kann. Die immer höhere Leistungsfähigkeit vernetzter Computersysteme fördert solche Begehrlichkeiten, mit denen das Risiko wächst, daß das Grundrecht auf informationelle Selbstbestimmung der einzelnen Personen letztlich auf der Strecke bleibt. Teilweise bisher nicht gekannte Gefahren für den Datenschutz werden durch die Entwicklung neuer Informations- und Kommunikationstechniken geschaffen, und nicht zuletzt macht die Verbreitung von Chipkarten in immer mehr Lebensbereichen es den Einzelnen schwerer, ihr Recht auf informationelle Selbstbestimmung zu wahren. Insgesamt ist es kaum noch möglich, die Übersicht zu behalten und zu wissen, wer welche personenbezogenen Daten gespeichert hat und verarbeitet.

Als Beleg für den zu erwartenden Effekt einer Verringerung der datenschutzrechtlichen Substanz mag auch die seit über 10 Jahren anhand verschiedener Gesetzentwürfe geführte Diskussion um die Änderung des Strafverfahrens gelten. Der Regierungsentwurf für ein **Strafverfahrensänderungsgesetz** aus dem Herbst 1996 ist - wie seine Vorgänger - zwar dem Umstand geschuldet, daß es dringend notwendig ist und immer dringlicher wird, der verfassungsgerichtlichen Rechtsprechung zum Grundrecht auf informationelle Selbstbestimmung auch im Rahmen der strafprozessualen Ermittlungstätigkeit sowie des Strafprozesses selbst Rechnung zu tragen und gesetzlich zu bestimmen, welche Datenverarbeitung zulässig sein soll. In materiell-rechtlicher Hinsicht

ist der Gesetzentwurf in weiten Teilen jedoch von Regelungen bestimmt, die eine Verschlechterung des Datenschutzes bis hin zur Aufgabe datenschutzrechtlicher Grundsätze bedeuten können. So sollen zum Beispiel Personen, die selbst keiner Straftat verdächtig sind, unter anderem dann längerfristig observiert werden können, wenn aufgrund bestimmter Tatsachen anzunehmen sein soll, daß sie mit einer tatverdächtigen Person in Verbindung stehen oder eine Verbindung herstellen. Ein solcher Eingriff, mit dem Lebensgestaltung und Verhaltensweisen einer gründlichen Durchleuchtung unterzogen werden sollen, ist außerordentlich intensiv.

Übertroffen wird er noch von dem immer wieder in der Diskussion stehenden sogenannten **großen Lauschangriff**, mit dem im Wege einer Grundgesetzänderung und einer zusätzlichen Änderung der Strafprozeßordnung die Voraussetzungen dafür geschaffen würden, daß künftig technische Mittel zur akustischen - und womöglich sogar optischen - Überwachung von Wohnungen eingesetzt werden können. Abhörwanzen und versteckte Videokameras könnten dann alle erfassen, die auch nur zufälligen, nachbarschaftlichen Kontakt zu einer tatverdächtigen Person hätten. Die in Artikel 13 Abs. 1 Grundgesetz geschützte **Unverletzlichkeit der Wohnung** sollte jedoch selbst zu Strafverfolgungszwecken nicht leichtfertig aufs Spiel gesetzt werden. Wird die Überwachung privater Kommunikation und privater Rückzugsräume zu Strafverfolgungszwecken ermöglicht, wären damit derzeit unabsehbare Risiken für die sozialen Beziehungen und die demokratischen Rechte der Bürgerinnen und Bürger verbunden.

Der Entwurf des Strafverfahrensänderungsgesetzes sieht außerdem vor, personenbezogene Daten, die im Strafverfahren - und dort eben eigentlich nur für Zwecke der Strafverfolgung - erhoben worden sind, auch der Polizei zu allgemeinen Zwecken der Gefahrenabwehr übermitteln zu können. Eine solche Durchbrechung der ursprünglichen Zweckbindung verletzt nicht nur den Grundsatz der **"informationellen Gewaltenteilung"**, sondern auch die der Rechtstaatlichkeit geschuldete Trennung der Aufgaben von Gefahrenabwehr und Strafverfolgung.

Zudem soll es den Strafverfolgungsbehörden nach dem Gesetzentwurf möglich sein, bestimmte, im Strafverfahren gewonnene personenbezogene Informationen für Zwecke künftiger Strafverfahren zu speichern. Dafür ist, da es bereits das zentrale staatsanwaltschaftliche Verfahrensregister und das Bundeszentralregister gibt, kein Bedarf ersichtlich. Wie viele andere Vorschriften des Gesetzentwurfs - insbesondere im Abschnitt über die Dateiregelungen - läßt auch die genannte Bestimmung keine Assoziation mehr an Datenschutz aufkommen, sondern liefert lediglich eine formalgesetzliche Grundlage für umfängliche Datenverarbeitungsmöglichkeiten. Es bleibt nur der dringliche

Wunsch, daß dieser Gesetzentwurf zur Änderung des Strafverfahrens einer Überarbeitung zugeführt wird und nicht unverändert Gesetzeskraft erlangt.

Möglicherweise **überschießende Sicherheitsbedürfnisse** haben während des Berichtszeitraums auch in anderen gesetzlichen Regelungsbereichen die Feder geführt. So verpflichtet beispielsweise das **Telekommunikationsgesetz** die Anbieter von Telekommunikationsdienstleistungen dazu, aktuelle Kundendateien zu führen, auf die die Regulierungsbehörde jederzeit ohne Wissen der Anbieter mittels eines von ihr vorgegebenen automatisierten Verfahrens Zugriff nehmen kann (§ 90 Abs. 2 TKG). Das fehlende Wissen um das Stattfinden eines Zugriffs bedeutet zugleich, daß gar nicht erkannt und kontrolliert werden kann, ob neben befugten Zugriffen etwa auch unbefugte Zugriffe erfolgen. Die Online-Abrufmöglichkeit kann die Regulierungsbehörde unter anderem auch für die Polizeien, Strafverfolgungsbehörden und Nachrichtendienste wahrnehmen (§ 90 Abs. 4 TKG), die im Einzelfall im übrigen noch eigene Auskunftsrechte gegenüber den Anbietern besitzen (§ 90 Abs. 3, § 89 Abs. 6 TKG). Damit steht das Telekommunikationsnetz in der Gefahr, verstärkt als Fahndungsnetz eingesetzt zu werden, was in früheren Zeiten schon aus rein technischen Gründen nur in sehr begrenzter Form möglich war. Eine § 89 Abs. 6 TKG vergleichbare Übermittlungspflicht findet sich auch in § 5 Abs. 3 des Entwurfs für ein Teledienstedatenschutzgesetz (siehe dazu unter 3.).

Aus den Zuständigkeitsbereichen der **Landesgesetzgebung** ist die anstehende Novellierung des **Meldegesetzes** für die Bürgerinnen und Bürger von besonderer Bedeutung. Mit dem Gesetzentwurf vom 9. Juli 1996 (Drucks. 12/1150) beabsichtigt die Landesregierung, neben der Umsetzung von Vorgaben des Melderechtsrahmengesetzes auch eine Reihe von Problempunkten aus der bisherigen Datenverarbeitungspraxis der Meldebehörden nunmehr einer normenklaren Regelung zuzuführen. Vorgesehen ist allerdings leider auch, den Meldebehörden weiterhin die Übermittlung von Einwohnerdaten an **Adreßbuchverlage** zu ermöglichen. Die Betroffenen sollen sich dagegen lediglich mit einem Widerspruch zur Wehr setzen können.

Vor dem Hintergrund des lebhaften Adressenhandels, der zumeist ohne das konkrete Wissen der Betroffenen stattfindet, und vor dem Hintergrund der zunehmenden - von den Gerichten allerdings überwiegend als illegal angesehenen - Verbreitung von Telefon- und Adreßbüchern auf CD-Rom sollte ganz darauf verzichtet werden, die Übermittlung von Meldedaten an Adreßbuchverlage vorzusehen. Selbst eine Zweckbindung, die den Verlagen die Datenverwendung nur für Adreßbücher in gedruckter Form erlaubt, dürfte kaum in der Lage sein, eine weitere Verarbeitung der aus den gedruckten Büchern gewonnenen Daten in elektronischer Form tatsächlich zu verhindern.

Die elektronischen Verzeichnisse sind qualitativ mehr als die Summe der Telefon- oder Adreßbücher. Sie erfassen zumeist nicht nur die Daten der Bevölkerung eines Ortes, sondern speichern bundesweit zum Beispiel Name, Vornamen, Namenszusätze, Berufsangaben, Straße, Hausnummer, Postleitzahl, Ort und Telefonnummer. Angaben zum Wohnumfeld und dem Charakter des Straßenzuges - reine Wohnstraße, Gewerbeanteil, Ein- oder Mehrfamilienhäuser und ähnliches - sind unter Umständen ebenfalls aufgeführt. Die Recherche- und Verknüpfungsmöglichkeiten sind nahezu grenzenlos. Recherchierbar ist anhand jedes einzelnen Merkmals - die Telefonnummer kann zum **Personenkennzeichen** werden. Zum zweifelhaften Erfolg führt die Suche auch schon, wenn nur Versatzstücke einzelner Merkmale bekannt sind. Die elektronischen Verzeichnisse können mit jeder beliebigen anderen Datei kombiniert und abgeglichen werden. Dadurch lassen sich umfassende **Persönlichkeitsprofile** erstellen - die Grundlage für das gezielte Direktmarketing.

Hier ist Vorsicht geboten, um diesen Entwicklungen nicht auch noch staatlicherseits Vorschub zu leisten. Sollte sich der Landtag jedoch dafür entscheiden wollen, die Melderegisterauskunft an Adreßbuchverlage im Meldegesetz vorzusehen, dann sollte sie wenigstens zwingend die vorherige Einwilligung der Betroffenen zur Voraussetzung haben. Aller bisherigen Erfahrung nach genügt ein bloßes Widerspruchsrecht nicht.

Datenschutz muß stärker **präventiv** ansetzen, sonst kann er die neuen Herausforderungen, vor denen er steht, nicht bewältigen. Rechtliche Steuerungslükken können nicht mehr nur nach alten Mustern geschlossen werden. Nationale Regelungen sind nach wie vor sinnvoll und nützlich, reichen perspektivisch jedoch bei weitem nicht aus, um zu verhindern, daß die Bürgerinnen und Bürger zu Informationsobjekten werden. Dem europaweiten Ausbau des ISDN-Netzes kann auch nur mit europaweiten Verkehrsregeln für die Datenautobahn begegnet werden. Der seit Jahren diskutierte Entwurf einer Europäischen ISDN-Datenschutzrichtlinie ist zwar immer noch nicht verabschiedet, doch liegt seit September 1996 immerhin der Gemeinsame Standpunkt des Rates vor (Gemeinsamer Standpunkt (EG) Nr. 57/96, ABl EG, C 315/30).

Neue Lösungen sind aber auch gefragt, damit das Recht seiner ohnehin begrenzten Steuerungswirkung nicht noch weiter verlustig geht. Die Schwierigkeiten und Abgrenzungsprobleme, die bei der Schaffung eines rechtlichen Rahmens für "Multimedia" derzeit sichtbar werden (siehe dazu unter 3.), zeigen lediglich exemplarisch, daß die **technische Entwicklung** tatsächliche Verhältnisse schafft, die die traditionellen Grenzen der Rechtsgebiete verwischen und überschreiten. Hinzukommt, daß weltweite Netzstrukturen es er-

schweren, Datenschutzverletzungen und die dafür Verantwortlichen überhaupt aufzuspüren. Um unter diesen Bedingungen den Schutz des Rechts auf informationelle Selbstbestimmung gewährleisten zu können, bedarf es rechtlicher Regelungen, die parallel zwei sich ergänzende Ansätze verfolgen sollten: Zum einen gilt es, die **subjektiven Rechte** der einzelnen Menschen zu stärken und auszubauen. Zum anderen ist die Entwicklung **datenschutzfreundlicher Technologien** durch das Recht anzustoßen, zu fördern und zu fordern.

Datenschutz durch Technik bedeutet, in die Informations- und Kommunikationstechnologie technische Vorkehrungen zu integrieren, die die Verarbeitung personenbezogener Daten so weit wie möglich entbehrlich machen, oder auch Verfahren zu nutzen, mit denen die Unbeobachtbarkeit der Kommunikation weitestgehend ermöglicht wird sowie die Vertraulichkeit, Echtheit und Unversehrtheit von Daten sichergestellt werden. Stichworte dafür sind beispielsweise **Datenvermeidung** und **Verschlüsselung**. Der Entwurf für ein **Teledienstedatenschutzgesetz** (siehe dazu unter 3.) enthält positive Ansätze in diese Richtung. So werden die Diensteanbieter zur **Datensparsamkeit** verpflichtet und haben nach Maßgabe ihrer Möglichkeiten die Nutzung und Zahlung der von ihnen angebotenen Teledienste **anonym** oder unter **Pseudonym** zu ermöglichen. Die Erstellung von Nutzungsprofilen ist nicht zulässig. Eine Ausnahme davon ist nur bei der Verwendung von Pseudonymen vorgesehen.

Der Einsatz sicherer **Verschlüsselungsverfahren** (siehe dazu unter 2.), mit denen Nachrichten nicht von Unbefugten entziffert werden können, bietet ein hohes Maß an Verläßlichkeit im Datenumgang. Er ist allerdings nicht unumstritten, da die Sicherheits- und Strafverfolgungsbehörden das genau gegenläufige Interesse haben, nämlich die Lesbarkeit von Informationen im Klartext. Dies ist zwar verständlich und nachvollziehbar, aber mit einer rechtlichen Regulierung oder gar einem Verbot der Verschlüsselung nicht zu erreichen. Wer die Begehung schwerster Straftaten vorbereitet - und allein um diese könnte es nur gehen -, wird sich von einer Verschlüsselung nicht durch ein Verbot abhalten lassen. Schon aus Gründen der Verhältnismäßigkeit könnte selbst eine Strafandrohung dafür nicht so hoch sein, daß sie denjenigen noch beeindrucken könnte, der die Begehung einer dieser Schwerststraftaten plant. Umgangen werden könnten ein Verbot oder andere Regulierungsformen zudem durch doppelte Verschlüsselung oder durch den Einsatz steganographischer Verfahren. Dabei werden Daten, die geheim bleiben sollen, in einem Strom anderer Daten gleichsam versteckt. Hinter oder in einer unverfänglichen, unverschlüsselten Textdatei oder einem digitalisierten Bild wird unbemerkt die eigentlich wesentliche Information übermittelt. Die organisierte Kriminalität würde sich dieser Methoden absehbar bedienen, das Nachsehen hätten diejenigen, die weniger Sicherheit für die Vertraulichkeit ihrer Daten

und damit eine Beschränkung ihrer Rechte im Hinblick auf unbeobachtete Kommunikation in Kauf nehmen müßten. Verfassungsrechtlich dürfte dies nicht unbedenklich sein.

Die Medienentwicklung und die Informationsgesellschaft werden noch eine Fülle neuartiger Fragen aufwerfen. Eines derjenigen Probleme, die bereits jetzt absehbar sind, ist das Risiko einer gesellschaftlichen Spaltung in informationsreiche und informationsarme Bevölkerungsteile. Einem demokratisch verfaßten Staat muß es ein Anliegen sein, daß das Stattfinden des öffentlichen Meinungs- und Willensbildungsprozesses dadurch nicht bedroht wird. Unter den Bedingungen der Informationsgesellschaft wird Information nicht nur Produktionsfaktor und Produktivkraft, sondern auch Voraussetzung für demokratische Teilhabe am politischen Kommunikationsprozeß, also für die Wahrnehmung von Grundrechten. Die Schaffung gleicher Möglichkeiten für den Zugang zu Informationen wird den "informationellen Sozialstaat" kennzeichnen. Dazu gehört zugleich jedoch auch, den Zugang zu den bei der Verwaltung vorhandenen Informationen erlangen zu können - wie es beispielsweise von der Landesverfassung Brandenburg bereits in Form eines subjektiven Einsichtsrechts in Akten und sonstige amtliche Unterlagen garantiert wird. Da dabei der Schutz des Rechts auf informationelle Selbstbestimmung zu wahren ist, hat in einer zeitgemäßen Datenschutzkonzeption auch ein **allgemeines Informationszugangsrecht** seinen Platz.

2. Datenschutz durch Technik und Organisation

2.1 Entwicklungen und Tendenzen

Informations- und Kommunikationstechnik ist künftig so zu konzipieren, daß ihre Nutzung in möglichst vielen Anwendungsfällen ohne die Hinterlassung elektronischer Spuren, daß heißt anonym, möglich ist. Grundsatz der Entwicklung neuer Technologien muß die Datenvermeidung sein.

Die zunehmende Verbreitung, Nutzung und Vernetzung von Informations- und Kommunikationstechnik bringt es mit sich, daß deren Benutzerinnen und Benutzer immer mehr elektronische Spuren hinterlassen. Dies führt dazu, daß der Schutz der Einzelnen zur Wahrung ihres jeweiligen Rechts auf informationelle Selbstbestimmung immer schwerer zu gewährleisten ist. In vielen Fällen besteht keine Kontrolle mehr darüber, welche Daten an welchem Ort, für welche Dauer und für welchen Zweck gespeichert werden. Die Gefahr des Mißbrauchs und der Zusammenführung zu komplexen **Persönlichkeitsprofilen** nimmt ständig zu. Bisherige Sicherheitsansätze zielten hauptsächlich darauf ab, die Hersteller und Betreiber von Informations- und Kommunikationstechnik durch Maßnahmen zu schützen, die die Integrität, Verfügbarkeit und Vertraulichkeit der Daten sicherstellten. Diese Sichtweise ist dahingehend zu verändern, daß zukünftig der Schutz der persönlichen Daten der Einzelnen und damit der Schutz der informationellen Selbstbestimmung in den Vordergrund gestellt wird. Es ist deshalb bereits beim Design und bei der Entwicklung technischer Systeme danach zu fragen, ob die Speicherung personenbezogener Daten zwingend notwendig ist. Hierbei ist **Datenvermeidung** und wenn dies nicht möglich ist, weitgehende Datensparsamkeit anzustreben. Begriffe wie Anonymisierung und Pseudonymisierung werden zunehmend eine große Rolle spielen (Abdruck im Anhang). Technologien für einen umfassenderen Datenschutz stehen auf verschiedenen Gebieten zur Verfügung. Sie müßten im oben genannten Sinne weiterentwickelt und fester Bestandteil zukünftigter "datenschutzfreundlicher" Systeme werden.

2.1.1 Internet

Das Internet dient heute bereits vielen öffentlichen Stellen zur Informationsgewinnung bzw. Informationsbereitstellung. Hierdurch entstehen Gefährdungen für die Nutzerinnen und Nutzer, insbesondere durch ungewollte Preisgabe von Daten und Ausforschung, sowie für die IT-Sicherheit angeschlossener interner Systeme.

Beim Anschluß an das Internet entsteht eine erhebliche Gefährdung der Datensicherheit der für die Verarbeitung personenbezogener Daten genutzten DV-Systeme und -Netze durch Ausspähung, Manipulation oder gar Zerstörung. Aus der Sicht des Datenschutzes ist ein unmittelbarer Anschluß an das Internet nur dann vertretbar, wenn er zur Erledigung der Aufgaben zwingend erforderlich ist, zuvor eine eingehende **Analyse** und **Bewertung** der damit verbundenen Risiken erfolgt ist und durch technische und organisatorische Maßnahmen die internen Systeme und Netze sicher **abgeschottet** werden können.

Der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat deshalb bereits im Dezember 1995 eine Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet veröffentlicht. Die Orientierungshilfe soll den für den Betrieb Verantwortlichen deutlich machen, mit welchen Risiken für die Sicherheit der "internen Netze" bei einem Anschluß an das Internet zu rechnen ist und wie diese Risiken über Firewalls begrenzt werden können. Dabei hängt die Stärke der Firewall wesentlich von der eingesetzten Technik und ihrer Administration ab. Insbesondere müssen Firewallsysteme eine differenzierte Kommunikationssteuerung und Rechtevergabe unterstützen sowie Authentifizierungsverfahren beinhalten.

Bevor eine öffentliche Stelle ihr Verwaltungsnetz mit dem Internet koppelt, muß sie eine eingehende Analyse und Bewertung des Kommunikationsbedarfs durchführen. Hieraus muß unter anderem hervorgehen,

- welche Daten geschützt werden müssen und nicht nach außen gelangen dürfen,
- wie der Schutz von Daten und Rechnern erfolgt,
- wie interne Strukturen nach außen unsichtbar gemacht werden,
- welche Internetdienste genutzt werden sollen,
- welches Authentifikationsverfahren eingesetzt wird,
- welche Kontrollmöglichkeiten (zum Beispiel Protokollierung) einzuschalten sind und
- welches Restrisiko bestehen bleibt.

Insbesondere bei der Beurteilung der Erforderlichkeit eines Internetanschlusses ist ein strenger Maßstab anzulegen. In jedem Fall ist zu prüfen, ob der geplante Verwendungszweck nicht schon durch den Anschluß eines isolierten Rechners erreicht werden kann.

Eine erste Anfrage bei verschiedenen öffentlichen Stellen ergab, daß diese zur Zeit den Internet-Zugang fast ausschließlich über separate, physikalisch von den Verwaltungsnetzen getrennte Endgeräte realisiert haben. Es bestehen jedoch teilweise Planungen, die internen Netze über Firewall-Techniken an das Internet anzubinden. Dieser Trend und die hierbei zugrunde liegenden Sicherheitsmaßnahmen sind kritisch zu beobachten.

Daneben ist zu prüfen, wie und in welchem Umfang personenbezogene Daten bei der Nutzung des Internet registriert werden und sich auf Grund dieser elektronischen Spuren Nutzungsprofile einzelner Anwenderinnen und Anwender erstellen lassen. Auch hier ist der Grundsatz der Datenvermeidung gleichwertig neben der Sicherung der Ressourcen zu beachten.

Das Internet entwickelt sich zu einem wichtigen Informations- und Kommunikationsmedium, das besondere Schutzmaßnahmen für nutzende Personen und angeschlossene IT-Systeme erfordert.

2.1.2 Online-Dienste und Internet-Provider

Online-Diensteanbieter und Internet-Provider sind Unternehmen, die Netzdienstleistungen anbieten und sich durch Mitgliedsbeiträge (Festbeträge) und nutzungsabhängige Gebühren finanzieren. Hierzu speichern sie Daten der Kundinnen und Kunden.

Online-Diensteanbieter unterscheiden sich von reinen Internet-Providern dadurch, daß sie neben einem Internetzugang eigene Inhalte, moderierte Foren und Serviceleistungen wie zum Beispiel homebanking anbieten. Bedingt durch die Mitgliedschaft bei einem Diensteanbieter/Provider werden von den Kundinnen und Kunden Bestandsdaten gespeichert, die für die Begründung und Abwicklung eines Vertragsverhältnisses erforderlich sind. Für die Vermittlung und Abrechnung von Dienstleistungen bzw. Angeboten werden daneben Verbindungs- und Abrechnungsdaten erhoben, gespeichert und genutzt. Gegebenenfalls werden darüber hinaus Interaktionsdaten gespeichert, die nachweisen, welche Nutzung der Angebote im einzelnen erfolgt ist. So erlauben zum Beispiel sogenannte Cookie-Funktionen in Web-Browsern, ohne Kenntnis der Nutzerinnen und Nutzer Navigationsprofile im Endgerät zu speichern und diese bei späteren Aktivitäten auszuwerten. Hierbei können Gewohnheiten und häufige Nutzung bestimmter Angebote zum Beispiel gezielt für Werbezwecke verwendet werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung vom 29. April 1996 (Abdruck im Anhang) Eckpunkte für die datenschutzrechtliche Regelung von Mediendiensten formuliert. Sie weist

auf die Gefahr hin, daß das Verhalten der Nutzerinnen und Nutzer unbemerkt registriert und zu Verhaltensprofilen zusammengeführt werden kann. Online-Dienste sollten deshalb so gestaltet werden, daß keine oder möglichst wenige personenbezogene Daten erhoben, verarbeitet und genutzt werden sowie auch anonyme Nutzungs- und Zahlungsformen möglich sind. Daneben haben Diensteanbieter zu gewährleisten, daß keine erkennbar unsicheren Netze und Dienste für die Übertragung personenbezogener Daten genutzt werden. Um die Vertraulichkeit und Integrität der übertragenen Daten sowie eine sichere Identifizierung und Authentifikation zwischen Teilnehmenden und Anbietenden zu gewährleisten, sind deshalb entsprechend dem Stand der Technik geeignete Verfahren zur Verschlüsselung und elektronischen Unterschrift (siehe unter 2.1.4) anzuwenden.

Zur Wahrung des Rechts auf informationelle Selbstbestimmung der Teilnehmerinnen und Teilnehmer sind angemessene datenschutzgerechte Maßnahmen für die neuen digitalen Dienste zu treffen. Die im Entwurf für ein Teledienstedatenschutzgesetz (siehe unter 3.) festgelegten Grundsätze zum Datenschutz bei Telediensten sind technisch umzusetzen.

2.1.3 Elektronische Mitteilungssysteme

Elektronische Mitteilungssysteme (e-mail) sind heute Bestandteil fast jeder Bürokommunikationssoftware. Sie werden zur Kommunikation innerhalb öffentlicher Stellen und in zunehmendem Maße auch zum behördenübergreifenden Nachrichtenaustausch genutzt. Da die Nutzerinnen und Nutzer dieser Systeme im allgemeinen die Übertragungswege zu ihren Kommunikationspartnerinnen und -partnern nicht kontrollieren können, ist die Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit der versandten Nachrichten ohne besondere Vorkehrungen nicht sichergestellt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 9./10. März 1995 eine Entschließung zum Datenschutz bei elektronischen Mitteilungssystemen verabschiedet (Abdruck im Anhang). Hierin zeigen sie die Sicherheitsaspekte auf, die beim Einsatz dieser Systeme zu berücksichtigen sind. Insbesondere sollten elektronische Mitteilungssysteme zum Schutz der Vertraulichkeit der zu übertragenden Nachrichten und zur Feststellung der Authentizität der Absender sichere Verschlüsselungsverfahren beinhalten und die Möglichkeit der elektronischen Unterschrift vorsehen. Daneben sollten Sicherheitsmechanismen von Netzen wie zum Beispiel geschlossene Benutzergruppen, Rufnummernidentifikation wie auch Möglichkeiten der Beweissicherung (Protokollierung von Sende-/Empfangsnachweisen) vorhanden sein.

Innerhalb der Landesverwaltung ist als elektronisches Postsystem das MHS/X.400 eingesetzt. In einigen Geschäftsbereichen ist dieser Dienst bereits als Regeldienst eingeführt und soll vorrangig gegenüber der Briefpost genutzt werden. Zum Einsatz dieses Systems habe ich in einer Stellungnahme gegenüber dem Innenministerium auf die oben angegebene Entschließung der Datenschutzbeauftragten des Bundes und der Länder hingewiesen und empfohlen, insbesondere die Möglichkeit einer geeigneten Verschlüsselung und der elektronischen Unterschrift zur Verfügung zu stellen. Weiter habe ich empfohlen, bis zur Realisierung derartiger Schutzmaßnahmen, personenbezogene Daten nicht über die private Domäne des Verwaltungsnetzes NRW hinaus in den öffentlichen Bereich und sensible personenbezogene Daten grundsätzlich nicht über X.400 zu versenden. Auf Vorschlag des Innenministeriums hat der Interministerielle Ausschuß für Automation daraufhin beschlossen, ein geeignetes und einheitliches Verschlüsselungsprodukt, das auch eine elektronische Unterschrift ermöglicht, für die Landesverwaltung zu beschaffen. Die Beschaffung eines Produktes ist mittlerweile erfolgt. Es kann davon ausgegangen werden, daß im Laufe des Jahres 1997 Verschlüsselung von allen Arbeitsplätzen aus möglich sein wird. Ich begrüße diesen Vorstoß der Landesverwaltung Nordrhein-Westfalen, die hierbei Bedenken wegen einer zukünftigen bundeseinheitlichen Lösung zur Verschlüsselung zurückgestellt hat.

*Elektronische Post nach **X.400** ist ein von der internationalen Organisation CCITT/ITU normiertes Verfahren. Architektur, Dienste und Protokolle sind festgeschrieben. Sie setzen auf dem Referenzmodell für die Verbindung offener Systeme (OSI 7-Schichten-Modell) auf. Weitere e-mail Produkte sind herstellerspezifisch. Sie kommunizieren über Gateways.*

Die vertrauliche Übertragung elektronischer Mitteilungen durch Verschlüsselung ist jedoch nicht nur in Weitverkehrsnetzen, sondern auch in innerbehördlichen Systemen eine notwendige Grundschutzmaßnahme. Auch hier kann durch Fehladressierung und unbefugtes Ausforschen im Netz oder durch Mißbrauch bei der Systemadministration der erforderliche Schutz nicht gegeben sein. Eingaben und Kontrollen in diesem Bereich haben gezeigt, daß die Sensibilität noch erhöht und die Einbringung von Grundschutzmaßnahmen erheblich verbessert werden muß.

Elektronische Mitteilungen/Post sind vor Ausforschung, Manipulation und Zerstörung besonders zu schützen.

2.1.4 Verschlüsselung

Auf Grund der Entwicklung der Informationstechnik zu immer weiterer Vernetzung der Systeme und zur Nutzung als Kommunikationsmittel, haben sich Verschlüsselungsverfahren zu zentralen Sicherheitsmaßnahmen zur Wahrung der Vertraulichkeit, Integrität und Authentizität entwickelt.

Die Verfügbarkeit von sicheren DES- und RSA-Verfahren in Softwareprodukten ist heute gegeben, so daß ein breiter Einsatz grundsätzlich möglich ist. Die Leistungsfähigkeit der Rechner und die Kosten für die erforderlichen Produkte gestatten es, Verschlüsselung als eine technisch angemessene Maßnahme im Sinne des § 10 DSG NW zur Erreichung eines hohen Schutzes zu fordern. So sollten, wie bereits unter 2.1.3 dargestellt, elektronische Nachrichtenübermittlungssysteme ohne Verschlüsselungsmöglichkeit nicht mehr betrieben werden. Zum Schutz sensibler Daten auf lokalen oder mobilen Datenspeichern ist ebenfalls der Einsatz leistungsfähiger, leicht bedienbarer Produkte möglich. Verschlüsselte Speicherung von Daten auf Datenträgern ist dann zu fordern, wenn die Datensicherheit durch die Art des Einsatzes der Computer (zum Beispiel durch Laptops) oder durch nicht ausreichend sichere Datenarchive zu gefährdet ist. Verschlüsselung ist hier ein wirkungsvolles Mittel vor unbefugter Einsichtnahme zum Beispiel nach Diebstahl oder Verlust.

> ***Verschlüsselung**: Der Data Encryption Standard (DES) ist ein in den USA normiertes symmetrisches Verschlüsselungsverfahren. Für die Ver- und Entschlüsselung wird der gleiche Schlüssel verwendet. Bei asymmetrischer Verschlüsselung werden hierfür jeweils verschiedene Schlüssel verwendet (ein Schlüsselpaar). Quasi Standard ist das RSA-Verfahren (nach den Erfindern Rivest, Shamir, Adleman). Beide Verfahren sind kombinierbar.*

In einer Entschließung vom 9. Mai 1996 haben die Datenschutzbeauftragten des Bundes und der Länder weitere Forderungen zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten aufgestellt (Abdruck im Anhang). Hierbei und bei anderen Formen des Transportes von Daten fordern sie, Verschlüsselungsverfahren einzusetzen, um dem Risiko zu begegnen, daß zu übertragende Daten unbemerkt mitgelesen oder verändert werden können. Diese Gefahr besteht sowohl beim Transport von Daten auf Disketten, Magnetbändern und anderen Datenspeichern als auch bei der Nutzung von Netzen. Auch im Hinblick darauf, daß in der Vergangenheit häufig genutzte Sicherungen beim Transport von Datenträgern, wie die Versendung als Wertpaket, nicht mehr möglich sind und zunehmend private Paketdienste für den Transport eingesetzt werden, sind zusätzliche Sicherungen erforderlich, die einen hinreichenden Schutz bieten.

Ein wirkungsvolles Mittel zur Prüfung der Unversehrtheit und Urheberschaft einer Nachricht ist die elektronische Unterschrift. Hierbei handelt es sich nicht um eine digitalisierte Unterschrift, sondern um die Bildung eines Authentikators, der einen Nachweis der Abstammung der Nachricht ermöglicht. Technisch erfolgt die Bildung einer elektronischen Unterschrift zum Beispiel in der Form, daß zunächst über eine Einwegfunktion ein eindeutiges Komprimat der Nachricht gebildet wird (Hashfunktion). Diese Zeichenfolge wird mit dem privaten Schlüssel eines asymmetrischen Verschlüsselungsverfahrens (RSA) bei der absendenden Person oder Stelle verschlüsselt und mit der Nachricht versandt. Bei der empfangenden Person oder Stelle kann dann über die inverse Operation mit dem öffentlichen Schlüssel das unverschlüsselte Hashkomprimat wieder hergestellt werden. Zur Kontrolle der Integrität der abgesandten Nachricht kann aus dieser erneut das Hashkomprimat gebildet werden. Sind beide Komprimate identisch, so ist die Nachricht unversehrt und authentisch.

Produkte zur Verschlüsselung und zur elektronischen Unterschrift werden teilweise gemeinsam angeboten. Sie sind einsetzbar und sollten verstärkt benutzt werden.

2.1.5 Chipkartensysteme

Chipkartensysteme bestehen aus miniaturisierten IT-Komponenten (Computern), die noch keine eigene Mensch-Maschine Schnittstelle besitzen. Zur Interaktion bedarf es zwischengeschalteter technischer Geräte (Kartenterminals, DV-Systeme). Die Risiken von Chipkarten entsprechen denen von transportablen Rechnern.

In den letzten Jahren hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wiederholt mit Verfahrensentwicklungen befaßt, die den Einsatz einer Prozessorchipkarte (Smart Card) zugrundelegen. In verschiedenen Entschließungen (teilweise Abdruck im Anhang) wurden konkrete Rechtsprobleme und Risiken beim Einsatz der Chipkarte zum Beispiel als elektronische Geldbörse, zur Realisierung einer Autobahnmaut oder zum Einsatz im Gesundheitswesen aufgezeigt. Der Arbeitskreis Technik der Datenschutzbeauftragten hat nunmehr Anforderungen zur informationstechnischen Sicherheit bei Chipkarten zusammengestellt. Um eine unbefugte Preisgabe, Veränderung und Vorenthaltung von Informationen beim Einsatz von Chipkarten zu vermeiden, sollten diese Systeme angemessene Sicherungsmaßnahmen beinhalten. Hierbei sind sowohl die Einzelkomponenten wie Hard- und Software der Chipkarte, des Kartenterminals und der zu nutzenden Systeme als

auch deren Zusammenwirken zu betrachten. Zusammenfassend sind folgende Schutzmaßnahmen zu nennen:

- Ausstattung des Kartenkörpers mit fälschungssicheren Authentifizierungsmerkmalen wie zum Beispiel Unterschrift, Foto, Hologramm,
- Steuerung der Zugriffs- und Nutzungsberechtigungen durch die Chipkarte selbst und nicht durch andere am Interaktionsprozeß beteiligte Systeme,
- Realisierung aktiver und passiver Sicherheitsmechanismen gegen eine unbefugte Analyse der Chipinhalte sowie der chipintegrierten Sicherheitsfunktionen,
- Benutzung allgemein anerkannter veröffentlichter Algorithmen für Verschlüsselungs- und Signaturfunktionen sowie zur Generierung von Zufallszahlen,
- Sicherung der Kommunikation zwischen der Chipkarte, dem Kartenterminal und dem gegebenenfalls im Hintergrund wirkenden System durch kryptografische Maßnahmen.

Daneben sollten Chipkarteninhaberinnen und -inhaber die Möglichkeit haben, auf neutralen, zertifizierten Systemumgebungen Dateninhalte und Funktionalitäten ihrer Chipkarte einzusehen. Das gesamte System ist zu dokumentieren und sollte ein vorgeschriebenes Mindestschutzniveau besitzen. Alle Einzelkomponenten sind auf der Basis der Grundsätze ordnungsgemäßer Datenverarbeitung zu evaluieren. Insgesamt sollten geeignete Kontrollmöglichkeiten vorhanden sein.

Da die Technik der Chipkarte sich insbesondere in bezug auf die Speicher- und Prozessorkapazitäten rasant entwickelt, wächst auch die Möglichkeit der Einbringung von Sicherheitsmerkmalen. Die Entwicklung ist aus Sicht des Datenschutzes zu beobachten. Eine Standardisierung der Mindestanforderungen ist dringend zu empfehlen.

2.1.6 Datenspeicherung auf CD-ROM

Die Datenspeicherung auf CD-ROM entwickelt sich im zunehmenden Maße als Alternative zu den bisher gebräuchlichen Datenträgern wie Magnetplatte, Diskette und Magnetband. Die fehlende Möglichkeit der Löschung von Datensätzen auf CD-ROM Datenträgern führt jedoch dazu, daß den Forderungen nach Löschung personenbezogener Daten, zum Beispiel bei unzulässiger Speicherung oder bei erforderlicher Berichtigung, nicht ausreichend Rechnung getragen werden kann.

Optische CD-ROM Datenträger werden heute noch hauptsächlich für den Vertrieb von Softwareprodukten (zum Beispiel Programme, Spiele, Literatur) verwendet. Bekanntestes Beispiel für die Speicherung personenbezogener Daten ist das elektronische Telefonbuch. Auf Grund der zu akzeptablen Preisen verfügbaren CD-ROM Brenner und Rohlinge ist es heute auch für einzelne Anwenderinnen und Anwender möglich, Daten und Programme auf diesem Medium zu speichern. Neben der fabrikmäßigen Fertigung von CD-ROM wird zukünftig auch die Eigenerstellung und damit die Nutzung als Sicherungsmedium für den Datenträgeraustausch und Datenabgleich zunehmen.

Sollen die auf CD-ROM enthaltenen Daten gelöscht werden, so ist dies derzeit nur durch Zerstörung der Speicherfläche (zum Beispiel Ätzen, Zerkratzen) oder durch physikalische Vernichtung des gesamten Datenträgers (Einschmelzen, Verbrennen, Schreddern) möglich. Daneben ist auch ein Aufgeben von Einzeldaten oder Datensätzen möglich. Hierbei wird die aktuelle Indexdatei bzw. Datenbank, in der Verweisdaten für den Zugriff enthalten sind, aktualisiert bzw. bereinigt. Ohne die Kenntnis dieser Verweisdaten sind die auf der CD-ROM abgelegten Nutzinformationen nicht gezielt und nur mit Aufwand verwertbar. Zu den Begriffen Löschen und Aufgeben wird auf die Ausführungen im 11. Tätigkeitsbericht (S. 149 f.) verwiesen.

Auf Grund der technischen Besonderheiten der CD-ROM sollten personenbezogene Daten nur dann auf diesem Medium gespeichert werden, wenn sie langfristig und mit gleichen Löschungsfristen archiviert bzw. gesichert werden sollen. Für kurz- bis mittelfristig sich ändernde Daten ist dieses Speichermedium unter Datenschutzgesichtspunkten zur Verwendung nicht geeignet.

2.1.7 Office-Produkte

In vielen Bereichen der öffentlichen Verwaltung werden heute integrierte Office-Pakete (Bürokommunikationsprodukte) eingesetzt. Diese Produkte erlauben insbesondere mit ihren Datenbank- und Tabellenkalkulationsprogrammen eine weitgehend freie Programmierung von Anwendungen.

Bei Kontrollbesuchen wurde festgestellt, daß in der Regel Vorgaben für den Einsatz integrierter Office-Produkte nicht gemacht worden sind. So ist im allgemeinen nicht festgelegt, in welchen Fällen konkrete Programmausgestaltungen dokumentiert zu hinterlegen sind und sicherzustellen ist, daß die definierten Einsatzbedingungen nicht unkontrolliert verändert werden. Den öffentlichen Stellen ist nicht bewußt, daß zum Beispiel mit der konkreten Ausprägung einer Anwendung zur Verarbeitung personenbezogener Daten auf der Basis benutzergenerierbarer Datenbankprodukte oder Tabellenkalkulationsprogramme auch der organisatorische und technische Rahmen für den Einsatz

vorzugeben ist, der unkontrolliert nicht verändert werden darf. Es sollte festgelegt sein, welche Maßnahmen der Speicher-, Zugriffs- bzw. Eingabekontrolle entsprechend § 10 Abs. 2 DSG NW vorzusehen sind. Werden diese Produkte frei und ohne Vorgabe eingesetzt, ist eine verbindliche Verarbeitungslogik sowie auch eine Kontrollmöglichkeit praktisch nicht gegeben.

Abzugrenzen ist die beschriebene Einsatzart der Office-Produkte von der Anwendung als individuelle Arbeitsunterstützung. Es ist festzulegen, wann eine individuelle Verarbeitung und wann eine verbindliche Verarbeitung gegeben ist. Hierbei ist nach meiner Auffassung eine individuelle Verarbeitung nur dann gegeben, wenn eine temporäre Verarbeitung vorliegt und auf Grund der Dokumentation des gesamten Vorgangs in der Akte alle Ergebnisse auch ohne DV-Unterstützung nachvollziehbar sind.

Die dauerhafte Verfügbarkeit von vollständigen Entwicklungslizenzen an den Arbeitsplätzen sollte deshalb allenfalls in den Fällen der individuellen Arbeitsunterstützung erlaubt sein. In den Fällen von verbindlicher Verarbeitung sollten genaue Vorgaben existieren und lediglich der Einsatz von Runtime Versionen zugelassen sein.

Gegen einen freien Einsatz von benutzergenerierbaren Datenbankprogrammen bestehen schwerwiegende datenschutzrechtliche Bedenken. Auch eine verbindliche Meldung zum Dateienregister gemäß § 23 Abs. 1 DSG NW ist bei diesem Betrieb nicht möglich.

2.2 Konzeption von IT-Sicherheit

Bei Kontrollbesuchen stellte sich heraus, daß die Planung und Einführung neuer IT-Systeme und Verfahren in der Regel ohne Zugrundelegung eines IT-Sicherheitskonzeptes erfolgt. Hierdurch wird in Kauf genommen, daß die bei der Benutzung neuer Systeme entstehenden Risiken erst im laufenden Betrieb erkannt und dann nur schwer oder gar nicht mehr gemindert werden können.

Nur durch die Erstellung eines Sicherheitskonzeptes in sehr frühen Entwicklungsphasen kann gewährleistet werden, daß die erforderlichen Maßnahmen zur IT-Sicherheit im Design und bei der Auswahl der Hard- und Software ausreichend berücksichtigt werden. Ist die Systemumgebung für ein neues Verfahren bereits festgelegt, haben sich die Sicherheitsmaßnahmen zwangsläufig daran zu orientieren.

Auch die EG-Datenschutzrichtlinie (vgl. Artikel 17, 20 in Verbindung mit Erw. Grund 46 - (Abl. EG 1995, L 281/31) betont den Aspekt, daß sowohl zum

Zeitpunkt der Planung von Verfahren, als auch zum Zeitpunkt der Inbetriebnahme und während des Betriebes geeignete technische und organisatorische Maßnahmen zu treffen sind, die die Sicherheit gewährleisten und somit jede unrechtmäßige Verarbeitung verhindern. Die IT-Richtlinien NW (vgl. MBl. NW. 1996, S. 1296/1297) verpflichten die Aufgabenträger in der Landesverwaltung ebenfalls, bereits bei der Verfahrensbeschreibung auch die Maßnahmen für die IT-Sicherheit und den Datenschutz festzulegen.

Eine Hilfestellung zur Erreichung einer hinreichenden IT-Sicherheit geben die Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Das IT-Sicherheitshandbuch des BSI dient dazu, die Anwenderinnen und Anwender bei der Untersuchung und Gewährleistung der IT-Sicherheit zu unterstützen. Hierzu wird ein vierstufiges Verfahren vorgeschlagen:

In der Stufe 1 (**Ermittlung der Schutzbedürftigkeit**) werden die IT-Systeme und Anwendungen erfaßt, abgegrenzt und bewertet, die Gegenstand der Untersuchung sind.

In der Stufe 2 (**Bedrohungsanalyse**) werden alle bedrohten Objekte (zum Beispiel Hardware, Diskette, Daten), und die jeweiligen Bedrohungen differenziert beschrieben (zum Beispiel Diskette ist bedroht durch Diebstahl, Zerstörung). Nach vollständiger Zusammenstellung sind die Schwachstellen des IT-Systems beschrieben.

In der Stufe 3 (**Risikoanalyse**) wird bewertet, wie schädlich sich die Bedrohungen auf den IT-Einsatz auswirken können, daß heißt welche Risiken aktuell bestehen. Zusätzlich wird festgelegt, welche Risiken tragbar und welche untragbar sind.

In der Stufe 4 (**Erstellung des IT-Sicherheitskonzeptes**) werden die Maßnahmen zusammengestellt, die ausgewählt worden sind, um die Risiken zu reduzieren und damit die Verarbeitungssicherheit zu erhöhen. Die Maßnahmen sind dann zu treffen, wenn der mit ihnen angestrebte Schutzzweck in einem angemessenen Verhältnis zum Aufwand steht.

Die beschriebene systematische Vorgehensweise für die Erstellung eines Sicherheitskonzeptes erfordert einen großen zeitlichen und fachlichen Aufwand. Dieser Aufwand kann nicht ausnahmslos für jedes IT-Projekt erbracht werden. Für Automatisierungsvorhaben, die auf Grund ihrer Bedeutung für die Funktionsfähigkeit der Verwaltung oder auch der Sensibilität der zu verarbeitenden Daten einen hohen Schutzbedarf besitzen, sollte die systematische Erarbeitung und Umsetzung eines IT-Sicherheitskonzeptes im oben angegebenen Sinne

jedoch zwingend durchgeführt werden. Für IT-Projekte, bei denen der Aufwand nicht angemessen ist und in denen keine sensiblen personenbezogenen Daten verarbeitet werden, kann das IT-Grundschutzhandbuch des BSI für die zu treffenden IT-Sicherheitsmaßnahmen zugrunde gelegt werden. Projektabhängig können allerdings noch weitere Maßnahmen erforderlich sein.

Planung und Einführung von IT-Technik sind auf der Basis eines fundierten Sicherheitskonzeptes durchzuführen.

2.3 PC Einsatz bei öffentlichen Stellen

Personal-Computer (PCs) sind auch bei den öffentlichen Stellen des Landes nicht mehr wegzudenken. Sie ergänzen und ersetzen teilweise in der Vergangenheit eingesetzte Großrechnertechnologie und erschließen daneben Arbeitsfelder, die bisher nicht erreichbar waren. Für die zu verarbeitenden personenbezogenen Daten entstehen damit Risiken, die neue Anforderungen an die Gewährleistung des Datenschutzes stellen.

Zusätzliche Risiken beim Einsatz von PCs entstehen hauptsächlich aus folgenden Gründen:

- PCs und Peripherie befinden sich meist in einer normalen Büroumgebung und nicht in einem geschützten Bereich,
- Hard- und Software bieten von Hause aus nur geringe Schutzmechanismen,
- PCs sind relativ klein und leicht zu transportieren,
- Datenträger besitzen wegen ihrer Handlichkeit ein hohes Mißbrauchspotential,
- Benutzerinnen und Benutzer eines PC bedienen, administrieren und nutzen das System in einer Person. Es findet keine Funktionstrennung statt. Dies beinhaltet alle mit diesen Funktionen verbundenen Rechte und damit nur geringe Verbindlichkeit der Verarbeitung der personenbezogenen Daten,
- Benutzerinnen und Benutzer besitzen häufig nur Kenntnisse über ihre Anwendungssoftware. Sicherheitsfunktionen und Risiken ihrer Systeme sind ihnen oftmals nicht geläufig.

2.3.1 Technische Maßnahmen zur IT-Sicherheit

Um einen Überblick über die bei PCs getroffenen Maßnahmen zur Sicherstellung des Datenschutzes bei den öffentlichen Stellen des Landes zu bekommen, wurde eine Befragung bei 54 öffentlichen Stellen durchgeführt.

Eine Übersicht der eingegangenen Antworten ergab folgendes Bild:

Öffentliche Stelle	Sum	1B/PC	nB/PC	Sich Pro.	Boots	mech. Sch.	Passw	Verschl.	Netze	zentr. DB	Laptop
LAND											
Oberste Landesbehörde	3	3	0	0	0	0	3	0	0	0	0
Landesoberbehörden	4	0	4	0	0	0	0	0	0	0	0
untere Landesbeh..											
Kreispolizeibehörden:	109	35	74	0	17	17	109	0	61	0	0
Finanzämter:	14	14	0	14	0	0	14	0	7	0	7
Schulamt:	7	1	6	0	7	6	7	0	7	0	1
Versorgungsämter:	37	6	31	34	0	34	34	0	35	0	0
Sonstiges:	131	131	0	0	0	0	131	0	129	0	1
Einricht. d. Landes:	31	27	4	3	3	3	12	0	5	0	0
Organe d. Rechtspflege:											
Staatsanwaltschaften	106	102	4	104	0	4	13	11	10	0	0
Justizvollzugsanst.	3	2	1	0	3	0	3	0	0	0	0
Notare:	20	0	20	0	0	0	0	0	0	0	0
Gerichtsvollzieher	1	1	0	0	0	0	0	0	0	0	1
KOMMUNEN:											
Kommunalverband:	1	1	0	0	0	0	1	0	0	0	0
Kreise:	388	372	16	11	0	35	388	0	150	5	8
Kreisfreie Städte:	188	88	100	186	0	73	188	0	175	0	1
Städte u. Gemeind.	234	154	80	164	0	60	220	0	139	56	0
Schulen:	9	9	0	4	0	0	3	1	2	2	0
HOCHSCHULEN:											
Fachhochschulen:	16	16	0	0	0	3	11	0	0	0	0
SONST. JUR. PERS.:											
Kammern:	30	30	0	0	0	30	30	0	30	30	0
Sozialversich.träger:	336	333	3	2	232	164	91	0	326	245	8
Versich.anstalten:	1050	200	850	700	700	350	700	700	0	0	200
Sparkassen:	2633	481	2152	67	80	718	1318	0	2481	1023	257
Sonst. Körpersch. u.Anst. d. öffentl. R.:	4	0	4	0	0	4	4	0	4	0	0
SUMME:	**5355**	**2006**	**3349**	**1289**	**1042**	**1501**	**3280**	**712**	**3561**	**1361**	**484**
Durchschnitt	**99**	**37**	**62**	**24**	**19**	**28**	**61**	**13**	**66**	**25**	**9**

Legende:

Sum	=	Gesamtsumme d. eingesetzen PCs	Passw	=	Paßwortschutz
1B/PC	=	1 Benutzer/PC	Verschl	=	Verschlüsselung v. Daten
nB/PC	=	mehrere Benutzer/PC	Netze	=	vernetzte PCs
SichPro	=	Sicherheitsprodukte	zentrDB	=	zentrale Datenbank
Boots	=	Bootschutz	Laptop	=	eingesetzte Laptops
mech.Sch.	=	mechanischer Schutz			

Tabelle 1: Übersicht der PC-Auswertung

Es wurden 5.355 PCs erfaßt. Dabei zeigte sich, daß bei den öffentlichen Stellen des Landes alle PC-Leistungsklassen vertreten sind. Der größte Teil gehört dabei in die 486-Leistungsklasse. Laptops werden dagegen bei den öffentlichen Stellen des Landes in nur geringem Umfang eingesetzt.

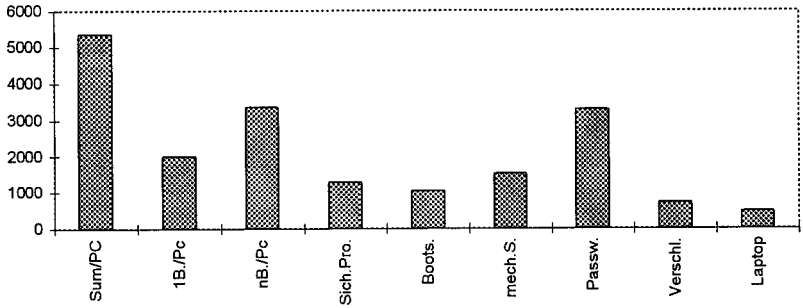

Bild 1: Darstellung der Einsatzart und Sicherheitsvorkehrungen beim PC-Betrieb

Mehr als die Hälfte der Anwendenden hat keinen "persönlichen" PC zur Verfügung, sondern teilt ihn mit weiteren Benutzerinnen oder Benutzern. Die Verfügbarkeit von Sicherheitsprodukten liegt auf den eingesetzten PCs nur bei ca. 20 Prozent. Die am häufigsten genannte Sicherheitsvorkehrung ist der Paßwortschutz. Verschlüsselungsmechanismen, die einen wichtigen Beitrag zur Erhöhung der Datensicherheit leisten können, sind bisher wenig verbreitet. Mehr als die Hälfte der erfaßten PCs ist in Netzwerke eingebunden. Für rund 1/3 der vernetzten PCs ist der Zugriff auf zentrale Datenbanken realisiert.

Werden die einzelnen Sicherheitsmaßnahmen weiter aufgeschlüsselt, so ergibt sich folgendes Bild:

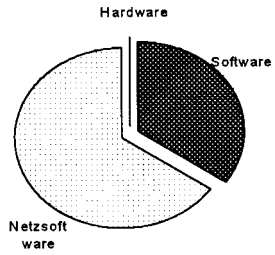

Bild 2: Sicherheitsprodukte

PC-Sicherheitsprodukte in Form von Hardwarekomponenten (zum Beispiel Steckkarten) waren kaum verbreitet. Moderne Softwareprodukte mit Funktionen wie zum Beispiel Virenschutz, kontrollierte Anmeldung, Online-Verschlüsselung von Festplatten und Diskettenlaufwerken, Zugriffskontrolle und Protokollierung wurden vor allem auf "stand-alone PCs", selten eingesetzt.
Ca. 2/3 der Sicherheitsfunktionen bezogen

sich auf standardmäßige Leistungen, die von den Netzwerkprodukten für die vernetzten PCs erbracht werden. So waren zum Beispiel individuelle Schreib- und Leserechte, die Zuweisung von Nutzungskennungen zu einem bestimmten Arbeitsplatz, die Beschränkung der Zugriffsberechtigung auf definierte Zeiträume, das Vier-Augen-Prinzip bei der Systemverwaltung und die verschlüsselte Übertragung von Paßwörtern über Netzwerkprodukte realisiert.

Die Authentifikation gegenüber dem PC durch ein Paßwort war zu 50 Prozent über Funktionen der Netzwerkbetriebssysteme realisiert. In ca. 25 Prozent der Fälle wurden Paßwortabfragen zur Vergabe von Rechten aus den jeweiligen Applikationen heraus gesteuert. Wird hier nicht gleichzeitig der Zugriff auf die Betriebssystemebene verwehrt, bietet diese Sicherung nur einen geringen Schutz für die mit diesen Applikationen erstellten Dateien, da ein Zugriff über andere Programme, zum Beispiel Texteditoren, möglich bleibt. Zu einem geringen Teil erfolgte die Paßwortabfrage aus dem BIOS (Basic Input/Output System) heraus. Unter dem Punkt "Sonstige" wurden ungenaue Angaben zusammengefaßt, die sich nicht genau einordnen ließen.

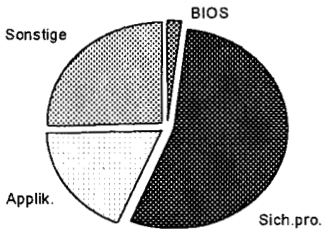

Bild 3: Paßwortschutz

Der Bootschutz ist ein Mechanismus, der ein Hochfahren (booten) des PC durch unberechtigte Personen verhindern soll. Herstellerseitig besteht die Möglichkeit, über das BIOS des PCs vor Hochfahren des Rechners eine Paßwortabfrage zu realisieren. Diese in der Mehrzahl der Fälle als Bootschutz realisierte Maßnahme ist relativ einfach zu umgehen und bietet nur wenig Sicherheit. Von verschiedenen Herstellern angebotene Hardwarekomponenten (zum Beispiel Steckkarten, deren Routinen noch vor denen des BIOS durchlaufen werden) und Softwarekomponenten, die einen höheren Schutz bieten, waren vergleichsweise wenig verbreitet.

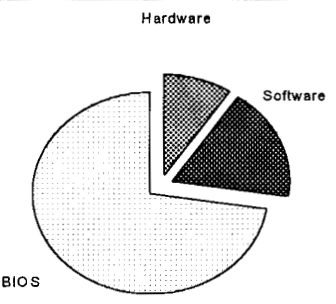

Bild 4: Bootschutz

Als mechanischer Schutz waren im wesentlichen Schlösser eingesetzt, mit denen Schnittstellen sowie Ein- und Ausgabegeräte vor unberechtigter Nutzung geschützt werden sollten. Am häufigsten war der Schutz von Diskettenlaufwerken realisiert. Verhindert werden sollte hierdurch zum Beispiel das Booten des Rechners von einer Diskette oder das Einspielen und Kopieren von Dateien über ein Diskettenlaufwerk. Die eingesetzten Produkte boten allerdings nur eine begrenzte Schutzwirkung.

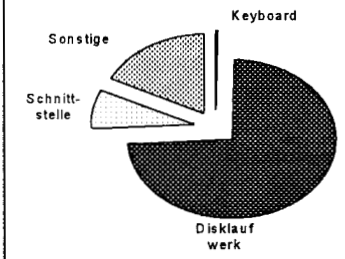

Bild 5: mechanischer Schutz

Unter dem Punkt "Sonstige" wurden ungenaue Angaben zusammengefaßt, die sich nicht einordnen ließen.

2.3.2 Kontrollbesuche

Um ein konkreteres Bild über die örtlichen Gegebenheiten, die Organisation des DV-Betriebes und die umgesetzten Maßnahmen zu erhalten, wurde bei acht öffentlichen Stellen ein Kontrollbesuch durchgeführt. Hierzu ist folgendes festzustellen:

Die übersandten Dienstanweisungen waren häufig nicht auf dem neuesten Stand. Sie enthielten zum Teil Verweise auf nicht mehr gültige Verfügungen oder bezogen sich auf nicht mehr aktuelle technische bzw. organisatorische Sachverhalte. Zum Teil existierten nur Rahmendienstanweisungen der übergeordneten Behörden, die an die örtlichen Gegebenheiten anzupassen gewesen wären. Dies war jedoch oft nicht erfolgt. Bei manchen öffentlichen Stellen lagen mehrere sich zum Teil widersprechende Dienstanweisungen vor. Den Mitarbeiterinnen und Mitarbeitern war häufig nicht klar, welche Regelungen für sie Gültigkeit hatten. Eine abschließend verbindliche Verfügungslage war selten vorhanden.

Die zum Gewährleisten der Datensicherheit erforderlichen internen Kontrollen wurden in der Regel nicht durchgeführt. Häufig war diese Funktion nicht institutionalisiert, indem sie einer Stelle oder Person zugewiesen war. Auf die Notwendigkeit der Einrichtung einer internen Kontrolle wurde schon im 11. Tätigkeitsbericht (S. 139 ff.) hingewiesen. Voraussetzung für eine effektive Kontrolle ist allerdings, daß sie unmittelbar der Behördenleitung unterstellt ist und dieser ihre Kontrollberichte direkt vorlegt. Daneben sind geeignete Unterlagen zu führen, aus denen die rechtliche Zulässigkeit der Verarbeitung und die vorgegebenen Einsatzbedingungen für alle Systeme und Anwendungen

unter dem Aspekt der Datensicherheit hervorgehen. Sowohl Kontrollberichte als auch geeignete Unterlagen konnten in der Regel nicht vorgelegt werden.

Für die Gewährleistung einer ausreichenden Zugangskontrolle, Zugriffskontrolle, Eingabekontrolle und Speicherkontrolle beim PC-Betrieb ist das Anordnen organisatorischer Maßnahmen allein nicht ausreichend. Ein wirkungsvoller Schutz kann nach meiner Auffassung nur erreicht werden, wenn auch geeignete Hard- und Softwaremaßnahmen realisiert sind. Die Sicherheitsprodukte müssen gewährleisten, daß die PCs nur bestimmungsgemäß im vorgegebenen Rahmen eingesetzt werden. Hinzuweisen ist hier auf Produkte, die vom Bundesamt für Informationstechnik zertifiziert wurden. Die Kontrollbesuche ergaben auch, daß an vielen Stellen die beschafften Produkte aus verschiedensten Gründen nicht eingesetzt wurden. Daher ist davon auszugehen, daß die Anzahl der eingesetzten Produkte noch erheblich unter dem auf Grund der Umfrage ermittelten Prozentsatz von 20 % liegt.

Ein weiterer kritischer Punkt bei der PC-Verarbeitung ist der Bereich der Datenträgerkontrolle. Um hier den notwendigen Schutz zu erreichen, ist es erforderlich, vollständige Verzeichnisse der übergebenen und eingesetzten Datenträger zu führen und Vorgaben für die Aufbewahrung zu machen. Ebenso sind Regelungen für defekte Datenträger zu treffen. Schnittstellen und Laufwerke von PCs sollten nur kontrolliert freigegeben werden können, und es sollte eine Vorschrift/Zwang zur Virenscannung und Verschlüsselung bestehen. Nur durch restriktive Maßnahmen in diesem Bereich kann insbesondere der sonst unüberschaubare Diskettenbetrieb ausreichend kontrolliert werden. Die vorgelegten Dienstanweisungen regelten diese Sachverhalte meist nur unzureichend. Aber selbst die vorhandenen Regelungen wurden nach Auskunft der Betroffenen überwiegend nicht umgesetzt. Die Erfahrungen aus den Kontrollbesuchen haben gezeigt, daß eine autonome Datensicherung für "stand-alone PCs" oder auch eine Freigabe von Diskettenlaufwerken bei vernetzten PCs ein Sicherheitsrisiko darstellt, das nicht hoch genug bewertet werden kann.

In vielen Bereichen der kontrollierten Stellen wurden integrierte Office-Pakete eingesetzt. Vorgaben für den Einsatz dieser Produkte wurden dabei nur selten gemacht. Da die freie Einsatzmöglichkeit eine verbindliche Verarbeitungslogik sowie eine Kontrolle praktisch unmöglich macht, bestehen hiergegen schwerwiegende datenschutzrechtliche Bedenken (siehe auch unter 2.1.7).

In einigen Bereichen der öffentlichen Verwaltung wird der Einsatz privater PCs zugelassen. Im 10. (S. 144 ff.) und im 11. (S. 128 ff.) Tätigkeitsbericht wurde zum Einsatz privater PCs ausführlich Stellung genommen. Es ist noch einmal darauf hinzuweisen, daß der Einsatz privater PCs für dienstliche Zwekke ein erhebliches Risiko für den Datenschutz darstellt.

Es bleibt festzuhalten, daß die zur Gewährleistung des Datenschutzes bei den öffentlichen Stellen erforderlichen technischen und organisatorischen Maßnahmen für einen geregelten Einsatz von PCs bisher nur unzureichend realisiert wurden. Sie haben mit der schnellen Einführung der PCs in der Verwaltung nicht Schritt gehalten. Die öffentlichen Stellen sind vielfach für die Risiken, die mit dem Einsatz von PCs einhergehen, nicht sensibilisiert. Die sich daraus für den Datenschutz ergebenden Gefahren sind nicht zu unterschätzen.

2.4 Autonome Datenverarbeitung bei Kommunen

Leistungsfähige Client - Server Systeme und Netzwerkbetriebssysteme erlauben seit einiger Zeit den Aufbau autonomer, dezentraler DV-Strukturen. Werden hierbei organisatorische und betriebliche Grundprinzipien außer acht gelassen, entstehen nicht hinnehmbare Risiken für die Datensicherheit.

In den 70iger und 80iger Jahren wurden in der öffentlichen Verwaltung für viele Bereiche zentrale Anwendungssysteme entwickelt und in Betrieb gesetzt. Beispiele sind auf kommunaler Ebene das Kraftfahrzeug- und Einwohnerwesen, auf Landesebene das polizeiliche Auskunftssystem. Für die Entwicklung und den Betrieb derartiger Systeme wurden an zentralen Stellen der jeweiligen Bereiche DV-Abteilungen und Rechenzentren aufgebaut. Die Benutzerinnen und Benutzer wurden über geschlossene Datennetze angebunden. Die DV-Abteilungen und Rechenzentren waren früher ein Hauptgegenstand datenschutzrechtlicher Überlegungen und Kontrollen. Hierbei wurden vielfältige Anregungen und Empfehlungen gegeben. Inzwischen kann festgestellt werden, daß bei dieser Ausprägung der Datenverarbeitung aus der Sicht des Datenschutzes ein weitestgehend sicherer Betrieb möglich ist.

Werden die IT-Entwicklungen der letzten Zeit betrachtet, so liegt der Schwerpunkt nunmehr in der Realisierung von dezentralen Systemen mit PC Endgeräten. Auf Grund dieser Entwicklungen wurden Kontrollbesuche bei drei Kommunen mit jeweils ca. 80 000 bis 90 000 Einwohnern durchgeführt. Zielsetzung war, die Sicherheit der jeweiligen autonomen, also von den kommunalen Gebietsrechenzentren losgelösten, Verarbeitungen zu prüfen.

2.4.1 Organisation der Datenverarbeitung

Dienstanweisungen, Dokumentationen, interne Kontrollen und Funktionstrennungen für den DV-Betrieb sind die organisatorische Grundlage einer ordnungsgemäßen Datenverarbeitung. Der Einsatz nur weniger Mit-

arbeiterinnen und Mitarbeiter erschwert das Einhalten dieser Basisanforderungen und kann zu kontrollfreien Räumen führen.

In großen Rechenzentren ist es üblich, die Aufgabengebiete Systemprogrammierung, Arbeitsvorbereitung, Maschinenbedienung, Arbeitskontrolle und Datenträgerverwaltung verschiedenen Bereichen zuzuordnen. Diese Funktionstrennungen sind ein wesentliches Hilfsmittel zur Sicherstellung ordnungsgemäßer DV-Verarbeitungen. Bei den aufgesuchten Kommunen waren die für die Informations- und Kommunikationstechnik zuständigen Sachgebiete jeweils nur mit wenigen (teilweise nur zwei) Beschäftigten besetzt. Funktionstrennungen, wie oben beschrieben, waren deshalb kaum zu realisieren. Das Fehlen jeglicher Funktionstrennung enthält jedoch ein hohes Maß an Mißbrauchspotential. So ist es, bedingt durch die Spezialkenntnisse der Mitarbeiterinnen und Mitarbeiter im Bereich Systemtechnik und ihre gleichzeitige Zuständigkeit für den Bereich Durchführung, Arbeitskontrolle und Datenträgerverwaltung leicht möglich, später nicht mehr nachvollziehbare, undokumentierte Veränderungen der verbindlich vorgegebenen Verarbeitung vorzunehmen. Damit ist die Datensicherheit entscheidend gefährdet.

Zur Aktualität und Qualität der Dienstanweisungen ist festzustellen, daß sie in der Regel fehlerhaft, nicht aktuell oder nicht verfügt waren. Zu ergänzen ist, daß bei vielen Systemen, die innerhalb von Stadtverwaltungen autonom in den jeweiligen Ämtern betrieben wurden, die Zuständigkeit für die Datensicherheit auf diese Ebene delegiert war. Auf Grund dieser Zuständigkeit hätten die Fachämter auch zusätzliche spezifische Regelungen für ihren DV-Betrieb treffen müssen. Im allgemeinen existierten aber keine zusätzlichen Regelungen. Den Ämtern war es nicht einmal bewußt, daß sie auf Grund ihrer Zuständigkeit ergänzende Regelungen hätten treffen müssen.

Sind, wie dargestellt, nur wenige Beschäftigte mit der Durchführung von Systemarbeiten beauftragt, so mangelt es in der Regel an einer umfassenden Dokumentation. Es wird oftmals leider als ausreichend angenommen, wenn sich die wenigen zuständigen Beschäftigten auf mündlicher Basis verständigen. Diese Haltung führt zu Risiken, die nicht hinnehmbar sind. Technisch komplexe Bereiche sollten umfassend geregelt und beschrieben sein. Es muß eine Verpflichtung bestehen, durch geeignete Anweisungen und Dokumentationen konkrete Handlungsvorgaben zu liefern. Eine Möglichkeit besteht darin, den für den DV-Betrieb zuständigen Stellen aufzuerlegen, ein IuK-Handbuch zu führen. Hieraus sollte verbindlich hervorgehen,

- welche Anweisungen für die Sicherheit und Verbindlichkeit des laufenden Betriebs getroffen wurden,

- welche Regelungen zur Bereitstellung, Einsatz und Pflege von Programmen und Systemen bestehen,
- die aktuelle technische Dokumentation,
- die Vorschriften für die Datenträgerverwaltung,
- die Regelungen für die Sicherung der DV-Räume,
- die Regelungen für Wartung und Fernwartung.

Dies gilt für alle Systemebenen und die Datennetze. Um auch eine Organisationskontrolle über den jeweils aktuellen Hard- und Softwarestand der eingesetzten Systeme zu haben, sollte klar definiert sein, daß System- und Programmänderungen der Freigabe durch Vorgesetzte bedürfen.

Eine wesentliche Voraussetzung zum Gewährleisten der Datensicherheit ist eine interne Kontrolle (vgl. 2.3.2, 11. Tätigkeitsbericht, S. 139 ff.) Bei den Besuchen wurde festgestellt, daß im allgemeinen interne Kontrollen nicht durchgeführt wurden und konkrete Vorgaben für die Durchführung nicht vorlagen.

Werden interne Kontrollen eingerichtet, reicht es nicht aus, die Kontrollen nur anlaßbezogen durchzuführen. Wie die Novellierung des Datenschutzgesetzes im Jahre 1988 zeigt, ist es nicht nur Aufgabe des Datenschutzes, den Mißbrauch zu verhindern, sondern vielmehr sicherzustellen, daß personenbezogene Daten der Bürgerinnen und Bürger in zulässiger Weise verarbeitet werden. Dies setzt regelmäßige, systematische, interne Kontrollen der Einhaltung der Datenschutzvorschriften bei der Verarbeitung personenbezogener Daten in allen Bereichen der Verwaltung voraus.

Eigene Datenverarbeitung setzt eine Organisation voraus, die einen definierten, kontrollierbaren Betrieb zuläßt.

2.4.2 Infrastruktur

Infrastrukturell erfordern Client - Server Systeme für die Unterbringung der zentralen Komponenten wie zum Beispiel Server oder Sternkoppler gesicherte Technikräume, für die Datenverwaltung sichere Tresore, Auslagerungs- und Löschungsmöglichkeiten und ein lokales Netz, daß in Subnetze gleicher Zugriffsklassen gegliedert werden kann.

Die Konzentration aller Server in einem IuK-Technikraum beinhaltet eine umfangreiche Datenspeicherung, die geeignete Sicherheitsmaßnahmen erfor-

dert. So sollten mindestens ausreichende Zugangskontrollen, Einbruchsicherungen und -überwachungen sowie eine sichere Datenträgerarchivierung, wie sie üblicherweise zur Lagerung großer Datenbestände genutzt wird, vorhanden sein. Vorgefundene Gegebenheiten wie Zugang der Rechnerräume über ungesicherte Verbindungstüren, Ausgabefächer (Schließfächer) für die DV-Listen im allgemein zugänglichen Treppenhaus, verschließbare Blechschränke mit einfacher Verriegelung als Datenträgerarchiv gewährleisten keinen ausreichenden Schutz.

Die Verwaltung des Datenbestandes ist für DV-Verfahren eine der sensibelsten Arbeiten. Deshalb ist hier besondere Sorgfalt geboten. Datenträgertresore und Archive sind Mindestvoraussetzungen für die Unterbringung des Datenbestandes. Ebenso unabdingbar für einen ordnungsgemäßen Betrieb ist eine klare Anweisung für alle durchzuführenden Arbeiten sowie eine Dokumentation über alle vorhandenen Datenträger. Es ist daher erforderlich, für jede DV-Anlage festzulegen, welche Maßnahmen zur Datenträgerkontrolle notwendig sind. Hierbei sollten die Art der Inventarisierung, die Maßnahmen für die Aufbewahrung und den Transport, die Regelungen für die Freigabe, Löschung und Vernichtung sowie die Regelungen für die Auslagerung abschließend festgelegt sein. Insbesondere muß sichergestellt sein, daß nur Berechtigte auf Datenträger Zugriff erhalten. Klare und umfassende Regelungen konnten häufig nicht vorgelegt werden. So lagerten teilweise Datenträger in größerer Anzahl außerhalb des Datenträgertresores; ebenfalls war es nicht möglich, den kompletten Bestand nachzuweisen. Verbindliche Regelungen für die Auslagerung von Datenbeständen sowie für den Transport existierten nicht. In einem Fall wurden die Datenträger auf einem offenen Wagen über die Flure in den Keller transportiert, ohne daß eine Überwachung des Transports und eine Kontrolle der Arbeiten mittels des Vier-Augen-Prinzips realisiert gewesen wäre.

Selbst für das Löschen von Datenträgern existieren teilweise keine verbindlichen Vorschriften oder technischen Hilfsmittel. Dies gilt ebenso für die Abgabe von Datenträgern wegen Unbrauchbarkeit oder aus sonstigen Gründen (zum Beispiel Vernichtung, Verkauf).

Bei der Vernetzung von Rechnern und PCs über ein lokales Netz (LAN) erhöht sich das Risiko für die Datensicherheit insbesondere dadurch, daß durch Manipulation der Netzwerkadresse oder durch Netzwerkanalyseprogramme Daten mitgelesen werden können. Dadurch können, sofern die Daten unverschlüsselt übertragen werden, personenbezogene Daten oder Paßwörter in falsche Hände geraten. Das Abhörrisiko ist besonders groß, wenn die Datenpakete ihren Weg über sämtliche Netzbeteiligten nehmen, da sie dann mit entsprechenden technischen Hilfsmitteln mitgelesen werden können. Um dieses Risiko des Mitle-

sens und Veränderns zu minimieren, sollten Rechnernetze in Subnetze gegliedert sein, in denen sich ausschließlich Geräte mit gleicher Zugriffsbefugnis befinden. Eine andere Maßnahme wäre der Einsatz von Verschlüsselungstechniken, die verhindern, daß ein einfaches Mitlesen erfolgen kann. Derartige Sicherheitsvorkehrungen waren in den besuchten Stellen nicht vorhanden.

DV-Systeme erfordern für Geräte, IuK-Räume, Netz und Datenträger Schutzmaßnahmen, die mißbräuchliche Verarbeitungen und Nutzungen wirkungsvoll verhindern.

2.4.3 Durchführung des Betriebes

Ein autonomer DV-Betrieb setzt voraus, daß die hierfür zu erledigenden Arbeiten der Betreuung von Systemen, Programmen und Daten personell und inhaltlich geleistet werden können. Ist dies nicht sichergestellt, sollten zentrale Dienststellen diese Arbeiten übernehmen.

Bei den Kontrollen ergab sich, daß teilweise die Systembetreuung allein in den Ämtern erfolgt. Dies bedeutete, daß Endanwenderinnen und Endanwender ohne spezielle DV-Erfahrung die Verantwortung für einen ordnungsgemäßen Betrieb übernehmen mußten. Bei dieser Vorgehensweise ist besonders zu bemängeln, daß nunmehr Funktionen der Anwendungsnutzung und der Systembetreuung in einer Hand liegen und hiermit die Kontrolle eines definierten Betriebs unmöglich wird. So können sich die in diesen Doppelfunktionen tätigen Anwenderinnen und Anwender zum Beispiel zeitweise besondere Rechte zuordnen oder Daten exportieren, ohne daß dies später nachvollziehbar ist.

Werden Programme selber entwickelt, sind Regelwerke für Entwicklung, Test und Freigabe zu erstellen. Zwei der kontrollierten Stellen verzichteten mangels Personal auf eigene Programmierung. Allerdings sind auch bei der Anwendung nicht selbst entwickelter Programme Vorgaben für die Freigabe und den Einsatz zu machen. Hier besitzt die datenverarbeitende Stelle ebenfalls die Verantwortung für die rechtliche Zulässigkeit und korrekte Arbeitsweise ihrer Systeme. Vor der Freigabe sind strukturierte Tests notwendig, deren Ergebnisse zusammen mit der Freigabe zu dokumentieren sind. In den besuchten Stellen existierten bislang weder Dokumentationen noch Regelungen.

Auch mußte bei einem Amt festgestellt werden, daß für den Betrieb des PC keine schriftliche Regelung vorhanden war. Der in einem auch der Öffentlichkeit zugänglichen Raum befindliche PC wurde ohne Einsatz der bereits erworbenen Sicherheitssoftware betrieben. Es waren weder Zugriffsbefugnisse noch Regelungen für die Datenträgerverwaltung festgelegt.

Überwiegend waren die PCs bei den kontrollierten Stellen über ein lokales Netz verbunden. Über zentrale Server wurden den jeweiligen Nutzerinnen und Nutzern einheitliche Werkzeuge für die Textverarbeitung, Tabellenkalkulation und individuelle Datenbanken angeboten. Die Datenbestände wurden zentral verwaltet, so daß keine eigene Datensicherung auf dem PC erfolgen mußte. Eine zentrale Anbindung aller PCs an einen Server und eine zentrale Datensicherung ist ein geeignetes Mittel, eine ausreichende Datenträgerkontrolle bei der PC-Verarbeitung sicherzustellen. Wenn eine Vielzahl von Geräten eingesetzt wird, besteht sonst die Gefahr eines unüberschaubaren Diskettenbetriebes. Die Maßnahme der zentralen Sicherung kann jedoch dann ins Leere laufen, wenn an einigen Arbeitsplätzen Diskettenlaufwerke installiert werden. Hier ist eine strenge Erforderlichkeitsprüfung notwendig, die leider nicht immer vorgenommen wurde.

DV-Technik und -Betrieb können nur dann sicher und verantwortungsbewußt betrieben werden, wenn die notwendige Sachkenntnis vorhanden ist und Sicherheitsmaßnahmen konsequent umgesetzt werden.

2.5 Einzelfragen der Datensicherheit

2.5.1 Makroviren

In der Vergangenheit galt der Grundsatz, daß die Verbreitung und Aktivierung von Computerviren nur durch ausführbare Programme erfolgen kann. Durch Makroviren erfährt diese Problematik eine neue Qualität. Auch der Umgang mit Texten und Dokumenten kann mittlerweile die Verbreitung und Aktivierung von schadenstiftender Software provozieren.

Obwohl es bereits 1989 erste Hinweise auf die Übertragung von Computerviren durch Makrosprachen gab, die Bestandteil vieler Anwendungsprogramme sind, fand der erste Makrovirus erst im Herbst 1994 eine größere Verbreitung. Seitdem beschleunigt sich das Auftauchen neuer Varianten jedoch zusehends.

Zur Zeit sind ca. 50 Makroviren bekannt. Die Schadensfunktionen reichen von der Ausgabe einer Meldung oder der Veränderung von Bildschirmoberflächen bis zur Formatierung ganzer Festplatten. Da es auch für Ungeübte relativ leicht möglich ist, bereits programmierte Makroviren zu modifizieren, ist mit einer raschen Vermehrung zu rechnen. In diesem Zusammenhang ist die Veröffentlichung der Quell-Codes von Makroviren in Fachzeitschriften, wie in der Vergangenheit geschehen, äußerst kritisch zu betrachten.

Ein weiterer Grund für die beschleunigte Verbreitung ist der Umstand, daß Makroviren häufig unabhängig von der verwendeten Rechner-Plattform lauffähig sind und dadurch eine Übertragung zwischen verschiedenen Systemplattformen möglich ist. Die Situation verschärft sich durch den Trend zur weltweiten elektronischen Datenübermittlung. Daneben ist aber auch der herkömmliche Weg der Verbreitung über Datenträgeraustausch eine nicht zu vernachlässigende Größe.

Um zu verhindern, daß über den Austausch von elektronischen Dokumenten Makroviren weitergegeben werden, sollte auf Formate ausgewichen werden, bei denen Makros nicht abgespeichert werden. Für formatierte Texte bietet sich hier das Rich Text Format (RTF) und für Tabellenkalkulationsdateien das Data Interchange Format (DIF) an.

***Makroviren** machen sich den Umstand zunutze, daß in vielen Anwendungsprogrammen (Textverarbeitungs-, Tabellenkalkulations- und Datenbankprogramme) die Möglichkeit besteht, Befehlsabläufe zu automatisieren. Diese Befehlsfolgen werden in Makros abgelegt. In diese Makros können Computerviren hineinprogrammiert werden. Die Aktivierung erfolgt dann unter Umständen automatisch bereits beim Öffnen einer Datei, die mit einem solchen Anwendungsprogramm erstellt wurde.*

Auch das Ausschalten der Makrofunktionen einer Anwendung, bisher als sicherer Schutz angesehen, ist mittlerweile kritisch zu betrachten. Ein Virus, das neue Techniken verwendet, kann bereits dann aktiv werden, wenn verdächtige Dokumente auf vorhandene Makros überprüft werden.

Durch geeignete Maßnahmen ist sicherzustellen, daß Datenaustausch und elektronische Post nur kontrolliert erfolgen. Um das Virenrisiko zu mindern, müssen eingehende Dateien vor der Weitergabe auf einem separaten PC auf Makroviren untersucht werden.

2.5.2 Fernwartung

Die öffentlichen Stellen nutzen, wenn kein eigenes Fachpersonal zur Verfügung steht oder wenn kurze Reparaturzeiten im Vordergrund stehen, häufig die Möglichkeit der Fernwartung von Soft- und Hardware durch Dritte. Da mit der Fernwartung in den überwiegenden Fällen auch der Zugriff auf personenbezogene Daten ermöglicht wird, müssen die entstehenden Risiken für die Datensicherheit durch besondere technische und organisatorische Maßnahmen aufgefangen werden.

Im Rahmen eines Besuchs bei einer Stadt stellte sich heraus, daß für die Erhaltung der Funktionsfähigkeit der Hard- und Software eines dezentralen DV-

Systems die Möglichkeit der Fernwartung genutzt wurde, ohne daß Überwachungsfunktionen und schriftliche Festlegungen zur Durchführung von Wartungsaktivitäten vorhanden waren. Fernwartung darf jedoch nur mit Wissen und Willen des Auftraggebers gestartet und durchgeführt werden. Dabei müssen alle durch die Wartung bedingten Zugriffe nachvollziehbar und überprüfbar bleiben. Dies kann zum Beispiel durch eine parallel geschaltete Datenstation und durch vollständige Protokollierung aller Aktivitäten erreicht werden. Während der Fernwartungsaktivitäten ist der Zugriff auf personenbezogene Daten, geschützte Dateien und Programme zu verhindern. Es sollte in jedem Fall gewährleistet sein, daß die Fernwartung jederzeit durch die öffentliche Stelle abgebrochen werden kann.

Ist eine Einsichtnahme personenbezogener Daten im Einzelfall nicht zu vermeiden, so ist sie jeweils auf das notwendige Maß zu beschränken. Dies bedeutet insbesondere, daß eine vorherige Risikoabschätzung erfolgen muß und die datenverarbeitende Stelle vertraglich umfassende Regelungen und Sicherheitsvorkehrungen zur Wartung und Fernwartung festgelegt hat. Für die offenbarten Daten ist festzuschreiben, daß sie einer strengen Zweckbindung unterliegen und eine Weitergabe an Dritte untersagt ist.

Eine der Fernwartung ähnliche Situation ist das bei einem Besuch festgestellte "Remote operating"-Verfahren, das zur Gewährleistung der Verfügbarkeit des zentralen Rechnersystems installiert wurde. Die Bedienung und Diagnose des Systems außerhalb der Dienstzeit führten zwei Beschäftigte über Laptop und Telefonanschluß durch. Die Bedingungen für die Bereitschaft waren in den Arbeitsverträgen festgelegt, nicht jedoch der Umgang mit dem Laptop außerhalb der Diensträume sowie die Randbedingungen für die Nutzung des Wählanschlusses. Da die beschriebene Betriebsart mit großen Risiken für die Datensicherheit verbunden ist, sind verbindliche Anweisungen von besonderer Bedeutung.

Vor Zulassung der Fernwartung ist zu prüfen, ob eine vollständige Kontrolle der Wartungsarbeiten und eine sichere Netzanbindung mit einer sicheren Authentifikation des Wartungspersonals möglich ist. Daneben sind umfassende vertragliche Regelungen mit der Wartungsfirma zu treffen.

2.5.3 Abschottung von Verfahren im Netz

Werden über die Verwaltungsnetze öffentlicher Stellen auch Verfahren bereitgestellt, die aufgrund gesetzlicher Vorschriften oder wegen der Sensibilität der zu verarbeitenden personenbezogenen Daten besondere Datenschutzmaßnahmen erfordern, so ist in erster Linie die Anforderung der Abschottung zu gewährleisten. Dieses Problem gewinnt durch den Trend

zu multifunktionalen DV-Arbeitsplätzen, aber auch im Hinblick auf die zunehmende Vernetzung und zentrale Administration besondere Bedeutung.

In einer Reihe von Fällen aus verschiedenen Bereichen der öffentlichen Verwaltung (Personal-, Beihilfe- und Patientendatenverarbeitung) wurde Stellung dazu genommen, wie einzelne in ein Gesamtsystem integrierte Rechner und Verfahren aufgrund der besonderen Sensibiltät der zu verarbeitenden personenbezogenen Daten wirksam abgeschottet werden können. Risiken bei einem Netzverbund entstehen dadurch, daß die Anwenderinnen und Anwender aufgrund der Multifunktionalität der DV-Endgeräte die Möglichkeit der unzulässigen Weiterverarbeitung von Daten besitzen, die Netzinfrastruktur (insbesondere beim LAN) ein Ausforschen, Abhören und unbefugtes Aufschalten ermöglicht und die Systembetreuung einen unkontrollierten Zugriff auf gespeicherte Daten besitzt.

Für den Betrieb im Netz sind deshalb folgende Maßnahmen vorzusehen:

- Verhinderung von unerlaubten Weiterverarbeitungsmöglichkeiten bei multifunktionalen Arbeitsplätzen; inbesondere Verzicht auf Mail-Funktionen, um unerlaubten Im-/Export zu verhindern, falls dies nicht bereits auf andere Weise verhindert wird,
- Erhöhung der Datensicherheit durch verschlüsselte Übertragung im Netz,
- Segmentierung des LAN in logische Subnetze (zum Beispiel über Router mit Filterfunktionen) mit Endgeräten jeweils gleicher Berechtigung,
- sichere Speicherung der Daten auf Datenträger durch Verschlüsselung als Datensicherheitsmaßnahme oder durch andere gleichwertige Maßnahmen, die eine Abschottung des Anwendungssystems hinreichend gewährleisten (zum Beispiel separater Server für die sensible Anwendung),
- Einführung von Kontrollmechanismen und Funktionen zur Einschränkung und Überwachung des System- bzw. Netzwerkadministrators,
- ergänzende organisatorische Maßnahmen in der Dienstanweisung, um die Datensicherheit bei sensiblen Anwendungsprogrammen zu erhöhen, insbesondere durch Maßnahmen in der Strukturorganisation (Funktionstrennung), in der Ablauforganisation (gesonderte Freigaberegelungen bei Programmänderungen, Programmdokumentation) sowie durch gesonderte Regelungen zum Datenträgertransport und zur Datenträgerverwaltung.

Sind Maßnahmen der Abschottung aufgrund des hohen Aufwandes nicht zu realisieren, sollte ein Betrieb im Gesamtnetz nicht zugelassen werden und die Anwendung in einem autonomen System betrieben werden.

Im Netz betriebene Anwendungsprogramme, die sensible personenbezogene Daten verarbeiten, erfordern zusätzliche Abschottungsmaßnahmen.

2.5.4 Einsatz von digitalen Telefonnebenstellenanlagen (TK-Anlagen)

Im Zuge der Modernisierung der Telekommunikation werden bei den öffentlichen Stellen zunehmend digitale Telefonnebenstellenanlagen eingesetzt. Aufgrund der mit dieser Technik verfügbaren umfangreichen Funktionsmerkmale entstehen zusätzliche Probleme hinsichtlich der Einhaltung des Datenschutzes und der Datensicherheit. Häufig sind die öffentlichen Stellen, wenn sie nicht über ausgebildete Fachkräfte verfügen, gegenüber dieser neuen Gefährdungslage nicht genügend sensibilisiert.

Beispiele für einen möglichen Mißbrauch durch Manipulation oder unberechtige Nutzung von Leistungsfunktionen sind die Möglichkeit der akustischen Raumüberwachung bei modernen ISDN-Telefonapparaten mit vorhandener Freisprecheinrichtung oder das Mithören von Gesprächen durch Aufschaltung in eine bestehende Gesprächsverbindung. Daneben gibt es je nach Hersteller oder Gerätetyp eine Vielzahl von Leistungsmerkmalen, die jeweils über die Systemsoftware der Steuereinheit aktiviert oder deaktiviert werden können. Die digitale Technik ist in dieser Hinsicht wesentlich angriffsanfälliger für Veränderungen und Manipulationen als die analoge, da die meisten Änderungen bereits mit Kommandoeingaben über das Betriebsterminal ein- oder ausschaltbar sind. Eine Beschreibung der Gefährdungslage bei Einsatz von digitalen TK-Anlagen hinsichtlich ihrer Funktionsfähigkeit ist zum Beispiel im Kapitel 8. 1 des Grundschutzhandbuches des Bundesamtes für Sicherheit in der Informationstechnik enthalten.

Kommt zur Sicherstellung der Verfügbarkeit der digitalen TK-Anlage noch der Abschluß eines Wartungsvertrages (einschließlich Fernwartung) hinzu, besitzt auch die Herstellerfirma die Möglichkeit, gegebenenfalls sogar ohne Kontrolle auf die digitale TK-Anlage zuzugreifen.

Einer öffentlichen Stelle, bei der eine solche Situation vorgefunden wurde, wurde empfohlen, verbindliche Regelungen für den Betrieb der digitalen TK-Anlage zu treffen und insbesondere den Umfang der Freischaltung von Leistungsmerkmalen in regelmäßigen Intervallen und nach besonderen Ereignissen durch einen Soll-Ist-Abgleich zu kontrollieren und zu dokumentieren.

Für die Gebührendatenverarbeitung, die über separate PC-Endsysteme erfolgte, sollten die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherheit gem. § 10 Abs. 2 DSG NW getroffen werden. Der Fernwartungsanschluß sollte nur in Notfällen freigeschaltet werden. Mindestens muß dann allerdings die Authentifikation des Wartungspersonals, der Abbruch der Verbindung bei sicherheitskritischen Ereignissen, ein automatisiertes Rückrufverfahren und die Protokollierung der Fernwartungsaktivitäten möglich sein. Bereits im Oktober 1992 haben die Datenschutzbeauftragten des Bundes und der Länder zum Thema "Datenschutz bei internen Telekommunikationsanlagen" eine Entschließung verabschiedet. Der Wortlaut dieser Entschließung ist in der Anlage 8 des 11. Tätigkeitsberichtes enthalten.

Freigabe und Nutzung von Leistungsmerkmalen einer TK-Anlage, Gebührendatenerfassung und -auswertung sowie die Wartung sind verbindlich zu regeln.

2.5.5 Datensicherheit bei Telefax

Beim Telefaxverfahren handelt es sich um einen Dienst, der grundsätzlich keine Datensicherheitsmaßnahmen enthält, der das offene Telefonnetz als Transportweg nutzt und in der Regel einen offenen Ausdruck beim Empfänger entstehen läßt. Auf Grund dieser Merkmale kann eine Telefaxübersendung mit dem Versand einer offenen Postkarte verglichen werden.

In den Tätigkeitsberichten hat die Datensicherheit bei der Versendung von Telefaxen schon mehrmals eine Rolle gespielt. Insbesondere im 12. Tätigkeitsbericht (S. 145 ff.) sind Maßnahmen zusammengestellt, die der Verbesserung der Datensicherheit bei der Übertragung von Unterlagen als Telefax dienen können. Die Sorglosigkeit im Umgang mit diesem Medium hat allerdings nicht abgenommen, so daß auch in diesem Berichtszeitraum wieder eine nicht unbedeutende Zahl von Fällen fehlgeleiteter Telefaxe mit personenbezogenem Inhalt zum Alltagsgeschäft meiner Dienststelle gehörten. Fehlerhaft adressierte oder fehlgeleitete Faxe bleiben zwar häufig folgenlos, doch können sie in einzelnen Fällen auch eine erhebliche Beeinträchtigung für die Betroffenen nach sich ziehen, so daß in allererster Linie jeder und jede einzelne aufgefordert sind, mehr Verantwortungsbewußtsein, Konzentration und Genauigkeit beim Umgang mit dem Faxgerät walten zu lassen und insbesondere personenbezogene Unterlagen im Regelfall nicht als Fax zu versenden.

Mit fortschreitender technischer Entwicklung und auch durch den Konkurrenzdruck des Marktes für Telefaxgeräte werden mit jedem neuem Gerät auch neue Zusatzfunktionen angeboten, die die Datensicherheit beim Telefaxverkehr verbessern, aber auch zusätzliche Datenschutzrisiken mit sich bringen können. Aus Datenschutzsicht bedenkliche Funktionsmerkmale sind zum Beispiel die

Programmierung einer zusätzlichen Rufnummer zwecks automatischer Rufumleitung bei Störung der ersten Rufnummer sowie die bei einigen Herstellern nicht dokumentierte Fernwartungsfunktion, die eine unerlaubte Kenntnisnahme der im Telefaxgerät gespeicherten personenbezogenen Daten (Journale, Verteilerlisten, Kurzwahlziele, gespeicherte Faxsendungen) ermöglicht. Zusatzfunktionen wie unter anderem codegesicherte Empfangsspeicherung, geschlossene Benutzergruppen können die Datensicherheit bei der Nutzung von Telefaxgeräten verbessern. Die sicherste Methode ist die verschlüsselte Übertragung im Telefonnetz, wobei das Verschlüsselungsgerät im Faxgerät integriert oder über spezielle Schnittstellen separat angeschlossen werden kann.

Ebensowenig wie auf einer Postkarte können personenbezogene Daten von öffentlichen Stellen ungeschützt per Telefax versandt werden. Eine sichere Verschlüsselung kann die Funktion des Briefumschlags erfüllen.

2.5.6 Datensicherheit beim Kontoauszugsdrucker

Die Presse berichtete, daß es bei einigen Geldinstituten mit Kenntnis der Kontonummer und der Bankleitzahl sowie einer manipulierten Magnetstreifenkarte möglich sei, die jeweiligen Kontostände Dritter an Kontoauszugsdruckern (KADs) abzufragen.

In der von mir erbetenen Stellungnahme zum oben genannten Presseartikel teilten mir die Sparkassen- und Giroverbände mit, daß es in ihren Verbandsgebieten bereits seit 1984 Sicherheitsvorkehrungen zum Schutz vor unberechtigten Abrufen von Kontoauszügen am KAD gäbe. Neben der Kontonummer und der Bankleitzahl würden bei KAD-Abfragen weitere Sicherheitsmerkmale geprüft, die kartenindividuell seien. Aus Sicherheitsgründen könnten keine näheren Angaben zu den zusätzlichen Prüfvorgängen gemacht werden. Probleme seien in diesem Zusammenhang bisher jedoch nicht aufgetreten.

Eine Beeinträchtigung des Datenschutzes durch den Einsatz des KAD konnte in diesem Fall nicht festgestellt werden.

2.5.7 Verletzung des Adoptionsgeheimnisses durch Software

Auch ein schon seit langer Zeit eingesetztes Anwendungsprogramm kann noch gravierende datenschutzrechtliche Unzulänglichkeiten besitzen.

Im Rahmen der Aufklärung eines möglichen Datenschutzverstoßes bei einer Stadt war es auch sieben Jahre nach erfolgter Adoption noch möglich, im Datenbestand des Einwohnermelderegisters auf den Geburtsnamen eines adoptier-

ten Kindes bei der Auswertung der Sicherungsbänder zurückzugreifen. Dem zuständigen Oberstadtdirektor wurde empfohlen sicherzustellen, daß ein erforderliches Löschen von Daten auch aus allen Sicherungsbeständen nach spätestens einem halben Jahr abgeschlossen ist.

Erst nach Einschaltung des Innenministeriums und ausführlichen Gesprächen war der zuständige Oberstadtdirektor bereit, das eingesetzte Programm so zu ändern, daß alle Daten, die nach vollzogener Adoption nicht mehr relevant sind, spätestens innerhalb eines halben Jahres auch auf den Sicherungsbändern gelöscht werden. Da dieses Programm ebenfalls bei anderen Gemeinden in Nordrhein-Westfalen eingesetzt wird, ist es damit gelungen, die bestehende Gefahr für das Adoptionsgeheimnis auch dort zu beseitigen.

Wenn ein Programm zu einer rechtswidrigen Datenverarbeitung zwingt, ist die Nutzung des Programms unzulässig. Soweit der Programmfehler nicht innerhalb kurzer Zeit zu beheben ist, ist für die Datenverarbeitung auf ein anderes Programm zu wechseln.

2.6 Datenschutzgerechter Umgang mit Schriftgut

2.6.1 Aufbewahrung von Asservaten

Werden in Verfahren große Mengen von Unterlagen beschlagnahmt, ist ein besonderes Augenmerk auf einen lückenlosen Nachweis zu legen. Können persönliche Akten teilweise nicht zurückgegeben werden, kann dies zu erheblichen Nachteilen für den Einzelnen führen.

Ein Bürger machte geltend, daß eine Staatsanwaltschaft bei ihm und seinem Steuerberater im Rahmen eines Strafverfahrens beschlagnahmte Aktenordner und sonstige Unterlagen nach Einstellung des Ermittlungsverfahrens nicht vollständig zurückgegeben habe. Es mußte festgestellt werden, daß eine ordnungsgemäße Asservierung der beschlagnahmten Unterlagen mit personenbezogenen Daten durch die Staatsanwaltschaft nicht erfolgt war. Die Staatsanwaltschaft hatte mit der Übernahme des Verfahrens eine Überprüfung der zu den Sachakten gehörenden Asservate nicht vorgenommen. So sah sie sich bei der Rückgabe nicht mehr in der Lage mit Sicherheit festzustellen, ob ein einzelner Ordner in Verlust geraten war und wo aus einer Akte entnommene Unterlagen verblieben waren. Sie hat damit geltende organisatorische Regelungen nicht beachtet (insbesondere § 2 Abs. 1 und Abs. 3 der Anweisung für die Behandlung der im amtlichen Gewahrsam gelangten Gegenstände [AV d. JM v. 25.08.1981, 1454 - I B. 153]).

Gegenüber dem Justizministerium des Landes Nordrhein-Westfalen wurde angeregt, die Gewahrsamssachenanweisung zu überarbeiten und zu verfügen, daß personenbezogene Asservatenunterlagen der besonders gesicherten Aufbewahrung entsprechend Abschnitt C der Gewahrsamssachenanweisung zuzuordnen sind. Dem ist das Justizministerium jedoch nicht gefolgt. Im Hinblick auf große Strafverfahren (beispielsweise in Wirtschaftsstrafsachen) wird der Aufwand als unverhältnismäßig und damit als nicht erforderlich im Sinne von § 10 Abs. 1 DSG NW angesehen.

Auch weiterhin muß erhöhte Sorgfalt bei der Verarbeitung von personenbezogenen Daten, verbunden mit entsprechenden Datenschutz- und Kontrollmaßnahmen, angemahnt werden.

2.6.2 Vernichtung von Unterlagen

Bei der Vernichtung von Unterlagen ist den öffentlichen Stellen oft nicht klar, daß ihre Verantwortung erst dann endet, wenn die Unterlagen vernichtet sind, daß heißt als "gelöscht" im Sinne des § 3 Abs. 2 Ziff. 6 DSG NW gelten können. Gerade die Vergabe eines Auftrags zur Vernichtung von Unterlagen an Dritte setzt eine besondere Sorgfalt voraus. Es kommt leider immer wieder vor, daß Schriftstücke mit sensiblen Verwaltungsdaten, die durch eine Firma vernichtet werden sollten, Dritten unberechtigterweise zur Kenntnis gelangen.

Ein Bürger übersandte Durchschriften von behördlichen Bescheinigungen einer Stadt, die zwar gestückelt waren, auf denen jedoch noch immer datenschutzrelevante Informationen erkennbar waren. Diese Unterlagen, die offensichtlich vernichtet werden sollten, wurden als Schreibblock in einer Justizvollzugsanstalt an Gefangene ausgegeben.

Die Stadt hatte die Unterlagen zur "datenschutzgerechten Vernichtung" an eine private Firma weitergegeben. Sie stellte sich auf den Standpunkt, daß ein Verstoß gegen Vorschriften des Datenschutzes nicht vorläge, da das Aktengut in datenschutzwidriger Weise erst an die Öffentlichkeit gelangt sei, nachdem es das Rathaus verlassen habe.

Die Stadt mußte darauf hingewiesen werden, daß das Vernichten von Unterlagen das Unkenntlichmachen von gespeicherten Daten ist und somit als "Löschen" eine Phase der Datenverarbeitung (§ 3 Abs. 2 DSG NW) darstellt. Auch wenn einer Privatfirma von der Stadt ein Auftrag zur Vernichtung der Unterlagen erteilt wird, bleibt sie als Auftraggeberin gemäß § 11 Abs. 1 DSG NW für die Einhaltung der Vorschriften des DSG NW und anderer Vorschriften über den Datenschutz verantwortlich. Ihre Verantwortung bleibt solange bestehen bis die Unterlagen als vernichtet angesehen werden können und der Vorgang der Datenverarbeitung damit abgeschlossen ist. Die Einhaltung der datenschutzrechtlichen Bestimmungen bis zu diesem Zeitpunkt ist durch geeignete Maßnahmen sicherzustellen. Sicherungsmaßnahmen, die sich nur bis zur Grenze des Behördengrundstücks erstrecken, obwohl die Vernichtung der Unterlagen an einem anderen Ort erfolgen soll, reichen nicht aus. Auch die "Weiterreichung" der gesetzlich normierten Verantwortung für die Einhaltung der datenschutzrechtlichen Bestimmungen an den Auftragnehmer durch die Verpflichtung auf eine "datenschutzgerechte Vernichtung" reicht als Maßnahme nicht aus. Das Gesetz hat vielmehr dieser besonderen Verantwortung des Auftraggebers in einer Reihe von Vorschriften Rechnung getragen, zum Beispiel in § 11 Abs. 1, 3 DSG NW.

Löschen:
Als Hilfsmittel bei der Beurteilung der Frage, ob eine Unterlage nach ihrer Zerkleinerung durch einen Aktenvernichter als vernichtet und damit als "gelöscht im Sinne von § 3 Abs. 2 Ziffer 6 DSG NW angesehen werden kann, sollte die Norm DIN 32757 (Vernichten von Informationsträgern) herangezogen werden.

Hinweise für eine unter dem Gesichtspunkt der Datensicherheit angemessene Vertragsgestaltung bei der Vernichtung von personenbezogenen Unterlagen können dem 11. Tätigkeitsbericht (S. 151 bis 155) entnommen werden.

Wegen der dargestellten Problematik ist aber aus datenschutzrechtlicher Sicht die Vernichtung der Unterlagen durch die öffentliche Stelle der Vergabe an ein privates Unternehmen vorzuziehen.

Die Verantwortung der öffentlichen Stelle für ihr Schriftgut besteht bis zu dessen vollständiger Vernichtung.

2.6.3 Postversand

Bei der Versendung ihrer Post lassen öffentliche Stellen häufig die Sorgfalt vermissen, die erforderlich ist, um den gesetzlichen Bestimmungen über den Datenschutz Rechnung zu tragen. Dies kann dazu führen, daß Dritte von sensiblen Inhalten der Schreiben Kenntnis erlangen.

Aus mehreren Beschwerdeschreiben wurden auch im aktuellen Berichtszeitraum Mängel beim datenschutzgerechten Postversand deutlich. Neben schlichten Versehen mußten allerdings auch Datenschutzverstöße festgestellt werden, deren Grundlage in der systematischen Verfahrensweise der jeweiligen öffentlichen Stelle bestand. Dies betrifft beispielsweise die Gestaltung von Vordrucken, wenn der Inhalt eines Schreibens zum Teil bereits im Adreßfenster sichtbar wird. Auch die Wahl des Materials oder die Ausführung einer Perforation kann die Ursache dafür sein, daß - wie geschehen - Bußgeldbescheide durch unberechtigte Personen eingesehen werden können. Datenschutzrechtlich unzulässig ist es ebenfalls, Postkarten für Empfangsbekenntnisse mit sensiblen personenbezogenen Daten wie zum Beispiel Namen, konkrete Benennung der Angelegenheit, Hinweis auf Regreßforderungen und ähliches vorzusehen.

In einem anderen Fall erwies sich das automatische Verschließen und Frankieren der ausgehenden Post nicht als fehlerfrei. Die stichprobenweise Prüfung der ausgehenden Post bot keine hinreichende Gewähr dafür, daß die Schreiben mit sensiblen personenbezogenen Daten in verschlossenen Briefumschlägen versandt wurden. In allen diesen Fällen wurden Empfehlungen zur Verbesserung der Datensicherheit ausgesprochen.

Angesichts der zwischenzeitlichen Privatisierung der Deutschen Post AG und dem Wettbewerb am Markt, rücken Fragen zu einem Versand mittels privater Unternehmen in den Blickpunkt. So habe ich mich zur Frage der Zulässigkeit des Einsatzes privater Zustell- oder Kurierdienste beim Versand von Anträgen auf Ausstellung von Pässen und Personalausweisen an die Bundesdruckerei der Auffassung des Bundesministeriums des Inneren angeschlossen, wonach private Zustell- oder Kurierdienste mit dem Versand nur dann zu beauftragen sind, wenn auf Grund eines Einzelnachweis- und Quittungssystems sowohl der Transportweg als auch der Erhalt jeder einzelnen Sendung nachgewiesen und in der Posteingangsstelle der Bundesdruckerei kontrolliert und dokumentiert werden kann. Das Innenministerium des Landes Nordrhein-Westfalen hat dies dem nachgeordneten Bereich mit der Bitte um Beachtung zur Kenntnis gebracht.

Auch beim Massengeschäft des Versands von Unterlagen mit personenbezogenen Daten durch öffentliche Stellen ist sicherzustellen, daß eine unbefugte Einsichtnahme nicht erfolgen kann.

3. Medien - Datenautobahn mit erhöhtem Unfallrisiko

Auf dem Weg in die moderne Informationsgesellschaft und in einer sich schnell verändernden Medienwelt ist das Schlagwort "Multimedia" ein zentraler Begriff. Die Digitalisierung und zunehmende Vernetzung hat die Informations- und Kommunikationstechnik, aber auch die Medien und ihre Nutzung bereits stark verändert. Die Verbreitung mobiler Sprach- und Datenübertragungsdienste hat zugenommen. Eine Vielfalt neuer elektronischer Dienste wird bereits breit genutzt. Telebanking und Teleshopping sind Begriffe, die den Wandel aufzeigen. Die zunehmende Nutzung von elektronischer Post, von Videokonferenzen und elektronischen Buchungsdiensten birgt ebenso Probleme für den Datenschutz wie der inzwischen von vielen vorgenommene Anschluß an das Internet. Durch die Veränderung in der Medienwelt ist der Rundfunkbegriff konkretisierungsbedürftig und die Abgrenzung zu neuen Diensten notwendig geworden.

Bei der Nutzung der neuen Kommunikationsmöglichkeiten werden personenbezogene Daten preisgegeben und Spuren in vernetzten Systemen hinterlassen. Zum einen sind es die Verbindungs- und Abrechnungsdaten. Zum anderen werden bei der Benutzung der Systeme aber auch Daten über den Zugriff auf bestimmte Informationen festgehalten, deren Auswertung zur Erstellung von Nutzungsprofilen mißbraucht werden kann. So läßt sich beispielsweise aus den gespeicherten Daten erkennen, wer sich welche Filme oder auch politischen Sendungen ansieht, wer welche Videos oder Information abgerufen hat, wer zu welchen Banken Kontakte aufgenommen hat, wer bei welchen Geschäften welche Waren bestellt oder wer bei welchen Reiseveranstaltern welche Reisen gebucht hat.

Die Datenschutzbeauftragten haben sich in den letzten Jahren mehrfach mit der Problematik befaßt, wie bei der Nutzung neuer Technologien der Schutz der Privatsphäre sichergestellt und das Recht auf informationelle Selbstbestimmung gewährleistet werden kann. Einige wichtige Vorgaben für einen wirkungsvollen Datenschutz sind

- der Grundsatz der **Datenvermeidung**, der bedeutet, daß nicht erforderliche personenbezogene Daten gar nicht erst erhoben werden und die Nutzerinnen und Nutzer somit so wenig Spuren wie möglich hinterlassen,
- die Verarbeitung der Daten einer strengen **Zweckbindung** zu unterwerfen und damit auf die den Betroffenen bekannten und von ihnen gebilligten Zwecke zu beschränken,

- die **Transparenz der Datenverarbeitung**, damit für die Betroffenen jederzeit erkennbar bleibt, in welcher Form die Verarbeitung ihrer Daten unter welchen Sicherheitskriterien erfolgt und
- die Sicherstellung **anonymer Zugänge** und anonymer **Abrechnungsverfahren**, etwa durch vorbezahlte Wertkarten, bei denen Gebühren für in Anspruch genommene Leistungen direkt von den Guthabenkarten abgebucht werden können, wodurch die Speicherung personenbezogener Daten weitgehend entfällt.

Bereits in der Entwicklung und Erprobung müssen Datenschutz- und Datensicherungsgesichtspunkte wesentliche Bestandteile von Pilotprojekten sein. Unabdingbar sind Information und Aufklärung über die Risiken der neuen Techniken, damit es den Nutzerinnen und Nutzern möglich ist, selbst zu entscheiden, ob und inwieweit sie eine Verarbeitung ihrer personenbezogenen Daten zulassen wollen oder nicht.

Datenverarbeitung, Telekommunikation, Informations- und Kommunikationsdienste, Hörfunk, Fernsehen und Mediendienste gehen zunehmend ineinander über und sind kaum noch klar voneinander abgrenzbar. Hinzu kommt die Aufhebung früherer Monopole im Rahmen der Postreform, die zu einer Neuordnung des Telekommunikationsmarktes geführt hat. Durch gesetzgeberische Aktivitäten wurde und wird versucht, die neuen Kommunikations- und Informationsstrukturen zu ordnen. Derzeit entsteht ein kompliziertes Regelungsgeflecht, das nicht zuletzt den unterschiedlichen Bundes- und Landeskompetenzen geschuldet ist. Dabei geht es um das Zusammenspiel des Telekommunikationsgesetzes (TKG) sowie der Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV) mit dem geplanten Informations- und Kommunikationsdienste-Gesetz (IuKDG), das selbst wiederum aus mehreren Einzelgesetzen bestehen soll, und dem Mediendienste-Staatsvertrag. Auslegungsprobleme und Abgrenzungsschwierigkeiten scheinen vorprogrammiert zu sein. Das Landesrundfunkgesetz wird zudem als Grundlage für Pilotprojekte im Medienbereich herangezogen. Zu den Regelungen im einzelnen:

Das 1996 verabschiedete **Telekommunikationsgesetz (TKG-BGBl. I, S. 1120)** stellt in § 85 Abs. 2 TKG die Einhaltung des **Fernmeldegeheimnisses** für den Fernmeldeverkehr privater Telefongesellschaften sicher. Unter Strafandrohung verboten ist nunmehr auch das unbefugte Abhören von Funkdiensten, wozu beispielsweise das Abhören schnurloser Telefone gehört (§§ 86, 95 TKG). Ebenfalls sind die Rechte der Kundinnen und Kunden bei der **Eintragung in Telefonverzeichnisse** gestärkt worden. So besteht gegenüber den Diensteanbietern jetzt die abgestufte Entscheidungsmöglichkeit, ob überhaupt eine Eintragung erfolgen soll und, sofern eine solche beantragt wird, welche

Angaben in Kundenverzeichnissen veröffentlicht werden sollen, ferner ob die Eintragung nur in gedruckten oder auch in elektronischen Verzeichnissen erfolgen soll (§ 89 Abs. 8 TKG).

Die Pflicht der Anbieter von Telekommunikationsdiensten, aktuelle Kundendateien zu führen und diese für den Zugriff der Regulierungsbehörde in einem automatisierten Abrufverfahren vorzuhalten (§ 90 Abs. 2 TKG), ist bereits unter 1. dargestellt worden. Die Sicherheits- und Strafverfolgungsbehörden, die Nachrichtendienste und andere Stellen können die Daten aus den Kundendateien jedoch nicht nur nach § 90 Abs. 4 TKG über die Regulierungsbehörde bekommen, sondern nach § 90 Abs. 3 TKG auch direkt von den Anbietern erhalten. Zudem können sie nach § 89 Abs. 6 TKG im Einzelfall auch auf die personenbezogenen Daten zugreifen, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses vom Anbieter erhoben worden sind. Diese umfassenden **Überwachungsmöglichkeiten** sind für sich genommen schon äußerst bedenklich. Verfassungsrechtlich zumindest zweifelhaft dürfte jedenfalls sein, daß das Gesetz es ausschließt, den Kundinnen und Kunden eine Mitteilung über die zu ihrer Person erteilten Auskünfte zu geben.

Die erst im Juli 1996 erlassene **Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV - BGBl. I, S. 982)** ist nach der Verabschiedung des TKG schon wieder anpassungsbedürftig. Die TDSV enthält gegenüber der früheren Rechtslage zwar schon einige Verbesserungen des Datenschutzes und eröffnet den Kundinnen und Kunden unter anderem Wahlrechte im Umgang mit ihren personenbezogenen Daten - so beispielsweise für die Eintragung in öffentliche Verzeichnisse -, doch wird auf der Grundlage der in § 89 TKG enthaltenen Ermächtigung eine **neue Telekommunikationsdienstunternehmen-Datenschutzverordnung** erlassen werden müssen. Durch die Digitalisierung der Telekommunikation sind im Vergleich zum herkömmlichen Telefonverkehr ganz neue Gefahren für das Grundrecht der Bürgerinnen und Bürger auf unbeobachtete Kommunikation entstanden, da in viel größerem Maße Datenspuren hinterlassen werden. Gerade auch in Mobilfunknetzen darf es keinen geringeren Datenschutz als in den traditionellen Festnetzen geben. Regelungsbedürftig sind insbesondere der auf das Erforderliche zu beschränkende Umfang der zulässigen Datenerhebung, Datenverarbeitung und -nutzung durch die Diensteanbieter, aber auch die Gewährleistung der Zweckbindung sowie die Festlegung von Fristen für die Löschung der Verbindungsdaten.

Die neuen Informations-, Kommunikations-, Tele- und Mediendienste erfassen nicht nur in weitem Maße die private Lebensgestaltung, sie haben vielmehr auch Auswirkungen auf viele Wirtschaftsbereiche. Erforderlich sind einheitli-

che rechtliche Rahmenbedingungen, die den Verbraucherschutz und die Rechte der Nutzerinnen und Nutzer zum Schutz ihrer personenbezogenen Daten sicherstellen. Die Zuständigkeit des Bundes für die Regelung der **Teledienste** und die Zuständigkeit der Länder für die Regelung der **Mediendienste** darf nicht dazu führen, daß ein unterschiedliches Datenschutzniveau für die jeweiligen Dienste festgelegt wird, zumal die Abgrenzung der Dienste voneinander ohnehin Probleme aufwerfen wird. Inzwischen liegen der Entwurf eines Informations- und Kommunikationsdienste-Gesetzes (IuKDG) der Bundesregierung und der Entwurf eines Mediendienste-Staatsvertrages der Länder vor. Mit beiden Entwürfen sollen grundlegende rechtliche Bedingungen für Angebot und Nutzung der neuen Dienste festgelegt werden.

Der **Entwurf des Informations- und Kommunikationsdienste-Gesetzes (IuKDG)** enthält als Artikelgesetz unter anderem folgende Gesetzentwürfe:

- Gesetz über die Nutzung von Telediensten (Teledienstegesetz - TDG)
- Gesetz über den Datenschutz bei Telediensten (TDDSG)
- Gesetz zur digitalen Signatur (Signaturgesetz - SigG).

Der **Teledienstegesetzentwurf (TDG)** erstreckt den Anwendungsbereich seiner Vorschriften auf alle elektronischen Informations- und Kommunikationsdienste, die durch Übermittlung mittels Telekommunikation die individuelle Nutzung von kombinierbaren Daten wie Zeichen, Sprache, Bilder, Töne oder Texte ermöglichen, und zwar unabhängig davon, ob dies ganz oder teilweise unentgeltlich oder gegen Entgelt erfolgt.

Inhaltlich als **Teledienste** erfaßt werden unter anderem Angebote

- im Bereich der Individualkommunikation wie Datenaustausch oder Telebanking,
- beim Einsatz und der Nutzung im Waren- und Dienstleistungsbereich wie beispielsweise Datendienste für Verkehrs-, Wetter-, Umwelt- oder Börsendaten sowie die Verbreitung von Informationen über Waren und Dienstleistungsangebote,
- zur Nutzung des Internets oder anderer Netze,
- zum elektronischen Abruf von Waren und Dienstleistungen in Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit wie beispielsweise beim Teleshopping oder auch beim Bezug von Presseinformationen.

Da die Regelungsbefugnis des Bundes durch die Zuständigkeit der Länder eingeschränkt ist, gilt das Teledienstegesetz nicht für den Rundfunk im Sinne des Rundfunkstaatsvertrages und die Mediendienste im Sinne des Entwurfs des Mediendienste-Staatsvertrages.

Der **Teledienstedatenschutzgesetzentwurf (TDDSG)** regelt den Schutz personenbezogener Daten bei Telediensten im Sinne des Teledienstegesetzes. Er stellt wesentliche Grundsätze für die Verarbeitung personenbezogener Daten auf, die weitgehend die von den Datenschutzbeauftragten aufgestellten Forderungen zum Schutz des Rechts auf informationelle Selbstbestimmung berücksichtigen. Zu begrüßen ist der im Gesetzentwurf festgeschriebene Grundsatz der **Datenvermeidung**. Damit ist die Ausgestaltung und Auswahl technischer Einrichtungen an dem Ziel auszurichten, keine oder sowenig wie möglich personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen. Weitere wichtige Grundsätze sind, daß die **Anonymität** der Nutzerinnen und Nutzer soweit wie möglich gewahrt werden muß und daß, soweit die Erhebung und Nutzung von personenbezogenen Daten im Rahmen eines Vertragsverhältnisses erfolgt, dies nur unter strenger **Zweckbindung** im Rahmen des Vertragszwecks geschehen darf. Zum Schutz der personenbezogenen Daten ist im übrigen sicherzustellen, daß der nicht autorisierte Zugriff auf diese Daten durch geeignete technische Maßnahmen ausgeschlossen wird.

Die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses über die Nutzung von Telediensten erforderlichen personenbezogenen Daten definiert der Gesetzentwurf als **Bestandsdaten**. Diese Bestandsdaten dürfen beispielsweise für Werbungs- oder Marktforschungszwecke nur mit der ausdrücklichen **Einwilligung** der Nutzerinnen und Nutzer verwendet werden. Keinen Schutz sollen die Bestandsdaten allerdings nach § 5 Abs. 3 des Gesetzentwurfs dann genießen, wenn sie für die Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes sowie des Zollkriminalamtes erforderlich sind. Dann sind die Diensteanbieter im Einzelfall zur Übermittlung der Bestandsdaten ihrer Kundinnen und Kunden an die ersuchende Stelle verpflichtet. Das bedeutet, daß den Polizeien und Strafverfolgungsbehörden, den Nachrichtendiensten und sogar Verwaltungsbehörden die personenbezogenen Daten durch die Diensteanbieter zu übermitteln sind.

Da die Teledienste als moderne Informations- und Kommunikationsdienste herkömmliche Druckerzeugnisse ergänzen und ersetzen, ist nicht ersichtlich, warum Angebote in elektronischer Form anders als herkömmliche Angebote in

gedruckter Form behandelt werden sollen, für deren Anbieter eine derartige Auskunftspflicht über ihre Abonnentinnen und Abonnenten nicht besteht. Auch sind vergleichbare Übermittlungspflichten von Leistungsanbietern hinsichtlich ihrer Kundinnen und Kunden in anderen Wirtschaftsbereichen nicht bekannt.

Würde diese Regelung tatsächlich in Kraft treten, wären beispielsweise Anbieter von Homebankingdiensten oder von Onlinezeitungen verpflichtet, der Polizei und selbst Verwaltungsbehörden außerhalb von strafrechtlichen Ermittlungsverfahren, beispielsweise für die Verfolgung von Ordnungswidrigkeiten, Auskunft über die Nutzerinnen und Nutzer ihrer Dienste zu geben. Dies geht weit über die bisherige Rechtslage hinaus und ist insbesondere wegen der **stärkeren Überwachbarkeit des Nutzungsverhaltens** und des intensiven **Eingriffs** in die grundrechtlich geschützte **Informations- und Meinungsfreiheit** nicht akzeptabel. Angesichts der bereits ausreichend vorhandenen Eingriffsbefugnisse nach der Strafprozeßordnung und den Polizeigesetzen ist auch kein Bedarf für die vorgesehene Regelung erkennbar.

Die Länder haben es glücklicherweise **abgelehnt**, eine entsprechende Regelung in den Entwurf des Staatsvertrages über Mediendienste aufzunehmen. Da in den Verhandlungen zwischen Bund und Ländern gerade auch die Absicht verfolgt wurde, in datenschutzrechtlicher Hinsicht eine unterschiedliche Behandlung der Nutzerinnen und Nutzer von Telediensten einerseits und Mediendiensten andererseits möglichst zu vermeiden, sollte § 5 Abs. 3 des Entwurfs für ein Teledienstedatenschutzgesetz ersatzlos gestrichen werden.

In einem früheren Stadium des Gesetzentwurfs war eine Regelung des sogenannten **Datenschutz-Audits** vorgeschlagen, wie sie im Entwurf für einen **Mediendienste-Staatsvertrag** der Länder nach wie vor enthalten ist. Danach können zur Verbesserung von Datenschutz und Datensicherheit Anbieter von Mediendiensten ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten sowie das Ergebnis der Prüfung veröffentlichen lassen. Zur Gewährleistung eines verbesserten Datenschutzes und im Hinblick auf eine einheitliche Behandlung von Telediensten und Mediendiensten sollte eine vergleichbare Regelung für Teledienste vorgesehen werden. Damit hätten die Anbieter von Telediensten wie die Anbieter von Mediendiensten die Möglichkeit, Datenschutz als Qualitätsmerkmal ihrer Produkte werbend umzusetzen. Über den Wettbewerb auch ausländischer Anbieter mit deutschen Anbietern würde das Datenschutz-Audit über den innerstaatlichen Regelungsbereich hinaus insgesamt eine Grundlage für bessere Datenschutzkonzepte schaffen. Nicht zuletzt ist das Datenschutz-

Audit aber auch eine wichtige Ergänzung einer effektiven Datenschutzkontrolle.

Der **Signaturgesetzentwurf (SigG)** soll Rahmenbedingungen für digitale Signaturen schaffen, unter denen diese als sicher gelten und Fälschungen digitaler Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können. Damit soll für die Übertragung und Speicherung digitaler Daten ermöglicht werden, Urheberschaft und Unverfälschtheit der digitalen Daten festzustellen und zu beweisen. Sichere Signaturverfahren sollen die Rechtssicherheit bei Übertragung und Speicherung digitaler Daten gewährleisten und darüber hinaus auch den Schutz für personenbezogene Daten erhöhen. Nach einer § 5 Abs. 3 TDDSG vergleichbaren und ebenfalls nicht zu akzeptierenden Regelung in § 12 Abs. 2 SigG soll die Zertifizierungsstelle allerdings verpflichtet sein, unter anderem der Polizei, den Strafverfolgungsbehörden und den Nachrichtendiensten Daten über die Identität eines Signaturschlüssel-Inhabers mit Pseudonym zu übermitteln. Hierfür fehlt es an einer nachvollziehbaren Begründung. Es ist nicht erkennbar, weshalb über die vorhandenen Eingriffsbefugnisse hinaus eine pauschale Aufdeckung der Pseudonyme gerechtfertigt sein soll. Der Gesetzgeber sollte die vorgesehene Vorschrift daher streichen (zur elektronischen Unterschrift siehe auch unter 2.1.4).

Der Entwurf eines **Mediendienste-Staatsvertrags** der Länder basiert auf der Länderzuständigkeit für Rundfunkfragen und schafft Regelungen für Mediendienste, die vom Bund mangels Zuständigkeit im Teledienstegesetz nicht geregelt werden. Zum Anwendungsbereich des Staatsvertrags gehören Angebot und Nutzung von neuen elektronischen Verteil- und Abrufdiensten, die sich an die Allgemeinheit wenden und nicht unter die Bestimmungen des Rundfunkstaatsvertrags fallen. Dies sind unter anderem Verteildienste in Form von direkten Angeboten an die Öffentlichkeit für den Verkauf oder den Kauf sowie andere Leistungserbringungen im Rahmen des Fernseheinkaufs, Verteildienste in Form von Fernsehtext, Radiotext und vergleichbarer Textdienste sowie Abrufdienste, bei denen Text-, Ton- oder Bilddarbietungen auf Anforderung übermittelt werden. Mit Ausnahme der bereits genannten Abweichungen entsprechen die datenschutzrechtlich bedeutsamen Bestimmungen des Mediendienste-Staatsvertragsentwurfs im wesentlichen denjenigen des Teledienstedatenschutzgesetzentwurfs.

Das Rundfunkgesetz für das Land Nordrhein-Westfalen (LRG NW) läßt die Durchführung von Modellversuchen mit neuen Rundfunktechniken, Rundfunkprogrammen oder Rundfunkdiensten zu. Die Landesregierung hat 1996 von der Ermächtigung in § 72 LRG NW Gebrauch gemacht und eine Verordnung über die Durchführung eines Modellversuchs mit digitalem Fernsehen

und neuen digitalen Kommunikationsdiensten in Nordrhein-Westfalen (**1. Medienversuchsverordnung - 1. MVVO**) sowie eine weitere Verordnung über die Durchführung eines Modellversuchs mit digitalem Hörfunk und neuen digitalen Kommunikationsdiensten in Nordrhein-Westfalen (**2. Medienversuchsverordnung - 2. MVVO**) erlassen. Mit den Modellversuchen sollen Erkenntnisse über die zukünftige Nutzung neuer Techniken, Programme und Dienste gewonnen und dazu beigetragen werden, die publizistischen und wirtschaftlichen Chancen der neuen digitalen Technologien zu erschließen. Ein Versuch in diesem Rahmen ist das inzwischen gestartete Multimedia-Pilotprojekt "Infocity NRW", bei dem mehrere Städte an Rhein und Ruhr durch ein Glasfaserhochgeschwindigkeitsnetz miteinander verbunden sind und in dem angeschlossene Kundinnen und Kunden interaktive Anwendungen wie Telebanking testen, per Bildschirm einkaufen, aber auch örtliche Informationen abrufen können.

In den Stellungnahmen zu den Verordnungsentwürfen habe ich unter anderem eine Präzisierung der von den Verordnungen erfaßten Informations- und Kommunikationsdienste und der damit jeweils verbundenen personenbezogenen Datenverarbeitung gefordert, da die Anforderungen an eine Datenverarbeitung jeweils auf den konkreten Zweck bezogen sein müssen. Nachdrücklich habe ich auch auf die Risiken für das Recht auf informationelle Selbstbestimmung insbesondere der an interaktiven Diensten beteiligten Personen hingewiesen, deren Nutzungsverhalten registriert sowie zu Verhaltens- und Persönlichkeitsprofilen zusammengeführt werden kann. Zu begrüßen ist, daß in beiden Medienversuchsverordnungen der Erkenntnisgewinn über Möglichkeiten zur Verbesserung des Datenschutzes in die Zweckbestimmung der Modellversuche aufgenommen worden ist. Damit ist die Erwartung verbunden, daß sowohl die Auswirkungen, die die Nutzung der Dienste auf das Recht auf informationelle Selbstbestimmung haben wird, als auch die technischen und organisatorischen Anforderungen zur Sicherstellung des Datenschutzes untersucht werden.

4. Einwohnerwesen

Die Daten aller Einwohnerinnen und Einwohner in den Gemeinden werden vor allem beim Standesamt und beim Einwohnermeldeamt verarbeitet. Die der Verarbeitung zugrunde liegenden Vorschriften des Personenstandsgesetzes und des Meldegesetzes bedürfen einer Anpassung an veränderte Erfordernisse der Praxis, wie auch einer Anpassung zur Gewährleistung des Rechts auf informationelle Selbstbestimmung der Bürgerinnen und Bürger. Im Berichtszeitraum habe ich sowohl zur **Novellierung** des **Meldegesetzes** des Landes Nordrhein-Westfalen (siehe unter 1.) als auch zu einem Vorentwurf zur Änderung des **Personenstandsgesetzes** (Stand: 25. März 1996) Stellungnahmen abgegeben.

Der Vorentwurf zur Änderung des **Personenstandsgesetzes** trägt in etlichen Fällen nichts zur Lösung bekannter Datenschutzprobleme bei, sondern weist vielmehr gegenüber früheren Vorentwürfen datenschutzrechtliche Rückschritte auf. So wird der Gedanke der **Transparenz** der Datenverarbeitung im Gesetzentwurf außer acht gelassen, indem die Betroffenen bei der Übermittlung von Informationen an Behörden und bestimmte sonstige Stellen nicht gleichzeitig über derartige Datenübermittlungen unterrichtet werden. Weiter ist etwa auch nicht das Verhältnis der Datenverarbeitung zu Zwecken **wissenschaftlicher Forschung** einerseits und zur Datenverarbeitung im Rahmen von Vorhaben für Ahnenforschung oder zeitgeschichtlicher Forschung andererseits im Gesetz aufgearbeitet worden. Datenschutzprobleme, wie etwa die Frage, wann und unter welchen Voraussetzungen personenbezogene Daten für derartige Vorhaben zur Verfügung gestellt werden können, bleiben nach dem Gesetzentwurf ungelöst. Zusätzlich fehlen präzise Rechtsgrundlagen für die **Mitteilungspflichten** der **Standesbeamten** über Standesamtsfälle an die verschiedenen Behörden und Stellen. Weder der Empfängerkreis ist abschließend genannt, noch der Umfang und Inhalt der Mitteilungen beschrieben, noch der Verwendungszweck festgelegt. Auch die Wahrung des **Adoptionsgeheimnisses** ist unzureichend geregelt. Der Vorentwurf zur Änderung des Personenstandsgesetzes enttäuscht somit Hoffnungen auf die Lösung datenschutzrechtlicher Probleme.

Charakteristisch und gleichzeitig datenschutzrechtlich besonders bedenklich ist, daß die Prüfung der Zulässigkeit einer Datenverarbeitung sich in der Praxis der Standesämter weitgehend an einer Verwaltungsvorschrift orientiert, nämlich der bundeseinheitlichen **Dienstanweisung für Standesbeamte**. So hatte etwa ein Standesamt die Anordnung des Aufgebots einer Bürgerin allein davon abhängig gemacht, daß eine beglaubigte Abschrift oder ein Auszug aus dem Familienbuch vorgelegt wurde. Dies entsprach der Dienstanweisung. Die dem Standesamt von der Bürgerin vorgelegte Abstammungsurkunde wurde als

unzureichend zurückgewiesen, obwohl das Personenstandsgesetz diesen Abstammungsnachweis als gleichwertig ausdrücklich zuläßt.

Einwohnerdaten sind bei allen öffentlichen Stellen ein begehrtes Gut. Eine Datenübermittlung setzt allerdings stets eine verfassungskonforme Rechtsgrundlage voraus. Daran fehlte es einer von einem Kreis eingerichteten Stabsstelle zur **Bekämpfung der Schwarzarbeit**, die per Online-Verbindung auf die Daten der Einwohnermeldeämter, die Daten der Kraftfahrzeugzulassungsstelle, die Daten der Ausländerbehörden sowie die Daten der Sozialämter zugreifen wollte. Gleiches galt für ein Hauptzollamt, das ebenfalls zur Bekämpfung der Schwarzarbeit von allen Bauämtern seines Bezirks in regelmäßigen Abständen Listen über neu genehmigte Bauvorhaben zu erhalten wünschte. Unzulässig ist es auch, Melderegisterauskünfte über Internet zu erteilen.

4.1 Kontrollfreie Bereiche im Einwohnermeldeamt

Datenschutzverstöße bei der Erteilung einfacher Melderegisterauskünfte sind rein tatsächlich nicht kontrollierbar, da viele Meldebehörden derartige Auskünfte nicht dokumentieren.

Auch in diesem Berichtszeitraum gab es in verschiedenen Gemeinden wieder Fälle, in denen Bürgerinnen und Bürger sich darüber beklagten, daß die Gemeinde ihnen die Frage nicht beantworten konnte, welche Auskünfte über sie an Dritte gegeben worden waren. Dies hat seine Ursache darin, daß die Gemeinden ihre Auskunftserteilung nicht protokollieren. Daher ist auch eine effiziente Datenschutzkontrolle in diesem Bereich nicht möglich. Die Führung solcher Protokolle ist bereits mehrfach erfolglos angemahnt worden. Auch das Innenministerium ist bislang bedauerlicherweise nicht tätig geworden. Dabei kann der von den Gemeinden vorgenommene Verweis auf hohe Fallzahlen nicht überzeugen, da beispielsweise im polizeilichen Informationssystem trotz hoher Fallzahlen eine Protokollierung erfolgt, die die Kontrolle von Fehlern und die Aufdeckung von Mißbrauchsfällen ermöglicht.

In der Vergangenheit ist dieser Datenschutzmangel gegenüber einigen Gemeinden förmlich beanstandet worden, ohne daß dies Wirkung gezeigt hätte. Wenige Gemeinden haben sich von der Notwendigkeit einer ausreichenden Dokumentation der Melderegisterauskünfte überzeugen lassen, doch besteht überwiegend noch der aufgezeigte datenschutzrechtliche Notstand.

Das Innenministerium bleibt aufgerufen, dafür Sorge zu tragen, daß bei den Einwohnermeldeämtern die Datenübermittlung an Dritte nachprüfbar dokumentiert wird.

4.2 Diskriminierung Transsexueller

Eine Diskriminierung Transsexueller kann auch bereits in einer scheinbar korrekten Anrede liegen.

Einer der körperlichen Geschlechtszugehörigkeit nach männlichen Person war durch Entscheidung des zuständigen Amtsgerichts nach dem Transsexuellengesetz gestattet worden, einen weiblichen Vornamen zu führen. Die Stadtverwaltung sah sich auf Grund dessen, daß eine Operation zur Geschlechtsumwandlung nicht durchgeführt worden sei, verpflichtet, diese Person im Rahmen eines Verwaltungsvorganges im Adressenfeld mit "Herrn Monika X" anzuschreiben und im Brief selbst mit "Sehr geehrter Herr X" anzureden. Einer hierzu eingeholten Stellungnahme des Innenministeriums war zu entnehmen, daß von einer Gemeinde nicht verlangt werden könne, eine Anrede zu verwenden, die objektiv im Widerspruch zu dem im Melderegister gespeicherten körperlichen Geschlecht der betroffenen Person stehe.

Demgegenüber vertrete ich die Auffassung, daß für die Adressierung eines Bescheides als personenbezogene Daten zur Aufgabenerfüllung der Gemeinde lediglich **Vorname, Name und Anschrift** erforderlich sind. Der Angabe weiterer Daten bedarf es nicht. Als Ausdruck der Höflichkeit ist es zwar üblich, auch die Anrede "Herr" oder "Frau" zu verwenden, doch darf die Anrede insoweit nicht die Qualität eines eigenen personenbezogenen Datums erreichen. Diese Qualität wird nur dann nicht erreicht, wenn die in der Anrede liegende Aussage erkennbar nicht über den erforderlichen Inhalt der Adressierung hinausgeht. **Dies setzt zwingend voraus, daß die Anrede sich allein an den geschlechtsspezifischen Vornamen der anzuschreibenden Person ausrichtet.** Nur dann enthält die Anrede keine zusätzliche eigene Aussage und Information über die Person; insbesondere nicht eine Information über ihr körperliches Geschlecht. Eine solche Zusatzinformation ist weder für die Adressierung noch für die Anrede im Schreiben erforderlich und damit unzulässig.

Hinzu kommt, daß durch die unzulässige Angabe des Geschlechts gegen das Ausforschungsverbot des Transsexuellengesetzes verstoßen wird. Das Auseinanderfallen von geschlechtsspezifischen Vornamen und dem tatsächlichen körperlichen Geschlecht kann nur in den Fällen einer Entscheidung des Gerichts nach den Vorschriften des Transsexuellengesetzes auftreten. Unzulässigerweise wird somit zugleich die Information übermittelt, die betroffene Person habe eine Entscheidung nach dem Transsexuellengesetz auf Änderung der Vornamen durchgeführt.

Die betroffene Stadt ist meiner Beanstandung gefolgt.

4.3 Gruppenauskünfte über EU-Bürgerinnen und -Bürger an politische Parteien

Eine Differenzierung zwischen Deutschen und Angehörigen anderer Staaten der Europäischen Union ist bei einer zulässigen Offenbarung von Meldedaten gegenüber den politischen Parteien nach der derzeit geltenden Rechtslage ausgeschlossen.

Im Vorgriff auf die Kommunalwahlen 1999 hat eine Gemeinde angefragt, ob es möglich sei, politischen Parteien eine Adressenliste der nicht-deutschen EU-Bürgerinnen und Bürger zukommen zu lassen. Die politische Partei wolle diesen Personenkreis gezielt ansprechen, um sie zu einer politischen Mitarbeit für die kommende Legislaturperiode zu gewinnen.

Auf der Grundlage des § 35 des Meldegesetzes für das Land Nordrhein-Westfalen (Meldegesetz NW - MG NW), der die entsprechende Datenübermittlung an politische Parteien im Zusammenhang mit Kommunalwahlen regelt, ist für die Zusammensetzung der Gruppe der Wahlberechtigten das Lebensalter der Betroffenen bestimmend. Hieraus wird deutlich, daß das Datum "Staatsangehörigkeit" nicht als Kriterium für die Gruppenauskunft gewählt werden darf. Auf der Grundlage von § 35 Abs. 1 Satz 1 MG NW ist daher eine derartige Auskunft nicht zulässig. Da diese Vorschrift Gruppenauskünfte im Zusammenhang mit Kommunalwahlen abschließend spezialgesetzlich regelt, scheidet auch ein Rückgriff auf § 34 Abs. 3 MG NW aus. Eine Datenübermittlung an die Parteien wäre deshalb nur mit ausdrücklicher schriftlicher Einwilligung der einzelnen Betroffenen möglich (§ 4 Satz 1 Buchstabe b DSG NW).

4.4 Auskunft bei bestehender Auskunftssperre

Die Auskunft über eine durch eine Auskunftssperre im Melderegister geschützte Person darf nicht die Tatsache der Auskunftssperre erkennen lassen.

Von einer Bezirksregierung war unter Berufung auf das Innenministerium die Auffassung vertreten worden, daß bei einem Auskunftsersuchen zu einem Datensatz mit Auskunftssperre den Auskunftsuchenden das Bestehen einer Auskunftssperre mitzuteilen wäre. Mit dem Hinweis auf die Auskunftssperre wird allerdings schon eine **Teilauskunft** erteilt, nämlich der Wohnort bekanntgegeben. Dies ist unzulässig. Für Auskunftssperren, die dem Schutz des Adoptionsgeheimnisses dienen, hat das Innenministerium im übrigen bereits

seit 1985 durch Erlaß verfügt, daß die Antwort in derartigen Fällen zu lauten habe: "hier nicht gemeldet.". Nichts anderes kann für Auskunftssperren bei Gefahr für Leben, Gesundheit, persönliche Freiheit oder für ähnliche schutzwürdige Belange gelten.

5. Ausländerangelegenheiten

Die datenschutzrechtlichen Bedenken gegen die umfangreiche Verarbeitung personenbezogener Daten von Ausländerinnen und Ausländern im **Ausländerzentralregister** sind bereits mehrfach dargelegt worden (vgl. 12. Tätigkeitsbericht, Seite 9/10). Ein besonderes Problem ist die **Aktualität** der **gespeicherten Daten** und die Bereinigung des Registers von (alten) Datensätzen. Ist etwa eine Ausländerin oder ein Ausländer im Besitz einer gültigen Aufenthaltsberechtigung und ein alter Datensatz mit einer Abschiebungsandrohung nicht gelöscht, so kann dies zu erheblichen Belastungen für die betroffene Person - etwa bei Grenzübertritten - führen.

Zur Beteiligung von Ausländerinnen und Ausländern am demokratischen Willenbildungsprozeß auf kommunaler Ebene gehört die Durchführung von **Ausländerbeiratswahlen**. Bei der Vorbereitung und Durchführung solcher Wahlen darf der Datenschutz nicht verletzt werden. Das aber würde geschehen, wenn die Kennzeichnung des Inhalts der Wahlbriefe auf dem **Briefumschlag** in der Weise erfolgen würde, daß dadurch Dritte erst die Ausländereigenschaft der Adressaten erfahren.

Auch wenn es vielleicht wünschenswert erscheinen mag, im Rahmen der Berichterstattung zur Ausländerbeiratswahl eine Aufbereitung der Wahlberechtigten nach Altersgruppen, Geschlecht und Nationalität in aggregierter Form vorzunehmen, so ist die hierfür erforderliche Auswertung des Wählerverzeichnisses durch das Amt für **Statistik** in der Gemeindeverwaltung wegen Fehlens der für diese Datenverarbeitung notwendigen Rechtsgrundlage nicht möglich. Weder in § 27 c der Gemeindeordnung für das Land Nordrhein-Westfalen (GO NW), der das Recht der Ausländerbeiräte regelt, noch in den Vorschriften des Kommunalwahlgesetzes, die in § 27 Abs. 11 GO NW für entsprechend anwendbar erklärt werden, ist eine solche Erlaubnisnorm enthalten.

Besondere datenschutzrechtliche Bedenken bestehen gegen die Verwendung von Fragebogen einiger deutscher Auslandsvertretungen zum Ausschluß von sogenannten Scheinehen wegen der darin enthaltenen unzulässigen intimen Fragen.

Aus anderen Bundesländern wurde durch Hinweise der dortigen Landesbeauftragten für den Datenschutz die Praxis einiger Auslandsvertretungen der Bundesrepublik Deutschland bekannt, Ausländerbehörden Fragebogen zu sogenannten Scheinehen zu übersenden, die von diesen unter Beteiligung der Betroffenen auszufüllen waren. Da es sich bei den Auslandsvertretungen um

Bundesbehörden handelt, geht diesem Sachverhalt der Bundesbeauftragte für den Datenschutz nach.

Auf Nachfrage haben verschiedene Ausländerbehörden Nordrhein-Westfalens versichert, daß bei der Überprüfung, ob es sich bei Eheschließungen zwischen deutschen und ausländischen Staatsangehörigen eventuell um sogenannte Scheinehen handeln könnte, kein Fragebogen als Entscheidungshilfe verwandt werde. In solchen Fällen werde in der Regel in einem persönlichen Gespräch mit beiden Ehepartnern unter Respektierung der Privat- und Intimsphäre versucht, eine eindeutige Klärung zu finden.

Bei einem Kontrollbesuch einer der Ausländerbehörden konnten allerdings keine konkreten Überprüfungsfälle vorgelegt werden unter Hinweis auf die hohe Zahl der Ausländerakten und einer fehlenden gesonderten Erfassung dieser Fälle. Nunmehr hat sich ein binationales Ehepaar aus dem Zuständigkeitsbereich eben dieser Behörde beschwert und schildert einen Sachverhalt der Datenerhebung, der nicht im Einklang mit Datenschutzgrundsätzen steht. Die Überprüfung dieses Falles dauert noch an.

6. Kommunalwesen

Wie vorauszusehen war (vgl. 12. Tätigkeitsbericht, Seite 23), sind durch die - neue - **Gemeindeordnung** in der Praxis nur wenige Datenschutzprobleme gelöst, vielmehr zusätzliche geschaffen worden. Dies betrifft beispielsweise die Frage nach dem Inhalt und Umfang der Datenerhebung im Rahmen der **Ehrenordnungen** der Räte (§ 43 Abs. 3 der Gemeindeordnung für das Land Nordrhein-Westfalen - GO NW).

So wurden im Rahmen einer Ehrenordnung unter anderem Fragen danach gestellt, ob ein Ratsmitglied Hausfrau/-mann sei, und welche regelmäßige Arbeitszeit (auch bei Hausarbeit) bestehe. Bei diesen Fragen ist kein Einfluß auf die Tätigkeit als Ratsmitglied denkbar. Die Tatsache, daß diese Angaben möglicherweise für die Berechnung eines Verdienstausfalles behilflich sein können, ist keine Rechtfertigung dafür, diese Daten im Rahmen der Ehrenordnung abzufragen. In den Fällen, in denen erkennbar ist, daß eine Angabe trotz Nennung im **Datenerhebungsformular** für die Ausübung des jeweiligen Mandats nicht von Bedeutung sein kann, braucht diese Angabe auch nicht gemacht zu werden. Mindestens verwirrend ist es, wenn die Formulare in ihrem Belehrungstext absolute **Vertraulichkeit** hinsichtlich **aller** im Formular genannten Daten zusichern. § 43 Abs. 3 Satz 4 GO NW sieht nämlich ausdrücklich die Veröffentlichung von Name, Anschrift, des ausgeübten Berufes sowie anderer vergüteter und ehrenamtlicher Tätigkeiten vor. Auch der Hinweis, daß alle **Änderungen** in den persönlichen oder wirtschaftlichen Verhältnissen unverzüglich dem Bürgermeister mitzuteilen seien, ist zu pauschal, da nur Daten verlangt werden dürfen, soweit sie für die Ausübung des Ratsmandates von Bedeutung sein können.

Es kommt vor, daß sich Ratsmitglieder über ihre Pflicht zur **Verschwiegenheit** (§ 30 Abs. 2 GO NW) hinwegsetzen und personenbezogene Daten von Bürgerinnen und Bürgern aus der Ratsarbeit im Einzelfall an die Presse weitergeben. In den bekanntgewordenen Fällen der Offenbarung von personenbezogenen Daten ist von den Sanktionsmöglichkeiten nach § 30 Abs. 6 GO NW für derartige Datenschutzverstöße bemerkenswerterweise kein Gebrauch gemacht worden.

6.1 Einwohneranträge und Bürgerbegehren

Unterschriftenlisten zur Unterstützung eines Bürgerbegehrens dürfen keiner zweckändernden Nutzung zugeführt werden.

Einige Probleme datenschutzrechtlicher Art sind bei der Durchführung der - in den Gemeinden noch neuen - Mitwirkungsmöglichkeiten aufgetreten. So sieht beispielsweise § 25 Abs. 4 Satz 2 GO NW zur zweifelsfreien Identifizierung der Personen, die Einwohneranträge unterzeichnen, vor, daß neben Namen, Vornamen und Anschrift auch das **Geburtsdatum** zu benennen ist, obgleich dies nur in seltenen Fällen erforderlich sein dürfte. Um die Berechtigung zur Unterzeichnung des Einwohnerantrags nachzuweisen, genügt zudem in aller Regel die Angabe des Alters. Auf meine Anregung hin hat das Innenministerium erklärt, es werde bei einer Änderung der Gemeindeordnung vorsehen, daß die Altersangabe ausreicht.

Unterstützungsunterschriftenlisten sind in anderen Gemeinden ohne Einwilligung der Betroffenen herangezogen worden, um Personen auszuwählen, die in die **Abstimmungsvorstände** für den Bürgerentscheid berufen werden sollten. Die Nutzung der in den Unterstützungsunterschriftenlisten enthaltenen personenbezogenen Daten für die Besetzung der Abstimmungsvorstände bedeutet eine **Zweckänderung** dieser Daten. Eine Erlaubnisnorm für diese Zweckänderung liegt nicht vor. Von einer mutmaßlichen Einwilligung kann nicht ausgegangen werden, da der Erklärungsinhalt der Unterschrift ein Einverständnis mit der Bestellung zum Abstimmungsvorstand nicht umfaßt. Auch dadurch, daß die Liste in aller Regel in der Öffentlichkeit unterzeichnet wird, wird sie nicht zu einer allgemein zugänglichen Quelle im Sinne von § 13 Abs. 2 Buchstabe f DSG NW. Eine zweckändernde Nutzung der in der Liste enthaltenen personenbezogenen Daten ist daher nicht möglich. Da eine Wiederholung des Vorfalls in einer der beiden Gemeinden für die Zukunft zu befürchten war, wurde die zweckändernde Nutzung der Daten aus der Unterschriftenliste beanstandet. Da die andere Gemeinde erklärte, diese Praxis nicht fortsetzen zu wollen, konnte auf eine Beanstandung in diesem Fall verzichtet werden.

6.2 Auflistung von Bauvorhaben an den Rat

Die Übermittlung einer monatlichen Auflistung aller Bauvorhaben in einer Gemeinde an den Vorsitzenden des Bauausschusses der Gemeinde sowie an die Ortsvorsteher in den Ortsteilen ist nur mit Einwilligung der Betroffenen oder in anonymisierter Form zulässig.

Die Bauverwaltung einer Gemeinde hatte Zweifel, ob es datenschutzrechtlich zulässig sei, dem Rat und den Ortsvorstehern monatlich Listen über Bauvorhaben mit den Angaben Bauherr mit Adresse, Bauregisternummer, Bauort, Bauvorhaben, Antragseingangsdatum, Entscheidungsdatum, Antragsart sowie jeweiliger Verfahrensstand zu übermitteln.

Wegen Fehlens einer bereichspezifischen Rechtsgrundlage für die gewünschte Datenverarbeitung sowie wegen Fehlens einer entsprechenden wirksamen Einwilligung bleibt nur die Möglichkeit, die Datensätze in der Auflistung zuverlässig zu **anonymisieren**. In der überwiegenden Zahl der Fälle könnte hierzu bereits die Schwärzung des Namens und der Adresse sowie die Schwärzung von Bauregisternummer, Antragseingangsdatum und Entscheidungsdatum ausreichen. Gegen die Weitergabe einer so anonymisierten Auflistung bestehen keine datenschutzrechtlichen Bedenken. Derartige Listen könnten sogar in öffentlicher Sitzung behandelt werden.

6.3 Verhältnis Beschwerdeausschuß zu Fachausschüssen

Der Beschwerdeausschuß besitzt zwar eine Allzuständigkeit für die Beschwerden der Bürgerinnen und Bürger einer Gemeinde, jedoch kann er nicht beliebig Datenverarbeitung betreiben, die in den Zuständigkeitsbereich anderer Fachausschüsse gehört.

Ein Bürger hatte sich an den Beschwerdeausschuß einer Gemeinde mit dem Hinweis gewandt, ein Dritter beziehe zu Unrecht Sozialhilfe. Das Sozialamt der Gemeinde hatte sich aus Datenschutzgründen zu Recht geweigert, dem Beschwerdeausschuß den zugrunde liegenden Verwaltungsvorgang vorzulegen, da die Zuständigkeit des Beschwerdeausschusses sich nicht auf die Nachprüfung der Belange Dritter erstreckt. Soweit - wie hier - ein Petent oder eine Petentin, ohne selbst betroffen zu sein, den Beschwerdeausschuß lediglich über Dritte betreffende Sachverhalte informiert, ist keine gesetzliche Befugnis zur Übermittlung von Sozialdaten durch das Sozialamt ersichtlich, es sei denn, der Beschwerdeausschuß könnte als Kontrollinstanz im Sinne des Sozialgesetzbuches angesehen werden, wofür allerdings keine Anhaltspunkte erkennbar sind; allenfalls käme hier der Sozialausschuß in Betracht. Wie zudem der Hauptsatzung der Gemeinde zu entnehmen war, wurden die Zuständigkeiten der Ausschüsse durch das Petitionsrecht der Bürgerinnen und Bürger der Gemeinde nicht berührt.

Soweit in den Gemeinden noch nicht geschehen, ist das Verhältnis von Beschwerdeausschuß zu den Fachausschüssen des Rates in den jeweiligen Hauptsatzungen der Gemeinden entsprechend klar zu regeln.

7. Verfassungsschutz

Gegen Ende des Berichtszeitraums gab es Anlaß, Fragen zum Verhältnis des neuen Sicherheitsüberprüfungsgesetzes (SÜG NW - GV. NW. 1995, S. 201) zum neuen Verfassungsschutzgesetz (VSG NW - GV. NW. 1995, S. 28) nachzugehen, deren Klärung noch nicht abgeschlossen ist. So etwa, ob die Verweigerung der Einwilligung des Ehepartners zur Einbeziehung in die Sicherheitsüberprüfung nach § 7 Abs. 4 SÜG NW als Anlaß genommen werden darf, nunmehr originär als Verfassungsschutzbehörde im Rahmen der Aufgabenstellung nach § 3 VSG NW tätig zu werden. Ein entsprechendes Problem dürfte sich auch aus der Regelung in § 6 Abs. 1 Satz 2 VSG NW ("Hinweis auf die **Mitwirkungspflicht**") bei einer Sicherheitsüberprüfung ergeben, obwohl in § 7 Abs. 2 SÜG NW auf die Einwilligung, also die **Freiwilligkeit**, der betroffenen Person abgestellt wird. Zudem gewährt § 24 Abs. 5 SÜG NW den betroffenen Personen unter bestimmten Voraussetzungen Akteneinsicht zu den im Rahmen der Sicherheitsüberprüfung über sie gespeicherten Daten, wohingegen § 14 Abs. 1 Satz 2 VSG NW ein solches Akteneinsichtsrecht gerade ausschließt.

Aus der Prüfpraxis im Berichtszeitraum ist ansonsten lediglich folgendes erwähnenswert: Im Rahmen der Vorbereitungen für die **Europawahlen** 1994 verschaffte sich der Verfassungsschutz Kopien von einer Reihe von Unterschriftenlisten, mit denen die Teilnahmemöglichkeit einer bestimmten politischen Partei an den Wahlen befürwortet wurde. Die Erhebung und weitere Verarbeitung der in den **Wahlunterstützungslisten** enthaltenen personenbezogenen Daten durch den Verfassungsschutz war nicht zulässig. Das Wahlgeheimnis hat einen solch hohen Stellenwert, daß in die Verfassungsgarantie seiner Unverletzlichkeit nur unter engen Voraussetzungen auf Grund einer ausdrücklichen Regelung in den Wahlgesetzen eingegriffen werden dürfte. Da inzwischen auch der Verfassungsschutz die Verarbeitung von Daten aus Wahlunterstützunglisten als unzulässig ansieht, hat er die Verarbeitung der Daten aus diesen Unterlagen rückgängig gemacht und angekündigt, auch die Unterlagen selbst zu vernichten. Ich gehe davon aus, daß die Beschaffung derartiger Unterlagen künftig unterbleibt. Im übrigen ist der Verfassungsschutz erfreulicherweise mehr als früher bereit, den Umfang seiner Auskunft gegenüber den einzelnen anfragenden Bürgerinnen und Bürgern zu erweitern. Diese Entwicklung kann und sollte verstärkt fortgesetzt werden.

8. Polizei

Am 26.07.1995 haben die Mitgliedstaaten der Europäischen Union das Übereinkommen über die Errichtung eines **europäischen** Polizeiamtes unterzeichnet. Dieses Übereinkommen befindet sich derzeit im Ratifizierungsverfahren, ein Vorentwurf des Zustimmungsgesetzes (EUROPOL-Gesetz) liegt vor. Wesentlicher datenschutzrechtlicher Inhalt dieses Entwurfs ist die Errichtung eines europäischen, automatisiert geführten Informationssystems, in das Mitgliedstaaten und EUROPOL Daten eingeben und aus dem Daten unmittelbar abgerufen werden können. Vorgesehen ist auch die Einrichtung von sogenannten Analysedateien, unter anderem für künftige Strafverfolgung. Gewährleistet werden soll ein einheitlicher Datenschutzstandard in den Mitgliedstaaten, soweit die Datenverarbeitung für EUROPOL erfolgt. Eine Gemeinsame Kontrollinstanz soll eingerichtet werden.

Die mit EUROPOL geschaffene zentrale Polizeieinrichtung, die bereits im 11. Tätigkeitsbericht (S. 16) vorgestellt wurde, und die Ratifizierung des Übereinkommens, zu dem bereits im 12. Tätigkeitsbericht (S. 31 f.) berichtet worden ist, wirft nach wie vor eine Reihe datenschutzrechtlicher Fragen auf. So können von dem europaweit zugänglichen Dateninformationssystem nicht nur Tatverdächtige, sondern gleichfalls Personen gespeichert werden, von denen **angenommen** wird, daß sie eine Straftat begehen werden. In den Analysedateien sollen sogar auch **bewertende Informationen** erfaßt werden dürfen über Personen, die noch nicht einmal selbst einer begangenen oder zu begehenden Straftat verdächtig sind, nämlich Zeugen, Opfer, potentielle Opfer, Kontakt- und Begleitpersonen sowie Personen, die Informationen liefern können.

Angesichts des nicht nur europaweiten, sondern wegen der zusätzlichen Übermittlungsmöglichkeit an Drittstaaten **internationalen Zugriffs** auf die Daten stehen die Betroffenen - immerhin nach unserem Rechtssystem als unschuldig geltende Personen - in der Gefahr, den Überblick zu verlieren und nicht mehr wissen zu können, wer was wann und bei welcher Gelegenheit über sie weiß. Die **Löschung** der Daten bleibt selbst nach Freispruch oder Verfahrenseinstellung **ungewiß**; nicht einmal der mitteilende Mitgliedstaat behält die Herrschaft über die Daten. Die individuelle Durchsetzung von Datenschutzrechten wird damit erschwert und zum Teil sogar unmöglich gemacht, eine wirksame Datenschutzkontrolle in Frage gestellt.

Der Entwurf des EUROPOL-Gesetzes läßt an mehreren Stellen, auch durch die wiederholte Bezugnahme auf den Entwurf eines BKA-Gesetzes (BT-Drs. 13/1550) die klare Tendenz erkennen, polizeirechtliche Kompetenzen zu La-

sten der bisher zuständigen Länder auf den Bund zu verlagern. Dies stellt in erster Linie ein verfassungsrechtliches Problem dar, jedoch ergeben sich auch datenschutzrechtliche Auswirkungen.

Zwar wird im Entwurf des EUROPOL-Gesetzes vorgesehen, daß die innerstaatlich eingebende oder übermittelnde Stelle (Landespolizeibehörde) die datenschutzrechtliche Verantwortung für die Daten trägt, die in das Informations- oder Analysesystem bei EUROPOL eingegeben werden sollen. Es ist jedoch fraglich, welche datenschutzrechtliche Verantwortung das BKA als Zentralstelle daneben für Länderdaten haben soll. Da im Bereich der internationalen Zusammenarbeit auch dem BKA die datenschutzrechtliche Verantwortung als Zentralstelle übertragen werden soll, läßt sich daraus der Schluß ziehen, daß dann auch Gefahrenabwehrdaten, die bisher in ausschließlicher Zuständigkeit der Länder erhoben, verarbeitet und genutzt werden können, in das "Eigentum" des Bundes wechseln und die Länder allenfalls "Mitbesitzer" wären.

Mit der im Berichtszeitraum begonnenen **Novellierung** des **Polizeigesetzes** soll neben der Anpassung bestimmter Vorschriften an aktuelle Änderungen in Spezialgesetzen auch eine Rechtsgrundlage für die Aufzeichnungsmöglichkeit des Fernmeldeverkehrs zum **Notruf 110** und für die weitere Verarbeitung der dabei gewonnenen Daten geschaffen werden. Da das Gesetzgebungsvorhaben noch nicht abgeschlossen ist, bleibt abzuwarten, inwieweit meine Anregungen berücksichtigt werden.

Seit Jahren muß die **Überarbeitung** der Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen (**KpS-Richtlinien**) vom **10. Februar 1981** (MBl. NW. S. 192) angemahnt werden. Gestützt auf diese Richtlinien werden bei der Polizei suchfähige Unterlagen über Beschuldigte, Verdächtige, gefangene Personen, bei denen erkennungsdienstliche Maßnahmen vorgenommen worden sind, zur Festnahme oder Inverwahrungnahme gesuchte Personen, vermißte Personen oder nicht identifizierte hilflose Personen, gefährdete Personen, Anzeigeerstatter und Hinweisgeber, Zeugen und Geschädigte, sowie noch andere Personen gespeichert. Die so gesammelten Daten stellen die zentrale Informationssammlung der Polizei dar. Um so wichtiger ist, daß die einer solchen Sammlung zugrundeliegenden Verwaltungsvorschriften im Licht des Rechts auf informationelle Selbstbestimmung der betroffenen Personen überarbeitet werden.

Telefonüberwachungsprotokolle gehören nicht in **Disziplinarakten**. Nach § 100 b Abs. 5 StPO dürfen die durch Maßnahmen zur Überwachung und Aufzeichnung des Fernmeldeverkehrs erlangten personenbezogenen Informa-

tionen in anderen Strafverfahren zu Beweiszwecken nur verwendet werden, soweit sich bei Gelegenheit der Auswertung Erkenntnisse ergeben, die zur Aufklärung der in § 100 a StPO bezeichneten Straftaten benötigt werden. Nach § 100 b Abs. 6 StPO sind die durch die Maßnahmen erlangten Unterlagen, wenn sie zur Strafverfolgung nicht erforderlich sind, unverzüglich unter Aufsicht der Staatsanwaltschaft zu vernichten. Damit ist ein Abheften von Telefonüberwachungsprotokollen, die zudem in großer Zahl Daten dritter Personen enthalten, in Disziplinarakten nicht möglich.

Nicht nur im Bereich der Polizei, sondern in allen Verwaltungsbereichen gibt es Fälle, in denen versucht wird, den Datenschutz zu **instrumentalisieren** oder vorzuschieben, obgleich keinerlei Datenschutzbelange berührt sind, sondern lediglich der Wille zur Verwaltungstransparenz fehlt. Erwähnt sei nur eines der Beispiele, das zwar ausgerechnet die Polizei betrifft, dem aber auch eine gewisse Pikanterie eigen ist: Die Auskunft nach den Kosten einer **Polizeieskorte** für eine **private Hochzeit** wurde einem Bürger zunächst "aus datenschutzrechtlichen Gründen" verweigert.

8.1 Prostituiertendatei

Vorratsdatensammlungen über Prostituierte sind unzulässig.

Einer Dateianmeldung konnte entnommen werden, daß die Polizeiinspektion eines Polizeipräsidiums eine Datei über Prostituierte führte mit der Zweckbestimmung "Verhütung von Straftaten; hier: illegale Prostitution".

Bei der Überprüfung stellte sich heraus, daß die Datei das Ergebnis eines Schwerpunkteinsatzes gegen die Straßenprostitution im Bereich des Sperrbezirks war. Mit Hilfe dieser Datei sollten Daten erfaßt werden, um den Tatvorwurf einer "beharrlichen" Zuwiderhandlung gegen das durch Rechtsverordnung erlassene Verbot belegen zu können, der Prostitution an bestimmten Orten überhaupt oder zu bestimmten Tageszeiten nachzugehen. Zum Zeitpunkt des Kontrollbesuchs war die Datei automatisiert nicht mehr vorhanden. Es existierten nur noch zwei Ausdrucke in Listenform, die inhaltlich veraltet waren.

Aus Gründen der Verhältnismäßigkeit bestehen bereits erhebliche Zweifel daran, ob die Datenerhebung und Speicherung für die Dauer des Einsatzes berechtigterweise geschah. Jedenfalls war nicht ersichtlich, daß die veralteten Listen noch für irgendeine Aufgabenerfüllung hätten erforderlich sein können. Zudem stellte das Bereithalten personenbezogener Daten in diesem Fall eine unzulässige Vorratsdatenhaltung dar.

Es wurde empfohlen, die Daten zu löschen und alle vorhandenen Ausdrucke ersatzlos zu vernichten.

8.2 Datenübermittlung an private Detektei

Die Nutzung von Polizeidaten für den Geschäftsbetrieb einer privaten Detektei ist in der Regel unzulässig.

Unter Angabe einer Fahrgestellnummer erkundigte sich eine private Detektei regelmäßig bei einem Polizeipräsidium nach weiteren Daten angeblich gestohlener, im Ausland sichergestellter Kraftfahrzeuge. Handelte es sich tatsächlich um ein als gestohlen gemeldetes Fahrzeug, wurden bereitwillig das Kennzeichen sowie der Tag der Entwendung mitgeteilt.

Hilfsbereitschaft dieser Art ist nach § 29 Abs. 2 PolG NW nicht zulässig. Ein **eigenes** rechtliches Interesse der Detekteien an der Datenübermittlung ist nicht anzunehmen. Ohne eine einzelfallbezogene Vollmacht des Kfz-Halters oder seiner Kfz-Versicherung kann auch nicht von einem **abgeleiteten** rechtlichen Interesse ausgegangen werden. Einer **regelmäßigen** Datenübermittlung der genannten Daten steht auch § 9 DSG NW entgegen. Nach § 9 Abs. 8 in Verbindung mit Abs. 5 DSG NW ist die regelmäßige Übermittlung von Daten für Stellen außerhalb des öffentlichen Bereichs nicht zulässig.

Das Innenministerium sollte gegenüber den Kreispolizeibehörden klarstellen, daß derartigen Auskunftsersuchen privater Detekteien nicht nachgekommen werden darf.

8.3 Weitergabe von Daten an Kaufhäuser

Verläuft die von einem Kaufhaus veranlaßte Taschenüberprüfung einer Kundin durch die Polizei negativ, so besteht im Regelfall kein Anspruch des Kaufhauses auf Übermittlung der Personalien der Kundin.

Die Allgemeinen Geschäftsbedingungen eines Kaufhauses enthielten die Aufforderung an die Kundschaft, mitgeführte Taschen entweder an der Information abzugeben oder außerhalb des Warenhauses zu deponieren. Kundinnen und Kunden, die trotz des Mitnahmeverbotes Taschen mit in den Verkaufsraum nehmen wollten, hätten diese dem Personal des Warenhauses zum Zwecke einer Kontrolle vorzuzeigen. Hierin sah das Kaufhaus eine verbindliche Hausordnung, die mit dem Betreten der Verkaufsräume akzeptiert werde.

Eine Kundin nahm ihre Tasche mit in das Kaufhaus und verweigerte anschließend eine Taschenkontrolle durch den Hausdetektiv. Die herbeigerufene Polizei überprüfte die Tasche mit negativem Ergebnis. Im Hinblick auf den vom Kaufhaus behaupteten Verstoß gegen die Hausordnung **übermittelten** die Polizeibeamten die Personalien der Kundin an das Kaufhaus, das diese Daten nutzte, um ein Hausverbot auszusprechen.

Die Hausordnung des Kaufhauses entsprach nicht der geltenden Rechtslage (vgl. BGH, Urteil vom 3. Juli 1996, NJW 1996,2574 ff.). Danach benachteiligt eine solche Klausel in den Allgemeinen Geschäftsbedingungen den Kunden unangemessen, weil sie von wesentlichen Grundgedanken der gesetzlichen Regelung abweicht, nach der Taschenkontrollen nur bei konkretem Diebstahlsverdacht zulässig sind. Deshalb verstößt die generelle Durchführung von Taschenkontrollen gegen die Bestimmungen des Gesetzes zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen.

Da die Hausordnung in diesem Punkt rechtswidrig war, lag in dem Verhalten der Kundin auch kein Verstoß gegen die Hausordnung des Kaufhauses. Somit war weder ein rechtliches noch ein berechtigtes Interesses des Kaufhauses vorhanden, das einen Anspruch gegenüber der Polizei auf Bekanntgabe der Personalien der Kundin hätte begründen können (vgl. § 29 Abs. 2 PolG NW). Nach der mit negativem Ergebnis geführten Überprüfung der Tasche war vielmehr das Geheimhaltungsinteresse der betroffenen Kundin zu beachten, aus diesem Anlaß heraus nicht auch noch mit einem rechtswidrigen Hausverbot belegt zu werden.

9. Rechtspflege

Im Bereich der Rechtspflege besteht auch weiterhin noch Nachholbedarf für Gesetze, die als Rechtsgrundlagen für bisher nur durch Verwaltungsvorschriften geregelte Datenverarbeitungen im Justizbereich dienen sollen. So hat die Bundesregierung am 22. Mai 1996 den Entwurf eines Gesetzes über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen (**Justizmitteilungsgesetz** - JuMiG) im Bundestag eingebracht (vgl. auch 12. Tätigkeitsbericht, Seite 12). Der Gesetzentwurf beruht auf einem Entwurf aus dem Jahre 1992, der durch Ablauf der Wahlperiode des Bundestages der Diskontinuität verfiel. Sowohl der neue Entwurf als auch die hierzu ergangene Stellungnahme des Bundesrates sind wenig datenschutzfreundlich. Der neue Entwurf wird derzeit im Bundestag beraten.

Als aus der Sicht des Datenschutzes besonders bedauerlich sollen lediglich zwei Punkte herausgestellt werden. **Eine Benachrichtigungspflicht** derjenigen Person, über die eine Mitteilung weitergegeben wird, ist nur noch in wenigen Ausnahmefällen vorgesehen, ansonsten erfolgt eine Auskunft an die Betroffenen nur auf Antrag. Auch die **Anordnungsbefugnis** für derartige Mitteilungen soll nicht mehr besonders qualifizierten Justizbediensteten, wie etwa richterlich oder staatsanwaltschaftlich Tätigen und Angehörigen des gehobenen Justizdienstes, vorbehalten bleiben. Eine ausreichende Berücksichtigung der schutzwürdigen Belange der Betroffenen im Rahmen der Entscheidung über eine Mitteilung scheint damit nicht mehr gewährleistet.

Durch das Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (**Geldwäschegesetz** - GWG) vom 25. Oktober 1993 (BGBl. I S. 1770) sind Kredit- und Finanzinstitute sowie Spielbanken verpflichtet, unter bestimmten Voraussetzungen Finanztransaktionen den zuständigen Strafverfolgungsbehörden anzuzeigen (§ 11 GWG). Im Berichtszeitraum konnte in diesem Zusammenhang wenigstens erreicht werden, daß das Justizministerium festgelegt hat, daß die bei den Staatsanwaltschaften eingehenden Geldwäscheanzeigen vor ihrer Registrierung dem zuständigen Dezernenten vorzulegen sind, um zu entscheiden, ob die Sache unter Berücksichtigung der Umstände des Einzelfalles als Js-Vorgang, das heißt als Strafsache, oder als AR-Vorgang einzutragen ist, das heißt als Angelegenheit, die lediglich im Allgemeinen Register der Staatsanwaltschaft festgehalten wird. Dies ist insgesamt als ein datenschutzrechtlicher Fortschritt zu bewerten (vgl. 12. Tätigkeitsbericht, S. 52/53).

Wenige Beispiele offenbarten das Datenschutzverständnis einiger **Notare**. Wenn es sich um die Erteilung von Kopien notarieller **Grundstückskaufverträge an Dritte** handelt, ist allenfalls die Übermittlung einer Teilkopie, etwa

beschränkt auf den Teil des Vertrages zu einem Wegerecht, zulässig. Ebenso ist das **Kopieren** der **Personalausweise** der Beteiligten und die Aufnahme der Kopien in den Beurkundungsvorgang nicht zulässig. Weiter stellt sich die Frage, inwieweit es zur Aufgabenerfüllung der Notare erforderlich ist, in die Urkunden bei den **Angaben zu den Beteiligten** Geburtsdatum und -ort sowie den Beruf aufzunehmen. Eine Überarbeitung der **Dienstordnung** der **Notare** unter Datenschutzgesichtspunkten ist im übrigen seit Jahren überfällig.

Auch wenn auf die Ausübung des **Gnadenrechts**, etwa durch den Ministerpräsidenten des Landes Nordrhein-Westfalen, das Datenschutzgesetz des Landes Nordrhein-Westfalen keine Anwendung findet (§ 2 Abs. 1 Satz 3 DSG NW), so bedeutet das gleichwohl nicht, daß die betroffenen Bürgerinnen und Bürger in einem Gnadenverfahren in datenschutzrechtlicher Hinsicht rechtlos gestellt wären. Wie in anderen Bundesländern sollte es allerdings auch in Nordrhein-Westfalen datenschutzkonforme Regelungen zur Datenverarbeitung in Gnadenverfahren geben, die ein ausgewogenes Verhältnis zwischen den Interessen des Gnadenträgers und den mit Gnadensachen befaßten Stellen sowie den Datenschutzbelangen der betroffenen Bürgerinnen und Bürger darstellen.

9.1 Auflagen bei Einstellungen nach § 153 a StPO

Nach § 153 a Abs. 1 StPO kann die Staatsanwaltschaft mit Zustimmung des Gerichts und der beschuldigten Person vorläufig von der Erhebung der öffentlichen Klage absehen und zugleich der beschuldigten Person unter anderem die Zahlung eines Geldbetrages zugunsten einer **gemeinnützigen Einrichtung** oder der Staatskasse auferlegen. Ist die Klage bereits erhoben, so kann das Gericht mit Zustimmung der Beteiligten das Verfahren vorläufig einstellen und zugleich der angeschuldigten Person Auflagen und Weisungen erteilen (§ 153 a Abs. 2 StPO).

Gegen das im Lande Nordrhein-Westfalen angewandte Verfahren, mit dem die gemeinnützigen Einrichtungen über die zu erwartenden Zahlungen von Geldbeträgen unterrichtet werden, bestehen seit langem datenschutzrechtliche Bedenken (vgl. etwa 6. Tätigkeitsbericht, Seite 42 bis 44). Am wenigsten würden die Belange der Betroffenen beeinträchtigt werden, wenn die Geldbeträge an die Gerichtskasse gezahlt werden könnten und die Staatsanwaltschaft oder das Gericht die Geldbeträge den jeweiligen gemeinnützigen Einrichtungen zuteilen würde. Ein solches Verfahren hat das Justizministerium jedoch bisher stets abgelehnt. Im Berichtszeitraum wurden in diesem Zusammenhang weitere datenschutzrechtliche Probleme deutlich.

So informierte ein Amtsgericht die gemeinnützige Einrichtung durch **Übersendung** einer Ausfertigung **des Beschlusses** über die vorläufige Einstellung. Dieser Beschluß enthielt naturgemäß mehr Daten, als zur Aufgabenerfüllung der gemeinnützigen Einrichtung erforderlich waren. Weiter war der Beschluß selbst so abgefaßt, daß der Betroffene nicht davon unterrichtet wurde, daß die gemeinnützige Einrichtung vom Gericht direkt über das Verfahren, sowie Inhalt und Umfang der Auflage informiert werden würde.

Bemerkenswert war dabei auch die Auffassung des Amtsgerichts, daß die Datenübermittlung an die gemeinnützige Einrichtung mit **Einwilligung** des Betroffenen erfolge. Die Zustimmung des Betroffenen zur Einstellung des Verfahrens nach § 153 a StPO sei gleichzeitig auch als datenschutzrechtlich relevante Einwilligung in die Übermittlung der Daten an die gemeinnützige Einrichtung anzusehen. Dabei wird allerdings übersehen, daß nach § 4 Abs. 2 BDSG eine wirksame Einwilligung eine entsprechende Unterrichtung und Belehrung in datenschutzrechtlicher Hinsicht voraussetzt, die hier jedoch nicht stattgefunden hatte.

Zur Lösung dieser - nicht allein Nordrhein-Westfalen betreffenden - Datenschutzprobleme hat das **Bundesministerium** der **Justiz** zu erkennen gegeben, daß es bereit wäre, im Interesse des Datenschutzes eine bundesgesetzliche Regelung zu erlassen, in der etwa die Zahlung an eine Gerichtskasse zur anonymisierten Weiterleitung an die gemeinnützige Einrichtung oder die Überweisung des Geldbetrages durch Verwendung eines Codewortes erlaubt werden könnte. An einer solchen Regelungsinitiative sieht es sich durch die ablehnende Haltung einiger Bundesländer, darunter auch der Haltung des Justizministeriums des Landes Nordrhein-Westfalen, gehindert. Diese **Verweigerungshaltung** des **Justizministeriums** ist zu bedauern.

Landesregierung und Landtag bleiben aufgerufen, das Justizministerium davon zu überzeugen, daß eine derartige Verweigerungshaltung nicht im Datenschutzinteresse der Bürgerinnen und Bürger des Landes Nordrhein-Westfalen liegen kann.

9.2 Speicherung von Daten Unschuldiger bei der Staatsanwaltschaft

Eine Bürgerin oder ein Bürger haben Anspruch auf Löschung ihrer Daten bei der Staatsanwaltschaft, wenn sich nach Abschluß des Ermittlungsverfahrens ihre Unschuld erwiesen hat. Derartige Daten sind gegebenenfalls zunächst zu sperren und dann unverzüglich zu **löschen** (vgl. 12. Tätigkeitsbericht, S. 49/50). Für das länderübergreifende staatsanwaltschaftliche Verfahrensregister

ist diese Frage nunmehr bereichspezifisch in § 476 Abs. 2 und 3 StPO geregelt, wonach Daten, in dem Fall, daß eine beschuldigte Person rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt wird, zwei Jahre nach der Erledigung des Verfahrens zu löschen sind, es sei denn, vor Eintritt der Löschungsfrist wird ein weiteres Verfahren zur Eintragung in das Verfahrensregister mitgeteilt. Gegenüber der bisher bei den Staatsanwaltschaften verbreiteten Praxis der langfristigen Speicherung einmal erhobener personenbezogener Daten ist diese Vorschrift ein Fortschritt. Es bleibt insoweit zu wünschen, daß eine entsprechende bereichspezifische Regelung auch für die übrige Verarbeitung personenbezogener Daten bei den Staatsanwaltschaften gefunden wird.

10. Strafvollzug

Das Strafvollzugsgesetz bedarf seit längerer Zeit der Überarbeitung. Anläufe zu seiner Änderung sind bisher jedoch gescheitert. In dem Vorläufigen Referentenentwurf eines Vierten Gesetzes zur Änderung des **Strafvollzugsgesetzes** (Stand: 10.04.1996) sind folgende datenschutzbezogene Themen unter anderem enthalten: Überwachung der Besuche, Überwachung des Schriftverkehrs, Vernichtung der erkennungsdienstlichen Unterlagen, Datenerhebung über Nicht-Gefangene, Unterrichtung über Datenerhebung, Datenübermittlung an dritte Stellen, Überwachung des Postverkehrs, Bekanntgabe von Daten innerhalb der Anstalt, Weitergabe von Untersuchungsergebnissen, Aufbewahrungsfristen und Datenschutzkontrolle. Dabei ist leider festzustellen, daß es in vielen Vorschriften des Entwurfs nicht gelungen ist, den Datenschutz für die Gefangenen zu verbessern.

Im täglichen Ablauf des Strafvollzuges gibt es zudem eine Reihe von Datenschutzproblemen, die immer wieder auftreten. Als Stichwörter sind insoweit zu nennen, Fahndungsfotos auf Vorrat, die Briefzensur, Verwendung von Paketmarken, Einkaufsscheine, Identifizierung von HIV-Kranken.

Obwohl in Nr. 23 Abs. 2 der Vollzugsgeschäftsordnung (VGO) verbindlich geregelt ist, daß von Strafgefangenen mit einer Vollzugsdauer von einem Jahr und mehr sowie von Sicherungsverwahrten **Lichtbilder** (Brustbilder, in Zivilkleidung) aufzunehmen und zu den Personalakten zu nehmen sind, besteht im Lande Nordrhein-Westfalen die Praxis, daß von **allen** Gefangenen derartige Lichtbilder angefertigt und aufbewahrt werden, da das Justizministerium durch Rundverfügung vom 16.09.1985 die eingeschränkte Regelung der Nr. 23 Abs. 2 VGO für das Land Nordrhein-Westfalen für nicht anwendbar erklärt hat. Verletzungen der Bestimmungen über die **Briefzensur** kamen im Berichtszeitraum mehrmals vor. Sowohl Verteidigerpost als auch die Post der Landesbeauftragten für den Datenschutz wurde geöffnet. Als Ergebnis der Überprüfung des jeweiligen Falles ergab sich stets menschliches Versagen. Nachdenklich stimmt es, wenn sich derselbe Fehler gegenüber einzelnen Gefangenen mehrfach ereignet und nach Aussage der Gefangenen stets dieselben Bediensteten dafür verantwortlich sein sollen.

Strafgefangene dürfen jeweils zu Weihnachten, zu Ostern und zu einem von ihnen zu wählenden weiteren Zeitpunkt, beispielsweise ihrem Geburtstag, ein Paket empfangen. Solche Pakete dürfen nur Nahrungs- und Genußmittel enthalten. Voraussetzung für den Empfang ist die Verwendung von **Paketmarken** und zwar für Weihnachtspakete gelbe Paketmarken, für Osterpakete grüne Paketmarken und für Wahlpakete weiße Paketmarken (Rundverfügung

des Justizministeriums vom 13.10.1988 - 4510-IV A.40). Nach Nr. 1.1.9 der Rundverfügung ist bei Paketen mit anderem Inhalt als Nahrungs- und Genußmitteln von der Verwendung einer Paketmarke abzusehen. Aus Nr. 1.1.12 der Rundverfügung ergibt sich, daß die Durchsuchung des Paketinhalts in Gegenwart des Gefangenen erfolgt. Werden also die Pakete ohnehin durchsucht, ist kein rechter Sinn für die Verwendung von Paketmarken ersichtlich. Da die Paketmarke jeder Person, die mit dem Paket zu tun hat, den Gefangenenstatus offenbart, sollte dieser nicht mehr zur Aufgabenerfüllung der Justizvollzugsanstalt erforderliche Eingriff in das Recht auf informationelle Selbstbestimmung der Gefangenen künftig unterbleiben. Auch werden immer wieder Fälle bekannt, in denen der Datenschutz beim Einkauf der Gefangenen beim Vertragskaufmann in den Anstalten aufgrund der Gestaltung und Nutzung der **Einkaufsscheine** defizitär ist. Auf Beschwerden von Bediensteten einer Justizvollzugsanstalt hin, daß ihnen gegenüber nicht die **HIV-Infizierung** der **Gefangenen** offengelegt werde, hat das Justizministerium es erfreulicherweise abgelehnt, eine solche Information aller Bediensteten als zur Aufgabenerfüllung erforderlich anzusehen.

11. Sozialbereich

Wer Sozialleistungen erhalten will, ist regelmäßig verpflichtet mitzuwirken, sonst kann die Leistung versagt werden. Dabei werden von den Sozialleistungsträgern zwangsläufig umfangreiche Daten über die persönlichen und wirtschaftlichen Verhältnisse der Bürgerinnen und Bürger gesammelt. Diese Daten unterliegen den strengen Bestimmungen des Sozialdatenschutzes. In den letzten Jahren wurden jedoch immer mehr Vorschriften erlassen, die das **Sozialgeheimnis aus § 35 SGB I praktisch durchlöchern**, so beispielsweise die automatisierten Datenabgleiche nach § 117 Bundessozialhilfegesetz. Durch die wachsende Zahl von Vorschriften, die die Auskunftspflicht über Sozialdaten festlegen und automatisierte Datenabgleiche zulassen, wird die Kontrolldichte erhöht und damit das Sozialgeheimnis ausgehöhlt. Aber auch die Praxis des Umgangs mit Sozialdaten zeigt, daß die Verpflichtung der Sozialverwaltung zur Wahrung des Sozialgeheimnisses nicht selten verkannt oder gar ignoriert wird.

Im Berichtszeitraum ging es in verschiedenen Fällen darum, in welchem Umfang die Sozialleistungsträger **Datenerhebungen** zur Klärung von Anspruchsvoraussetzungen vornehmen dürfen und wie weit **Mitwirkungspflichten** der Betroffenen reichen. So wurden beispielsweise Empfängerinnen und Empfänger von Sozialhilfe durch ein Sozialamt veranlaßt, sich ihre **Bewerbungen** von Arbeitgebern, bei denen sie sich beworben hatten, auf einem **Sammelnachweis des Sozialamtes bestätigen** zu lassen. Der Umfang der damit verbundenen **Selbstoffenbarung** der Betroffenen gegenüber Arbeitgebern ist allerdings unverhältnismäßig groß und somit datenschutzrechtlich **unzulässig**. Zwar darf das Sozialamt einen Nachweis über die Versuche, Arbeit zu finden, verlangen, aber es muß dabei das Verfahren so gestalten, daß nicht die eventuellen künftigen Arbeitgeber **untereinander** von den jeweiligen Bewerbungen der Betroffenen erfahren. Sogenannte "Sammelnachweise" dürfen deshalb nicht verwendet werden, sondern allenfalls neutrale, als Einzelnachweis zu gestaltende Vordrucke, die nicht die Angabe des Sozialamts aufweisen. Bei allem ist freilich zu berücksichtigen, daß die Meldung beim Arbeitsamt und die Vorstellung bei den von dort vermittelten Arbeitgebern als Nachweis der Bereitschaft zur Arbeitsaufnahme ausreicht.

Im Rahmen der Sozialhilfegewährung unzulässig ist ebenfalls der Einsatz von **Formularen**, mit denen das Sozialamt zur Klärung der Einkommens- und Vermögensverhältnisse in **allgemeiner Form** ermächtigt werden soll, Auskünfte bei nicht näher bezeichneten Stellen einzuholen - unter anderem Banken und Sparkassen. Das Sozialamt hat im Einzelfall zu entscheiden, gegenüber welcher Stelle genau eine Auskunftsermächtigung in Frage kommt. Dar-

über hinaus kann ohne konkrete Anhaltspunkte nicht verlangt werden, daß einer Einholung von Auskünften pauschal zugestimmt werden soll. Denn dies würde eine überflüssige und damit nicht erforderliche Ermittlungstätigkeit des Sozialamts darstellen. Der Vordruck wird nach Mitteilung des Sozialamts nicht mehr verwendet.

In einem Jugendamt mußte festgestellt werden, daß für verschiedenartige Prüfungsvorgänge jeweils derselbe Fragebogen verwendet wurde. So verlangte es für die Entscheidung über einen Antrag auf Stundung von Elternbeiträgen nach § 17 des Gesetzes über Tageseinrichtungen für Kinder das Ausfüllen eines Formulars, das für die Überprüfung der Leistungspflicht unterhaltspflichtiger Angehöriger vorgesehen war. Dieses Formular hätte nicht schematisch und undifferenziert für die Prüfung einer momentanen, den vorliegenden Stundungsantrag möglicherweise begründenden Härte verwendet werden dürfen, so daß ein neues Formular zu erstellen war.

11.1 Datenschutzprobleme bei Durchführung des Asylbewerberleistungsgesetzes

Asylbewerberinnen und Asylbewerbern steht das grundrechtlich verbürgte Recht auf informationelle Selbstbestimmung zu. So brauchen sie weder unverhältnismäßige Anwesenheitskontrollen zur Überprüfung der Leistungsberechtigung zu erdulden, noch Namensaufdrucke auf Warengutscheinen hinzunehmen, die bei Gutscheineinlösung in Geschäften zur Selbstoffenbarung zwingen.

Ein Sozialamt ließ für eine Asylbewerberunterkunft eine **Anwesenheitsliste** führen, die fortlaufende Eintragungen darüber enthielt, ob Asylbewerberinnen und Asylbewerber täglich ein- oder zweimal "gesichtet" oder nicht angetroffen wurden. Angaben über Fehlzeiten sollten die Prüfungsgrundlage dafür darstellen, ob weiter Leistungen nach dem Asylbewerberleistungsgesetz bezogen werden könnten.

Vor Einführung der Anwesenheitsliste war jedoch nicht geprüft worden, auf welche Weise der tatsächliche Aufenthalt unter Beachtung des Verhältnismäßigkeitsgrundsatzes festgestellt werden kann. Dem Hinweis, die Leistungsberechtigung sei ebenso überprüfbar, wenn das Sozialamt nach entsprechender Unterrichtung der Betroffenen lediglich stichprobenweise Kontrollen vornähme, die in Verdachtsfällen - auf bestimmte Personen beschränkt - gegebenenfalls erhöht werden könnten, zeigte sich das **Sozialamt** aufgeschlossen. Es **hat erklärt, die Liste nicht mehr zu führen**.

"Einkaufskarten machen uns das Leben schwer", "An Ladenkassen wie abgestempelt"

Solche oder ähnliche - tatsächliche - Schlagzeilen vermitteln einen Eindruck von dem Gefühl vieler Asylbewerberinnen und Asylbewerber, wenn sie vom Sozialamt mit vollständigem **Namensaufdruck** versehene Warengutscheine zur Einlösung in einem Geschäft erhalten. Diese Praxis verschiedener Gemeinden ist **nicht datenschutzkonform**. Sie diskriminiert zudem Asylbewerberinnen und Asylbewerber gegenüber Geschäftsleuten. Diese haben keine gesetzliche Befugnis, sich vor der Warenaushändigung Legitimationspapiere der Betroffenen vorlegen zu lassen, weshalb der Name der Betroffenen auf dem Warengutschein von vornherein **ungeeignet** ist, dessen Verkauf oder Weitergabe an Unbefugte zu unterbinden oder irgendeine sonstige Funktion zu erfüllen. Zwar haben fast alle Gemeinden mitgeteilt, auf den Namensaufdruck künftig zu verzichten, doch mußte in einem Fall auch eine förmliche Beanstandung ausgesprochen werden.

- Für den bei Einlösung des Warengutscheins zur Selbstoffenbarung führenden Namensaufdruck gibt es keine gesetzliche Grundlage. Insbesondere kann dieser Aufdruck nicht auf die datenschutzrechtliche Übermittlungsvorschrift des § 16 Abs. 1 Satz 1 d) DSG NW gestützt werden, weil hier nicht das Sozialamt die Übermittlung veranlaßt. Vielmehr hat die Vorlage von Warengutscheinen zwangsläufig eine Selbstoffenbarung der auf die Waren angewiesenen Betroffenen zur Folge. Sie unterliegen in ihrer Entscheidung, von dem Warengutschein Gebrauch zu machen oder nicht und damit ihre Daten gegenüber Dritten preiszugeben, offensichtlich Zwängen und Nöten. Aus dem Grundrecht auf informationelle Selbstbestimmung wie auch dem landesverfassungsrechtlichen Grundrecht auf Datenschutz ergibt sich für das Sozialamt die Verpflichtung, in die **Warengutscheine** nur die für deren **Verwendungszweck erforderlichen** Daten aufzunehmen. Dies sind ausschließlich die Angaben, die der Händler bei Aushändigung der Waren und das Sozialamt bei Vergütung der ausgehändigten Waren gegenüber dem Händler kennen muß. **Namen** von Leistungsberechtigten gehören **nicht** hierzu.

- Das Verhältnis zwischen Sozialamt und Asylbewerberinnen sowie Asylbewerbern (hier: Ausgestaltung eines Warengutscheins) ist dem öffentlichen Recht zugeordnet. Deshalb sind Warengutscheine entgegen der Auffassung der betroffenen Gemeinde nicht einer zivilrechtlichen Anweisung oder einem Inhaberpapier vergleichbar.

- Vorkehrungen zum Schutz vor Warengutscheinmißbrauch und der Schutz des Grundrechts auf informationelle Selbstbestimmung schließen sich nicht aus. Mißbrauchsrisiken können mit anderen Maßnahmen vermindert werden.

Die Auffassung, daß die Namen von Asylbewerberinnen und Asylbewerbern keine in Warengutscheine aufzunehmenden Angaben sind, wird auch vom Innenministerium geteilt. Es wäre schön, wenn sich die für den Datenschutz Verantwortlichen in den Kommunen dieser Problematik verstärkt annähmen, weil die wirklich Betroffenen erfahrungsgemäß schweigen.

11.2 Erneut im Blickpunkt: Datenschutzmängel bei Gewährung von Sachleistungen im Rahmen der Sozialhilfe

Durch Presseberichte, Beschwerden und eine Kleine Anfrage (Drucksache 12/237) wurde bekannt, daß Sozialämter bei der Gewährung von Beihilfen als Sachleistungen **Lieferfirmen** die **Anschriften von Sozialhilfeempfängerinnen und -empfängern** angeben. Hierdurch **übermitteln** sie den Lieferanten die Tatsache des **Sozialhilfebezugs**, ohne daß dies zur Aufgabenerfüllung erforderlich ist. Darauf, daß die Sozialhilfeempfängerinnen und -empfänger vor einer Bekanntgabe ihrer Daten gegenüber privaten Dritten geschützt sind, wurde bereits im 9. Tätigkeitsbericht (S. 62/63) in Übereinstimmung mit der Auffassung der Landesregierung sowie des Städtetages Nordrhein-Westfalen und des Landkreistages Nordrhein-Westfalen (Drucksache 10/5055, S. 38) hingewiesen. Gleichwohl sieht die Praxis nach wie vor zum Teil anders aus. Denn insbesondere knappe Haushaltsmittel veranlassen Sozialämter oft zum Abschluß von Lieferverträgen mit günstigen Rabattsätzen - etwa über eine Vielzahl von Waschmaschinen oder sonstigen Haushaltsgeräten.

Daß die Sozialämter zu wirtschaftlicher und sparsamer Haushaltsführung verpflichtet sind, ist unbestritten. Sie haben bei ihrer Tätigkeit jedoch auch die Grundrechte der Betroffenen zu wahren, hier besonders das Recht auf informationelle Selbstbestimmung. Bei der Gewährung von **Geldleistungen** zum Kauf beispielsweise eines Kühlschrankes treten **keine datenschutzrechtlichen Probleme** auf.

Soll jedoch ein Kühlschrank als **Sachleistung** gewährt werden, wird der Umstand des **Sozialhilfebezuges** mindestens der **privaten Lieferfirma** bekannt. Die Übermittlung von Sozialdaten unterliegt strengen Voraussetzungen. Sie ist nach § 67 b Abs. 1 SGB X nur zulässig, soweit sie von einer speziellen Vorschrift im Sozialgesetzbuch ausdrücklich erlaubt oder angeordnet wird oder die Einwilligung der betroffenen Person in die Datenübermittlung vorliegt. Keine

der Voraussetzungen ist hier erfüllt. Weder existiert eine Erlaubnisnorm, noch ist eine Einwilligung der Betroffenen in die Weitergabe ihrer Anschrift als Lieferadresse vorhanden. Eine rechtswirksame Einwilligung könnte aber auch nicht eingeholt werden, da sie die Freiwilligkeit der Entscheidung voraussetzt, von der keine Rede sein kann. Wird der Kühlschrank nur bei einer Einwilligung in die Datenübermittlung gewährt, herrscht faktischer Zwang. Die Bekanntgabe der Daten an die Lieferfirma stellt somit eine **unbefugte Übermittlung von Sozialdaten** dar und ist datenschutzrechtlich unzulässig.

Die weit überwiegende Mehrheit der betroffenen Sozialämter hat diese Rechtsauffassung **akzeptiert** und ist den ausgesprochenen Empfehlungen gefolgt. Auf meine Anregung hin hat auch das Ministerium für Arbeit, Gesundheit und Soziales mittlerweile mit **Runderlaß** vom 30.09.1996 - II A 5 - 5001.16/ II A 5 - 5000.521 - klarstellend darauf hingewiesen, daß die grundsätzliche Zulässigkeit der Sachleistungsgewährung bei einmaligen Leistungen keine Einschränkung des Grundrechts auf informationelle Selbstbestimmung zur Folge haben darf. Insbesondere mangele es für eine Übermittlung von Sozialdaten aufgrund haushaltsrechtlicher Erwägungen an einer Ermächtigung im Sozialgesetzbuch.

Ein Sozialamt widersetzt sich jedoch unter Berufung auf Äußerungen des Städtetages Nordrhein-Westfalen und zwei Gerichtsentscheidungen (VG Bremen, Urteil vom 04.10.1990, NVwZ-RR 1991, 564 und OVG Münster, Beschluß vom 08.11.1996 -8 A 2729/93-) dieser Rechtslage. Die ältere Entscheidung des VG Bremen vermag nicht zu überzeugen, da die Kammer bei der Prüfung der Erforderlichkeit der Datenübermittlung allein auf die haushaltsrechtlichen Grundsätze der Sparsamkeit und Wirtschaftlichkeit abgehoben und diese wie eine "Befugnisnorm" zur Datenübermittlung gewertet hat. Die Verpflichtung zur sparsamen und wirtschaftlichen Haushaltsführung durchbricht aber das Grundrecht auf informationelle Selbstbestimmung und das aus ihm folgende Sozialgeheimnis nicht, sondern umgekehrt finden die Haushaltsgrundsätze daran ihre Grenze. Auf den Beschluß des OVG Münster kann sich das Sozialamt ebenfalls nicht allgemein berufen. Das Gericht hat hier zwar die Bekanntgabe von Name und Anschrift eines Sozialhilfeempfängers an eine Lieferfirma unbeanstandet gelassen. Die Besonderheit des zugrundeliegenden Sachverhalts bestand jedoch darin, daß der Kläger die ordnungsgemäße Verwendung der ihm zur Verfügung gestellten Mittel dem Sozialleistungsträger gerade nicht nachgewiesen hatte. Aus dieser Entscheidung läßt sich also keineswegs der Schluß auf eine generelle Zulässigkeit der Übermittlung von Sozialdaten an Lieferfirmen ziehen.

11.3 Beschäftigungs- und Qualifizierungsangebote für arbeitsuchende Empfängerinnen und Empfänger von Sozialhilfe

Eine Einwilligungserklärung, mit der ein Sozialamt die vorherige Zustimmung arbeitsuchender Hilfeempfängerinnen und -empfänger für eine Übermittlung ihrer personenbezogenen Sozialdaten an Dritte einholt, um damit Beschäftigungs- und Qualifizierungshilfe zu leisten, muß datenschutzrechtlichen Anforderungen genügen.

Ein Sozialamt hatte arbeitsuchenden Hilfeempfängerinnen und -empfängern die Möglichkeit eingeräumt, auf freiwilliger Basis selbst über die Übermittlung ihrer Daten an eine Beschäftigungs- und Qualifizierungsgesellschaft entscheiden zu können. Ihnen wurde hierzu allerdings eine Einverständniserklärung vorgelegt, die datenschutzrechtlichen Anforderungen nicht genügte. Der Kontakt mit dem Sozialamt führte zur Änderung des Erklärungsformulars.

Einwilligungserklärungen müssen

- vor der **Übermittlung eingeholt** werden,
- grundsätzlich **in Schriftform** erfolgen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist; dabei ist zu beachten, daß eine stillschweigende oder mutmaßliche Einwilligung unwirksam ist,
- ohne Schwierigkeiten **erkennen lassen, welche Daten** von wem an wen und zu welchem Zweck im Einzelfall **übermittelt** werden sollen sowie
- den **Hinweis** enthalten, **daß** Hilfeempfängerinnen und -empfänger die **Einwilligung verweigern können** und welche Rechtsfolgen dann eintreten.

11.4 Eingeschränkte Auskunftspflicht des Sozialamtes gegenüber der Polizei

Eine Stadtverwaltung hat um Rat gebeten, ob ihr Sozialamt zur Unterrichtung der Polizei über den Aufenthalt eines ratsuchenden Bürgers in ihren Amtsräumen verpflichtet ist.

Nach § 35 Abs. 1 SGB I hat jeder Anspruch darauf, daß die ihn betreffenden Sozialdaten von den Leistungsträgern nicht unbefugt erhoben, verarbeitet und genutzt werden (**Sozialgeheimnis**). Die personenbezogenen Daten im Sinne dieser Vorschrift genießen als Teil des allgemeinen Persönlichkeitsrechts den Grundrechtsschutz auf informationelle Selbstbestimmung gemäß Artikel 1

Abs. 1 i.V.m. Artikel 2 Abs. 1 GG. Zu den nach § 35 Abs. 1 SGB I **geschützten** Einzelangaben gehört neben der Eigenschaft als Sozialhilfeempfängerin oder -empfänger **auch** der **vorübergehende Aufenthalt bei einem Sozialleistungsträger**, soweit ein Zusammenhang mit der Inanspruchnahme von Sozialleistungen besteht.

Gleichwohl ist unter gewissen Voraussetzungen eine Datenübermittlung an die Polizei zulässig: So ist zur Durchführung eines Strafverfahrens wegen eines Verbrechens oder wegen einer sonstigen Straftat von erheblicher Bedeutung eine Übermittlung von Sozialdaten gemäß § 73 SGB X zulässig, soweit sie auf **richterliche Anordnung** erfolgt ist. Im Rahmen der **Amtshilfe** ist es gemäß § 68 zulässig, Name, Vorname, Geburtsdatum und -ort, **derzeitige Anschrift** des Betroffenen sowie Namen und Anschriften seiner derzeitigen Arbeitgeber zu übermitteln, soweit kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Die Beziehungen einer Person zu einem Sozialleistungsträger, also auch der bisher nicht bekannte vorübergehende Aufenthalt im Sozialamt, gehören dagegen nicht zu den übermittelbaren Daten. Die **derzeitige Anschrift**, die § 68 SGB X als Ausnahmevorschrift für übermittelbar hält, kann mit dem **vorübergehenden Aufenthalt nicht gleichgesetzt** werden. Seit Inkrafttreten des SGB X besteht daher in NRW nicht mehr die Praxis, Fahndungslisten an die Behörden zu geben, damit diese Besucher bei der Polizei melden. Das hat in der Praxis der polizeilichen Fahndung bisher auch nicht zu erkennbaren Defiziten geführt, da Täter erheblicher Straftaten beim Sozialamt nicht vorzusprechen pflegen.

Eine Übermittlungsbefugnis oder gar -pflicht des Sozialamtes zur Unterrichtung der Polizei über den vorübergehenden Aufenthalt von Ratsuchenden besteht nicht. Die Mitarbeiterinnen und Mitarbeiter der Sozialämter sind keine Hilfsbeamten der Staatsanwaltschaft und keine Fahndungsorgane.

11.5 Fehlerhafte Beschlagnahme einer Jugendamtsakte

Zu Recht war ein Jugendamt der Auffassung, daß eine auf telefonischen Antrag einer Staatsanwaltschaft erwirkte gerichtliche Beschlagnahme (gemäß §§ 94, 98 StPO) einer Jugendamtsakte mit den Vorschriften des Sozialdatenschutzes nicht in Einklang stand.

Eine Übermittlung von Sozialdaten für die Durchführung eines Strafverfahrens ist nach § 73 SGB X nur zulässig, wenn sie richterlich angeordnet ist. Dabei muß die richterliche Anordnung darauf gerichtet sein, Sozialdaten zu übermitteln. Ein Gerichtsbeschluß, mit dem nur allgemein die Beschlagnahme der Jugendamtsakte gemäß §§ 94, 98 StPO angeordnet wird, ist nicht ausreichend.

Gericht und Staatsanwaltschaft haben die vom Gesetzgeber abschließend im Sozialgesetzbuch getroffenen Regelungen, §§ 67 a bis 78 SGB X, für die Befugnis der Leistungsträger zur Übermittlung von Sozialdaten (vgl. bereits 9. Tätigkeitsbericht, S. 65) zu beachten. Danach unterliegen Akten von Leistungsträgern, die in § 35 SGB I näher bezeichnet sind, einem Beschlagnahmeverbot. Wenn die Voraussetzungen der §§ 73 oder 68 SGB X nicht gegeben sind, bleibt den Strafverfolgungsbehörden der Weg, die Einwilligung der betroffenen Person in die Aktenübersendung (§ 67 b SGB X) einzuholen.

Der Schutz des Sozialgeheimnisses gilt grundsätzlich auch gegenüber den Gerichten. Das Sozialgeheimnis ist, soweit keine gesetzliche Offenbarungsbefugnis vorliegt, gerichtsfest.

11.6 Vorbeugung gegen Übergriffe

Eine in Scheidung lebende Bürgerin hatte den Wohnort gewechselt und beim Einwohnermeldeamt eine **Auskunftssperre** eintragen lassen, um sich und ihre Kinder vor ihrem aggressiven Ehemann zu schützen. Auf die Bitte einer Mitarbeiterin des bisher zuständigen Jugendamtes, das noch in das Verfahren vor dem Familiengericht eingeschaltet war, hatte sie ihre neue Anschrift dem Jugendamt offenbart, weil mit dem Wohnungswechsel auch ein Wechsel der örtlichen Zuständigkeit des Jugendamtes eingetreten war. Hinsichtlich ihrer neuen Anschrift ließ sie sich zwar ausdrücklich Vertraulichkeit zusichern, doch gab das Jugendamt in seinem Abschlußbericht dennoch die neue Adresse preis, weil es sich für verpflichtet hielt, sie dem Familiengericht wegen der Änderung der örtlichen Zuständigkeit mitzuteilen. Diesen Bericht erhielt auch der Rechtsanwalt des Ehemannes, der damit Kenntnis von der neuen Anschrift der Betroffenen nehmen konnte.

Hier wurden die Befürchtungen der Frau hinsichtlich ihres gewalttätigen Ehemanns formalen Verwaltungsabläufen untergeordnet. Zwar ist die Übermittlung der neuen Anschrift an das Familiengericht allein aus datenschutzrechtlicher Sicht nicht zu beanstanden. Es hätte allerdings eine Verständigung über die Geheimhaltung der Anschrift gegenüber dem Ehepartner zwischen Jugendamt und Gericht angestrebt werden müssen. Ein Hinweis, daß Ansprechpartner für Fragen des Umgangsrechts nunmehr das Jugendamt des neuen Wohnorts der Betroffenen ist, hätte ausgereicht.

11.7 Datenschutzmängel bei Schwerbehindertenausweisen

Aus der Verpflichtung des Leistungsträgers zur Wahrung des Sozialgeheimnisses können Schwerbehinderte gegenüber dem Leistungsträger beanspruchen, nur solche Angaben in den Schwerbehindertenausweis

aufzunehmen, die für dessen Verwendungszweck unbedingt erforderlich sind.

Aus einem Schwerbehindertenausweis ist unter Umständen der gesamte Entwicklungsverlauf einer Schwerbehinderung über einen Zeitraum von mehreren Jahren ersichtlich. Das so entstandene "**Behinderungsprofil**" wird Dritten bei der Vorlage des Ausweises zwangsläufig offenbart, obwohl der Ausweis lediglich dem Nachweis für die Inanspruchnahme von Rechten und Nachteilsausgleichen dienen soll, die Schwerbehinderten nach dem Schwerbehindertengesetz oder auch anderen Vorschriften auf Grund ihrer **aktuellen** Situation zu gewähren sind. Daher bestehen erhebliche Zweifel, ob die in der Schwerbehindertenausweisverordnung getroffenen, mit Eingriffen in das Recht auf informationelle Selbstbestimmung der Schwerbehinderten verbundenen Regelungen über die Gestaltung von Schwerbehindertenausweisen in jedem Detail erforderlich und damit verhältnismäßig sind. Auch eine vom Gesetzgeber gewollte verwaltungsökonomische Verfahrensweise bei Ausstellung und Gestaltung der Schwerbehindertenausweise darf nicht zu **unverhältnismäßigen Belastungen** betroffener Schwerbehinderter führen.

Beim Ministerium für Arbeit, Gesundheit und Soziales wurde die Überarbeitung der Vorschriften angeregt, damit künftig sichergestellt wird, daß irrelevante Daten Dritten nicht bekanntgemacht werden müssen.

12. Gesundheitsbereich

Die ärztliche Schweigepflicht ist in den ärztlichen Berufsordnungen verankert und schützt die Persönlichkeitssphäre von Patientinnen und Patienten. Technischer Fortschritt und steigender Kostendruck im Gesundheitswesen gefährden jedoch in zunehmendem Maße die Wahrung des Arztgeheimnisses. Der fortschreitende **Einsatz von Technik** - Stichwort: Telemedizin - wirft neue Probleme auf, insbesondere im Hinblick auf die Datensicherheit. Der auf den gesetzlichen Krankenversicherungen lastende Kostendruck zwingt die Leistungsträger zu verstärkter Kontrolle ärztlicher Abrechnungen mit der Folge, daß das **Arzt-Patientengeheimnis** in die Gefahr gerät, brüchig zu werden. Hier sind die Datenschutzbeauftragten ebenso gefordert wie bei der Diagnoseverschlüsselung, die im Gesundheitswesen mehr Transparenz und Effizienz herstellen soll, keinesfalls aber zu gläsernen Patientinnen und Patienten führen darf.

Auch in anderen Bereichen des Gesundheitswesens steht der Schutz des Arzt-Patientengeheimnisses im Vordergrund. So gehört es beispielsweise zum "Alltagsgeschäft" des Datenschutzes, darauf aufmerksam zu machen, daß Daten von Patientinnen und Patienten im Regelfall nur mit ihrer **Einwilligung** an Dritte übermittelt werden dürfen. Dies gilt auch für Patientendaten, die zu Forschungszwecken übermittelt werden sollen. Sind die Voraussetzungen des § 6 GDSG NW nicht erfüllt, besteht für die Ärztinnen und Ärzte das Risiko, sich nach § 203 StGB strafbar zu machen. Die ärztliche Schweigepflicht ist im übrigen - wenn auch in eingeschränktem Umfang - über den Tod der Betroffenen hinaus zu wahren.

Empfindliche Gesundheitsdaten werden auch von den Krankenkassen verwaltet. Im Zuge von durch das Gesundheitsstrukturgesetz bedingten Änderungen der Organisationsstrukturen einiger Krankenkassen wird von einem Teil der Krankenkassen eine zentrale Verarbeitung und ein dezentraler Zugriff auf Versichertendaten angestrebt. Mit entsprechenden Online-Verbindungen wird bei bestimmten Krankenkassen eine landesweite oder überregionale Zugriffsmöglichkeit auf alle Versichertendaten bei den angeschlossenen Geschäftsstellen eröffnet. Dies begegnet datenschutzrechtlichen Bedenken. Denn es bedeutet für die Kundinnen und Kunden dieser Krankenkassen, daß eine unüberschaubare Vielzahl von Beschäftigten in jeder Geschäftsstelle des gesamten Bundesgebietes auf alle bei der Krankenkasse vorhandenen Gesundheitsdaten zugreifen können. Für Notfälle mag es im Einzelfall sinnvoll sein, daß überall auf einen Stammsatz von Daten (zum Beispiel, ob die betreffenden Personen versichert sind) zurückgegriffen werden kann. Für den Regelfall ist jedoch der **Zugriff** auf sämtliche Krankheitsdaten der Versicherten bei **einer Geschäfts-**

stelle ausreichend (s. dazu auch die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 09./10.03.1995, Abdruck im Anhang). Davon unberührt bleibt selbstverständlich ein **geschäftsstellenübergreifender Zugriff** auf alle Versichertendaten, **wenn** dies die bzw. der **Versicherte ausdrücklich wünscht**.

Fragen zur Reichweitc des Rechts auf informationelle Selbstbestimmung stellen sich auch bei der anstehenden gesetzlichen Regelung eines **Transplantationsgesetzes**. Hier ist die Organspende an die **ausdrückliche Zustimmung** der Spenderin oder des Spenders zu knüpfen. Damit bedarf es keiner Dokumentation von Ablehnungen und keines Organspenderegisters, so daß das Recht auf informationelle Selbstbestimmung weitestgehend gewahrt bleiben kann (s. dazu auch die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 14./15.03.1996, Abdruck im Anhang).

Die an der vertragsärztlichen Versorgung teilnehmenden Ärztinnen und Ärzte sind nach § 295 Abs. 1 SGB V verpflichtet, die auf den Arbeitsunfähigkeitsbescheinigungen und den Abrechnungsunterlagen einzutragenden **Diagnosen** nicht mehr in freier Formulierung anzugeben, sondern sie nach dem Diagnoseschlüssel **ICD-10 zu verschlüsseln**. Erfolgt dies nicht, riskieren sie eine Verweigerung ihres Honorars.

Die bisherige Verfahrensweise, Diagnosen frei formuliert auf den Abrechnungsunterlagen zu verzeichnen, hat automatisierte Verfahren zur Abrechnung und Wirtschaftlichkeitsprüfung weitgehend ausgeschlossen. Da die Einführung solcher Verfahren wegen der Kostensteigerungen im Gesundheitswesen als notwendig angesehen wurde, bedurfte es gesetzlicher Regelungen zur Vereinheitlichung von Diagnoseangaben. Vor diesem Hintergrund wurde im Gesetzgebungsverfahren die Einführung der Diagnoseverschlüsselung unter großem Zeitdruck und ohne ausreichende Erörterung ihrer Konse-

Diagnoseschlüssel ICD-10 *("International Statistical Classification of Diseases" in der 10. Fassung):*
Die "Internationale Statistische Klassifikation der Krankheiten und verwandter Gesundheitsprobleme" (ICD-10-Code) ist die deutsche Fassung einer systematischen Klassifikation der Weltgesundheitsorganisation für die Erforschung von Krankheits- und Todesursachen. In ca. 14 000 Ziffern enthält sie zum Teil vielfach untergliederte medizinische und psychologische Diagnosen mit einem vierstelligen Schlüssel, aber auch Angaben zur sozialen Situation, zum Geisteszustand etc. und Symptomdiagnosen (zum Beispiel pathologisches Stehlen). Häufige Diagnosen wie zum Beispiel "grippaler Infekt" fehlen jedoch.

quenzen beschlossen. Während der Gesetzesberatungen wurde insbesondere davon ausgegangen, daß die ursprünglich für wissenschaftliche Zwecke entwickelte Klassifikation der Krankheiten auch für die Abrechnung und Kontrolle ärztlicher Leistungen geeignet sei. Es hat sich jedoch nach der von ärztlicher Seite und insbesondere von den Datenschutzbeauftragten des Bundes und der Länder erhobenen Kritik herausgestellt, daß die **Zwecktauglichkeit** der Diagnoseverschlüsselung nach dem ICD-10-Code **zweifelhaft** und vor allem der **Umfang der Datenübermittlungen problematisch** ist. Die Verwendung des ICD-10-Codes wäre damit in vielen Fällen unverhältnismäßig.

Zur Zeit wird auf Bundesebene unter Beteiligung des Bundesbeauftragten für den Datenschutz über eine praktikable Fassung der Diagnoseverschlüsselung beraten, die unter Beachtung der datenschutzrechtlichen Bestimmungen den Notwendigkeiten der Leistungsabrechnung, der Leistungsdokumentation und der Wirtschaftlichkeitskontrolle in der ambulanten und stationären Versorgung entspricht. **Umfang und Differenzierungsgrad von Diagnoseangaben** sollen auf das für die Wahrnehmung der gesetzlichen Aufgaben der Krankenkassen, Krankenhäuser und Kassenärztlichen Vereinigungen notwendige Maß **begrenzt werden**.

Nach einem vom Bundesministerium für Gesundheit im Sommer 1996 vorgelegten Entwurf für die Neufassung des § 2 a Abs. 1 der Betäubungsmittel-Verschreibungsverordnung waren weitgehende Unterrichtungspflichten von Ärztinnen und Ärzten gegenüber den obersten Landesgesundheitsbehörden vorgesehen, um **Mehrfachverschreibungen** des Drogen-Substitutionsmittels **Methadon** an dieselbe Person zu **verhindern**. Gegen die Erforderlichkeit des vorgesehenen Meldeverfahrens wurden datenschutzrechtliche Bedenken erhoben, weil eine die Substitutionsbehandlungen betreffende ärztliche Meldepflicht bereits gegenüber der Kassenärztlichen Vereinigung und der Krankenkasse zur Vermeidung von Mehrfachsubstitutionen existiert. Selbst wenn diese Meldepflicht entfiele, hätte die geplante Regelung jedoch einer besonderen gesetzlichen Ermächtigung bedurft, da die in § 13 Abs. 3 BtMG vorgesehene Verordnungsermächtigung insoweit nicht genügt. Darüber hinaus führte eine solche Regelung zur Entstehung ohnehin problematischer **länderübergreifender Personenregister** bei den obersten Landesgesundheitsbehörden.

Erneut war im Berichtszeitraum der Umfang der **Unterlagen** streitig, den der **Medizinische Dienst der Krankenversicherung (MDK)** anfordern kann. Auf die frühere Rechtslage ist bereits im 11. Tätigkeitsbericht ausführlich eingegangen worden (siehe S. 66/67 mit zustimmender Auffassung der Landesregierung, Drucksache 11/6876, S. 47). Auch nach Inkrafttreten der Vorschriften des Zweiten Gesetzes zur Änderung des Sozialgesetzbuchs vom 13.06.1994

- BGBl. I S. 1229 - sind Leistungserbringer gemäß § 276 Abs. 2 Satz 1 2. Hs. SGB V verpflichtet, Sozialdaten auf Anforderung des MDK unmittelbar an diesen zu übermitteln, soweit dies für die gutachtliche Stellungnahme und Prüfung erforderlich ist. Nicht vorgesehen ist, daß die Leistungserbringer Unterlagen zu übermitteln haben, die ihnen von anderen Leistungserbringern (Krankenhäusern, Kurkliniken, Konsiliarärzten) zugänglich gemacht worden sind. Die **Übermittlung von Sozialdaten** an den MDK ist somit auf Unterlagen **beschränkt**, in denen von dem jeweiligen Leistungserbringer selbst für die Betroffenen erbrachte Leistungen dokumentiert sind. Dazu gehören allerdings auch die im konkreten Auftrag der behandelnden Ärztin oder des behandelnden Arztes erstellten Unterlagen (wie zum Beispiel Röntgenbilder und Laborbefunde) oder solche Fremdbefunde, die die Leistungserbringer in ihre Beurteilung mit einbezogen haben.

12.1 Chipkarten im Gesundheitsbereich

Die berechtigten Interessen von Patientinnen und Patienten und ihr Grundrecht auf informationelle Selbstbestimmung müssen auch bei Einführung von Chipkarten im Gesundheitswesen künftig Ausgangspunkt aller Überlegungen sein.

Auch im Gesundheitsbereich wird die Nutzung von Chipkarten und von zentralen Datensammlungen geplant. Gerade die sensiblen Gesundheitsdaten bedürfen jedoch eines **besonderen Schutzes**. Angesichts der Möglichkeit, auf den Karten oder in zentralen Netzen eine Vielzahl von Gesundheits- und Krankheitsdaten zu speichern, die potentiell von verschiedensten Institutionen zu vielfältigsten Zwecken genutzt oder auch mißbraucht werden könnten, ist eine grundsätzlich **kritische Haltung** angebracht. Dies gilt insbesondere im Hinblick auf sogenannte **multifunktionale Chipkarten**. Derartige Karten beinhalten einen winzigen Mikrochip sowie einen sehr leistungsfähigen optischen Speicher (Beispiel: "Hybridkarte"). Solche Speichermedien können fortlaufend mit Patientendaten bestückt werden. Sie sind daneben auf Grund ihrer hohen Speicherkapazität in der Lage, auch umfangreiche Patientendaten zu speichern, etwa Laborbefunde oder Ultraschallaufnahmen. Im Raum stehen Visionen einer Totalspeicherung medizinischer Daten mit arztbezogenen Zugriffsberechtigungen, die von der Eingabe einer Patienten-Codenummer abhängen. Die damit verbundenen **Risiken** für das Recht auf informationelle Selbstbestimmung wären kaum übersehbar.

Die Verschiedenartigkeit der Chipkarten, über die nachgedacht wird, zwingt zu **differenzierten Antworten**. Die Datenschutzbeauftragten des Bundes und der Länder haben in ihrer **Entschließung** vom 09./10.11.1995 (Abdruck im

Anhang) **datenschutzrechtliche Anforderungen** an den Einsatz von Chipkarten im Gesundheitswesen formuliert und sind in einen Dialog mit der Ärzteschaft getreten. Die Bundesärztekammer stimmt insbesondere der Forderung der Datenschutzbeauftragten zu, daß die **freie Entscheidung** der Betroffenen zur Verwendung einer Chipkarte gewährleistet sein muß. Weiterer Diskussions- und Klärungsbedarf besteht allerdings noch zu folgenden Problemen:

- Die Einführung und insbesondere zunehmende Verbreitung von Chipkarten, aber auch die Verwendung von krankheitsspezifischen Karten mit zunächst begrenztem Einsatzbereich kann bei Patientinnen und Patienten unmerklich zu einem sozialen Anpassungsdruck führen, Chipkarten anzunehmen. Dies birgt die Gefahr, daß die **freie Entscheidung für oder gegen die Chipkartenverwendung in Frage gestellt wird.** Die Ärzteschaft stellt demgegenüber das ärztliche Interesse an weitgehender Information über die in den Chipkarten gespeicherten Gesundheitsdaten in den Vordergrund.
- Auf Chipkarten sollte auch künftig nicht der in § 291 Abs. 2 SGB V abschließend festgelegte Datensatz der Krankenversichertenkarte gespeichert werden, weil andernfalls die vom Gesetzgeber getroffene Entscheidung, Datensatz und Nutzungszwecke der **Krankenversichertenkarte** zu begrenzen, in Frage gestellt wäre. Dies sieht die Ärzteschaft bisher anders.
- Weiter obliegt es nach Auffassung der Datenschutzbeauftragten dem Gesetzgeber, den rechtlichen Rahmen für den Zugriff auf außerhalb der Obhut der Ärztin oder des Arztes des Vertrauens automatisiert gespeicherte Gesundheitsdaten vorzugeben.
- Schließlich wird aus medizinischer Sicht der optimale Informationstransfer mittels Chipkarte als wünschenswert bezeichnet. Nach der gegenwärtigen Rechtslage hängt die Übermittlung personenbezogener, dem Arzt-Patientengeheimnis unterliegender Daten jedoch in weitem Umfang ausschließlich von der Einwilligung der Patientinnen und Patienten ab.

Eine **krankheitsspezifische Patientenkarte**, die zur Zeit in einem Pilotprojekt einer Universitätsklinik und insbesondere zur Nachsorgebetreuung erprobt wird, wirft demgegenüber weniger Probleme auf. Zur Gewährleistung der Datensicherheit ist bei dieser Karte die Zuteilung einer **persönlichen Identitätsnummer** (PIN) für jede Patientin und jeden Patienten vorgesehen. Sie stellt sicher, daß die genau festgelegten medizinischen Daten, die auf der Karte gespeichert werden, nur nach Eingabe dieser Nummer von dem Lesegerät der Ärztin oder des Arztes abgerufen werden können. Davon unabhängig haben Patientinnen und Patienten ein **eigenständiges Leserecht** für alle auf der Chipkarte befindlichen Daten. Wegen der psychisch belastenden Krankheitssituation ist die **Aufklärung** der Betroffenen über die Einsatzbreite der Patien-

tenkarte besonders wichtig. Die **Einwilligungserklärung** zur Verarbeitung der personenbezogenen Daten muß zudem **präzise** formuliert sein.

12.2 Übertriebene Arztdokumentation

Die Grenzen einer angemessenen ärztlichen Dokumentation sind auch bei Notfalluntersuchungen in einem Krankenhaus überschritten, wenn zur Erstellung der Diagnose sachfremde oder unzumutbare Fragen gestellt und diskriminierende Äußerungen in Arztberichten festgehalten werden.

In der Neurochirurgischen Klinik der Medizinischen Einrichtungen einer Universität wurden einem Patienten mit sehr starken Kopfschmerzen vom notfalldiensthabenden Arzt folgende Fragen gestellt: "Sind Sie verheiratet? Haben Sie Kinder? Sind Sie homosexuell? Wann haben Sie zuletzt einen AIDS-Test machen lassen? Hatten Sie in letzter Zeit wechselnde Geschlechtspartner?". Bei der weiteren Behandlung in der Notaufnahmestation einer anderen Klinik der Medizinischen Einrichtungen wurde er von der dort tätigen Ärztin gefragt, ob er sich einem AIDS-Test unterziehen wolle. Hierüber solle er jedenfalls nachdenken. Anschließend hat der Patient Kenntnis von einem das Untersuchungsergebnis enthaltenden Konsiliarbrief der Neurochirurgische Klinik erhalten. Hierin befand sich neben Diagnoseangaben und Untersuchungsergebnissen in einer Rubrik "**weitere Probleme**" die Angabe "**Homosexualität**".

Es bestehen bereits Zweifel, ob die vom Patienten beklagten Kopfschmerzen die Frage nach einer HIV-Infektion und die weiteren Fragen aus dem Intimleben rechtfertigten. Dies unterliegt jedoch letztlich der ärztlichen Beurteilung für die Erforderlichkeit der im Rahmen diagnostischer Überlegungen zu stellenden Fragen.

Jedenfalls wurden hier Vorschriften des Datenschutzes verletzt. Patientendaten dürfen im Krankenhaus nur erhoben und gespeichert werden, soweit dies zur Durchführung unter anderem der ärztlichen Dokumentationspflicht erforderlich ist (§ 10 Abs. 1 Satz 1 Buchstabe a) GDSG NW). Nachvollziehbare Gründe für die dem Patienten gestellten Fragen sowie die Speicherung der Angabe "Homosexualität" in dem Konsiliarbrief waren weder aus der Stellungnahme der Medizinischen Einrichtungen ersichtlich noch sonst erkennbar. Die Erhebung und Speicherung der mit den Antworten auf die oben genannten Fragen verbundenen Daten waren **datenschutzrechtlich** ebenso **unzulässig** wie der Vermerk über die Homosexualität des Betroffenen. Hinzu kommt die Benennung der Homosexualität in der speziellen Rubrik "weitere Probleme", die diskriminierenden Charakter trägt.

Auf Grund des Folgenbeseitigungsanspruchs des Patienten müssen die in diesem Zusammenhang erhobenen Daten daher **gelöscht**, das heißt in den Arztunterlagen unumkehrbar unkenntlich gemacht werden. Dies habe ich den Medizinischen Einrichtungen mitgeteilt und darüber hinaus darauf hingewiesen, daß die Angabe "Homosexualität" im Konsiliarbrief in der Rubrik "weitere Probleme" **weder erforderlich noch** für den Patienten **zumutbar** war. Den Medizinischen Einrichtungen wurde weiter empfohlen, künftig Patientendaten nur zu erheben, soweit dies medizinisch erforderlich ist und an andere behandelnde Ärztinnen und Ärzte nur weiterzugeben, wenn das Einverständnis der Patientin oder des Patienten vorliegt oder anzunehmen ist. Auch wurde gebeten sicherzustellen, daß entweder das verwendete Formular geändert, insbesondere die Rubrik "weitere Probleme" gestrichen wird, oder unter dieser Rubrik nur medizinische Probleme von den behandelnden Ärztinnen und Ärzten benannt werden.

Ich gehe davon aus, daß in Zukunft Daten über die sexuelle Orientierung von Patientinnen und Patienten weder erhoben noch übermittelt werden.

12.3 Aufklärung vor Hausbesuchen durch den Sozialpsychiatrischen Dienst

Hausbesuche des Sozialpsychiatrischen Dienstes, die im Wege der vorsorgenden Hilfe gemäß § 8 des Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (PsychKG) erfolgen, müssen Betroffenen sowohl unter Mitteilung der Rechtsgrundlage als auch mit dem Hinweis auf die Freiwilligkeit der Inanspruchnahme dieser Hilfe frühzeitig angekündigt werden.

Zur vorsorgenden Hilfe nach dem PsychKG stattete der Sozialpsychiatrische Dienst eines Gesundheitsamtes einer Bürgerin ohne vorherige Anmeldung einen Hausbesuch ab und teilte ihr erst danach die entsprechende Rechtsgrundlage hierfür schriftlich mit. Dabei wurde jedoch nicht berücksichtigt, daß vorsorgende Hilfe Betroffenen nicht aufgezwungen werden kann und es ihnen überlassen bleiben muß, vor dem Hausbesuch **selbst zu entscheiden**, ob sie eine solche Form der Beratung wünschen oder nicht. Hierüber sind die Betroffenen **frühzeitig aufzuklären**, und zwar uneingeschränkt und unabhängig vom Krankheitsbild. Durch die Vorgehensweise des Gesundheitsamtes kann leicht der falsche Eindruck entstehen, es bestehe eine Verpflichtung oder gar ein Zwang, sich beraten zu lassen.

Das Gesundheitsamt hat versichert, Betroffene künftig vor beabsichtigten Hausbesuchen im Rahmen der vorsorgenden Hilfe regelmäßig zu informieren sowie auf die Freiwilligkeit der Maßnahme hinzuweisen.

12.4 Landesweite Zusammenführung von Daten im Rahmen einer Vorstudie zur Kindesentwicklung

Eine Universitätsklinik wollte in einer Vorstudie Querschnittserhebungen über Geburten (Perinatalerhebungen) zusammenführen mit Befunden, die bei Einschulungsuntersuchungen erfaßt wurden. Hiergegen wurden folgende **datenschutzrechtliche Bedenken** erhoben:

- In einem Anschreiben an die Eltern gingen die Ärzte der Universitätsklinik von der rechtlich nicht zutreffenden Annahme aus, daß die Gesundheitsämter im Rahmen der Einschulungsuntersuchung Fragen zu Schwangerschaft und Geburt stellen dürften. Bereits im 10. Tätigkeitsbericht (S. 87/88) wurde - in Übereinstimmung mit der Auffassung der Landesregierung (Drucksache 11/3176, S. 42) - darauf hingewiesen, daß eine derart weitgehende Ausforschung sensibler Daten wie zum Beispiel die Frage nach Schwangerschaft und Geburtsverlauf den Rahmen einer Einschulungsuntersuchung sprengt. Die Untersuchung hat sich auf die Beurteilung der Schulfähigkeit aus medizinischer Sicht anhand des aktuellen körperlichen Zustandes des Kindes zu beschränken. Gesundheitsämter können sich darüber hinaus nicht außerhalb ihrer gesetzlichen Aufgabenerfüllung - wenn auch auf freiwilliger Grundlage - Kenntnis über Daten verschaffen (zum Beispiel Geburtsgewicht, Geburtsklinik, Geburtsjahrgang der Mutter), die für die Einschulungsuntersuchung irrelevant sind.
- Zudem dürfen die Daten der Perinatalerhebungen nur im Rahmen ihrer Zweckbestimmung verwendet und verarbeitet werden. Dieser bereits mit Beschluß der Datenschutzbeauftragten des Bundes und der Länder vom 10.05.1985 erhobenen Forderung (siehe 7. Tätigkeitsbericht, S. 73/74) widersprach das Vorhaben der Zusammenführung von Daten aus Einschulungsuntersuchungen mit Daten der Perinatalerhebungen, unabhängig davon, ob die Vorstudie tatsächlich als anonymisiert hätte angesehen werden können.

Das um Stellungnahme gebetene Ministerium für Arbeit, Gesundheit und Soziales hat mitgeteilt, aus gesundheitspolitischer Sicht halte es das Ziel der Studie zwar für gewichtig, es teile jedoch die Auffassung, daß das Vorhaben unter den bestehenden Rahmenbedingungen rechtlichen Bedenken begegne.

13. Statistik

Mit dem Statistikgeheimnis als einem der bestgehüteten Geheimnisse überhaupt wurde vor Jahren bei der Volkszählung geworben. Anfragen von Bürgerinnen und Bürgern, die bei Mikrozensusbefragungen und anderen statistischen Erhebungen Auskünfte erteilen müssen, signalisieren immer wieder Unsicherheit und Unbehagen hinsichtlich der Verwendung ihrer Daten.

Mit dem neuen **Mikrozensusgesetz** vom 17.01.1996 - BGBl. I S. 34 - wurde das Erhebungsprogramm der Repräsentativstatistik über die Bevölkerung und den Arbeitsmarkt sowie die Wohnsituation der Haushalte neu geregelt. Der Mikrozensus soll in den Jahren 1996 bis 2004 unter Berücksichtigung der Anforderungen der EU-Arbeitskräftestichprobe durchgeführt werden. Auch künftig ist die Einbeziehung von bis zu 1 % der Bevölkerung in die Erhebung vorgesehen. Jährlich wird mindestens ein Viertel der Auswahlbezirke wie bisher durch neue Auswahlbezirke ersetzt. Wiederum sind neben Pflichtauskünften freiwillige Auskünfte vorgesehen. Die Anzahl der Fragen hat zugenommen - auch derjenigen mit Auskunftspflicht. Insgesamt ergibt sich jedoch eine gewisse Verringerung der Belastung der zu Befragenden, weil bestimmte Fragengruppen künftig nur alle vier Jahre und bei nur 0,5 % der Bevölkerung erhoben werden.

Nach der **EU-Unternehmensregisterverordnung** (Verordnung [EWG] Nr. 2186/93 des Rates vom 22.07.1993 über die innergemeinschaftliche Koordinierung des Aufbaus von Unternehmensregistern für statistische Verwendungszwecke - ABl EG L 196/93 -) sind die Mitgliedstaaten der Europäischen Union dazu verpflichtet, **Register über Unternehmen** zu errichten und fortzuführen. Die Register sollen bestimmte Angaben zur Unternehmenstätigkeit sowie unternehmensbezogene Statistiknummern enthalten, die den Statistischen Ämtern die Zusammenführung der statistischen Daten aus verschiedenen Registern der beteiligten Verwaltungen ermöglicht.

Zur Umsetzung dieser Verordnung in nationales Recht wird zur Zeit der Entwurf eines **Statistikregistergesetzes** erarbeitet. Er sieht im wesentlichen vor, daß die Finanz**behörden**, die Bundesanstalt für Arbeit, die Handwerkskammern und die örtlichen Gewerbemeldestellen **aus ihrem Datenbestand Angaben über Unternehmen** (zum Beispiel über Umsätze, Betriebseinkünfte, Anzahl der sozialversicherungspflichtigen Beschäftigten, wirtschaftliche Haupt- und Nebentätigkeiten, aber auch Hilfsangaben wie Adreßdaten) **an die statistischen Ämter zum Aufbau und zur Führung eines Unternehmensregisters übermitteln**. Besonders die beiden folgende Punkte sind datenschutzrechtlich problematisch und bedürfen der Änderung:

- Es ist nicht notwendig, die Übermittlung von Umsatz- und Beschäftigtendaten vorzusehen, weil nach den Regelungen der EU-Unternehmensregisterverordnung Zuordnungen zu Größen- und Beschäftigtenklassen genügen.
- Soweit es tatsächlich erforderlich sein sollte, weiteren Stellen Mitteilungspflichten aufzuerlegen, ist dies im Statistikregistergesetz selbst zu regeln und nicht einer Verordnung zu überlassen.

14. Finanzwesen

Abgabenordnung - die heile Welt der Steuerverwaltung?

Die bisherigen langjährigen Bemühungen, die Abgabenordnung mit bereichspezifischen Datenschutzregelungen zu ergänzen, scheinen trotz anderslautendem Votum der Landesregierung in ihrer Stellungnahme zum 12. Tätigkeitsbericht vom 22.12.1995 (vgl. LT-Vorlage 12/291, S. 10) gescheitert zu sein. In der Steuerverwaltung existiert nach wie vor die Auffassung, mit dem Steuergeheimnis in § 30 Abgabenordnung (AO) seien alle Vorkehrungen für den Datenschutz erschöpfend vorhanden.

Es trifft zwar zu, daß die Regelungen in § 30 AO, die zum Teil auch im Straftatbestand des § 355 StGB enthalten sind, nicht nur das unbefugte Offenbaren oder Verwerten der Angaben der Auskunftspflichtigen ausschließen und auch die besonderen Gefährdungen, denen diese Angaben unter den Bedingungen der automatisierten Datenverarbeitung ausgesetzt sind, berücksichtigen (vgl. § 30 Abs. 2 Nr. 3, Abs. 4 AO). Doch zeigen die Probleme in der Praxis, daß es insbesondere vor dem Hintergrund der zunehmenden Automation normenklarer **bereichspezifischer Datenschutzregelungen** bedarf, um die immer wieder auftretenden Schwierigkeiten zu beseitigen. Dies betrifft beispielsweise sowohl die beabsichtigte Einführung der automatisierten Besteuerungsverfahren, die einen bundesweiten Abruf von Steuerdaten innerhalb der Finanzverwaltung ermöglichen sollen, als auch die zentral geführte - möglicherweise auch zu automatisierende - Steuerfahndungsdatei.

Das Finanzministerium des Landes Nordrhein-Westfalen hält die Rahmenregelungen für ein automatisiertes Steuerdatenabruf-Verfahren in § 30 Abs. 6 AO für ausreichend. Es will sich deshalb mit einer Verwaltungsregelung begnügen. Demgegenüber bleibt es bei der datenschutzrechtlichen Forderung, daß automatisierte Abrufverfahren, in denen Steuerdaten von der speichernden Stelle zum Abruf bereitgestellt werden, ohne daß diese prüfen kann, ob der Abruf berechtigt erfolgt ist, einer präzisen gesetzlichen Regelung bedürfen. Denn durch ein bundesweites Automationsvorhaben mit Online-Abrufen von Steuerdaten wird bereits in besonderer Weise in das Grundrecht der Steuerpflichtigen auf informationelle Selbstbestimmung eingegriffen.

14.1 Probleme kommunaler Vollstreckungsmaßnahmen

Streitig ist, ob Vollstreckungsbeamtinnen und -beamte alle aus den unterschiedlichsten Gründen bei der Stadtkasse gesammelten Daten über die Bankverbindungen von Bürgerinnen und Bürgern zur Kenntnis erhalten

und nutzen dürfen, und auch, ob sie jede Schuldnerin oder jeden Schuldner öffentlich anprangern dürfen, indem das Auto mit Hilfe einer Parkkralle stillgelegt und für jedermann deutlich sichtbar ein Pfandsiegel angebracht wird.

Vollstreckungsbeamtinnen und -beamte einer Stadt sind in aller Regel der Stadtkasse zugeordnet und halten es daher für selbstverständlich, die dort vorhandenen Kenntnisse auch für ihre Aufgabenerfüllung zu nutzen, wie beispielsweise die Bankverbindungen von Bürgerinnen und Bürgern. Dem wäre datenschutzrechtlich nicht viel entgegenzusetzen, wenn nicht die Bankverbindung zu einem ganz anderen Zweck bei der Stadtkasse gespeichert worden wäre. Die Nutzung auch zum Zwecke der Vollstreckung ist nur gerechtfertigt, wenn die **Zweckänderung** rechtlich zugelassen ist. Im Vollstreckungsgesetz steht hierzu nichts; es fehlt eine der Vollstreckung im Steuerrecht vergleichbare Regelung, nach der zur Vorbereitung der Vollstreckung die Vermögens- und Einkommensverhältnisse der Vollstreckungsschuldnerinnen und -schuldner ermittelt und aus Steuerverfahren bekanntgewordene Daten auch für die Vollstreckung wegen anderer Geldleistungen verwendet werden dürfen (vgl. § 249 Abs. 2 AO). Eine solche Nutzung ist nach dem Landesdatenschutzgesetz ebenfalls nicht erlaubt, weil sie in der Aufzählung der ausnahmsweise zulässigen Zweckänderungen des § 13 Abs. 2 DSG NW nicht enthalten ist.

Ein bundesweites Medienecho rief die Praxis einiger nordrhein-westfälischer Städte hervor, die sich zur **Eintreibung ausstehender Geldforderungen** der Methode bedienten, die auf öffentlichen Straßen und Plätzen geparkten Kraftfahrzeuge der jeweiligen Schuldnerinnen und Schuldner mit einer **Parkkralle** stillzulegen und daran gut sichtbar außen ein **Pfandsiegel** anzubringen. Durch diese Art und Weise der Vollstreckung wird der Öffentlichkeit bekannt, daß die Stadt gegen die Halterin oder den Halter des Kraftfahrzeuges vollstreckt.

Dagegen bestehen datenschutzrechtliche Bedenken, weil nach dem Vollstrekkungsgesetz eine derartige öffentliche Bekanntgabe **weder erforderlich noch verhältnismäßig** ist. Zum einen ist das Anbringen des Pfandsiegels **außen** am Fahrzeug in der Regel nicht notwendig; es soll nur dann angebracht werden, wenn das Fahrzeug im Gewahrsam des Schuldners verbleibt. Durch das Anlegen der Parkkralle ist das Fahrzeug stillgelegt, der Gewahrsam der Schuldnerin oder des Schuldners also gebrochen. Zum anderen bewirkt das Anbringen des Pfandsiegels außen am Fahrzeug die öffentliche Bekanntgabe der Pfändung. Dies ist unverhältnismäßig, weil neben der an sich schon wirkungsvollen Stillegung des Fahrzeuges außerdem noch eine Prangerwirkung erzielt wird.

14.2 Privatisierungstendenzen in der kommunalen Steuerverwaltung

Tatsächliche - oder manchmal auch nur vermeintliche - Kosteneinsparung führt zunehmend zur Verlagerung von Aufgaben der öffentlichen Verwaltung auf private Unternehmen. Problematisch wird dieses Outsourcing zumindest im Bereich hoheitlicher Eingriffsverwaltung, für die die Steuerverwaltung ein klassisches Beispiel ist. Bloße Unterstützungsleistungen, bei denen keine relevanten personenbezogenen Daten zur Kenntnis genommen werden können, sind allerdings datenschutzrechtlich unbedenklich.

So stellte sich im Berichtszeitraum mehrfach die Frage, wie Städte die alljährliche Versendung der **Lohnsteuerkarten** unter Mithilfe privater Unternehmen datenschutzgerecht organisieren können. Keine grundsätzlichen Bedenken bestehen gegen diese Hilfstätigkeit privater Firmen, solange die dort tätigen Personen lediglich Namen und Anschriften der betroffenen Bürgerinnen und Bürger zur Kenntnis nehmen können - etwa wenn die Firma die Lohnsteuerkarten bereits in verschlossenen Umschlägen erhält. Dagegen stellt es eine unbefugte und damit **unzulässige Offenbarung** von Steuerdaten an Privatpersonen dar, wenn alle auf der Lohnsteuerkarte ausgedruckten Steuerdaten, wie Familienstand, Kinder, Konfession und Steuerklasse von den Beschäftigten der privaten Firma gelesen werden können.

Eine Abgabe von Lohnsteuerkarten, die sich noch nicht in den verschlossenen Umschlägen befinden, kann - im Gegensatz zur Auffassung des Finanzministeriums - auch nicht als eine zulässige Datenverarbeitung im Auftrag nach § 11 DSG NW angesehen werden. Die allgemeine Vorschrift über die Datenverarbeitung im Auftrag nach dem Landesdatenschutzgesetz verbietet sich nämlich als Ermächtigung für die Verarbeitung von Daten durch private Stellen, weil schon die Auftragsvergabe unzulässig ist (vgl. Stähler, Datenschutzgesetz Nordrhein-Westfalen, 2. Auflage, Köln 1988, Anmerkung 1 zu § 11). Eine Offenbarung von Steuerdaten, die mit der Auftragsvergabe zwangsläufig verbunden ist, kann nach § 30 Abs. 4 AO nur befugt erfolgen, wenn sie für die Durchführung von Besteuerungsverfahren erforderlich ist. Die Erforderlichkeit ist jedoch nicht gegeben, da die Lohnsteuerkarten eben auch im verschlossenen Umschlag an die Firma gegeben werden können. Auch wenn das dargestellte Problem altbacken oder gar lächerlich erscheinen mag, ist es ein häufiger Gegenstand von Beschwerden.

Ein anderer Fall von Outsourcing weckt Assoziationen an die Volkszählung und den Protest von Bürgerinnen und Bürgern. Mehrere Gemeinden in Nordrhein-Westfalen haben ein **privates Unternehmen** damit beauftragt, alle Haushalte und Betriebe im Gemeindegebiet persönlich aufzusuchen und durch **Befragung** festzustellen, ob dort Hunde gehalten werden. Dabei sollen die Mitarbeiterinnen und Mitarbeiter des privaten Unternehmens an Hand von Listen, die vom kommunalen Steueramt mit Straßenbezeichnung und Hausnummer versehen sind, in den Haushalten die Frage nach der **Hundehaltung** stellen, den **Namen** des Hundehalters und die **Anzahl** der Hunde eintragen. Nach Abschluß der Befragung sollen die ausgefüllten Listen an das Steueramt der jeweiligen Gemeinde zurückgegeben werden.

Datenschutzrechtlich geht es dabei um zwei Fragen: Dürfen die Gemeinden, denen in Nordrhein-Westfalen auf Grund eigenen Satzungsrechtes die Erhebung von Hundesteuern möglich ist, eine flächendeckende Befragung aller Haushalte und Betriebe durchführen, um so den Bestand der im Gemeindegebiet gehaltenen Hunde festzustellen? Dürfen sich die Gemeinden hierzu eines privaten Unternehmens bedienen?

Zunächst könnte von vornherein eine flächendeckende Hundebestandsaufnahme durch Befragung aller Haushalte als unzulässige Steuerfahndung angesehen werden. Für eine Steuerfahndung gäbe es keine Rechtsgrundlage, weil eine nach der Abgabenordnung zugelassene Ermittlung in unbekannten Steuerfällen auf das kommunale Steuerwesen nicht übertragbar ist. Nach der nordrhein-westfälischen Mustersatzung (Runderlaß des Innenministeriums vom 01.10.1970 und vom 04.05.1977, SMBl. NW. 61215), die von den Gemeinden nahezu wörtlich übernommen ist, kann allerdings eine allgemeine Hundebestandsaufnahme durchgeführt werden. § 11 Abs. 4 der Mustersatzung befugt Beauftragte der Gemeinde, Auskünfte über die auf dem Grundstück, im Haushalt oder im Betrieb gehaltenen Hunde einzuholen. Darüber hinaus ist in § 11 Abs. 5 ausdrücklich die Durchführung von **Hundebestandsaufnahmen** geregelt. Allerdings wird darin eine bestimmte Verfahrensweise festgelegt. Danach sind die Grundstückseigentümerinnen und -eigentümer, Haushaltungs- und Betriebsvorstände sowie deren Stellvertretungen zur wahrheitsgemäßen Ausfüllung der ihnen vom Steueramt übersandten Nachweisungen verpflichtet. Dies spricht für die Durchführung nur einer schriftlichen Befragung. Bei dem Ausfüllen der übersandten Nachweise haben die Grundstückseigentümerinnen und -eigentümer, Haushaltungs- und Betriebsvorstände sogar Auskunft über die auf dem Grundstück, im Haushalt oder Betrieb gehaltenen Hunde sowie deren Halterinnen und Halter zu erteilen. Die schriftliche Befragung umfaßt daher auch die Befragung von Dritten über steuerpflichtige Personen und soll flächendeckend durchgeführt werden.

Insoweit fragt sich, ob eine stattdessen mündlich durchgeführte Befragung der Haushalte im Gemeindegebiet nicht eher der datenschutzrechtlichen Grundforderung entspricht, die **Betroffenen unmittelbar selbst zu befragen**. Deshalb bestehen gegen eine solche mündliche Befragung - bis zu einer eindeutigen Regelung in den Gemeindesteuersatzungen - dann keine durchgreifenden Bedenken, wenn die Beantwortung **freiwillig** ist und die angetroffene Person sich auch dafür entscheiden kann, die Frage schriftlich gegenüber dem Steueramt zu beantworten. Bei der Durchführung einer solchen mündlichen Befragung muß außerdem gewährleistet sein, daß minderjährige Kinder, nicht zum Haushalt gehörige Personen - wie Besuch oder Reinigungskräfte - überhaupt nicht und in Betrieben nur Betriebsvorstände oder deren Stellvertretungen befragt werden dürfen.

Offen ist noch, ob die Gemeinden ein **privates Unternehmen** mit der Durchführung einer solchen Befragung beauftragen dürfen. Grundsätzliche Bedenken können dann nicht bestehen, wenn der Gesetzgeber selbst eine Beauftragung privater Unternehmen zugelassen hat, wie dies beispielsweise im Landesabfallgesetz geschehen ist. Ob § 11 Abs. 4 der Mustersatzung, der eine Auskunftspflicht gegenüber den Beauftragten der Gemeinde regelt, auch die Beauftragung privater Personen erfaßt, ist zweifelhaft. Allerdings wird überwiegend die Auffassung vertreten, daß eine Beteiligung Privater an der Erfüllung von Aufgaben der öffentlichen Verwaltung dann unbedenklich ist, wenn sie in der Form der **Verwaltungshilfe**, das heißt mit weisungsabhängiger Hilfstätigkeit ohne eigene Entscheidungsbefugnis tätig werden (vgl. Wolff/Bachof/ Stober, Verwaltungsrecht II, 5. Auflage, München 1987, § 104 Rdnr. 5; Kammergericht Berlin, Beschluß vom 23.10.1996 in NZV 1997, 48 stellt zum rechtmäßigen Einsatz eines "Verwaltungshelfers" entscheidend darauf ab, ob der Hoheitsträger die tatsächliche Sachherrschaft über den Geschehensablauf bei der Überwachung durch private Ermittler behält).

Da die Firmenmitarbeiterinnen und -mitarbeiter keine Befugnisse haben, etwa die Identität der angetroffenen Personen festzustellen oder Grundstücke zu betreten, um nach Gegenständen zu suchen, die auf eine Hundehaltung schließen lassen, sondern sich ohne eigene Entscheidungskompetenz an die ihnen gegebenen Weisungen hinsichtlich ihrer Informationspflichten, des Befragungsumfangs und der sonstigen Umstände der Durchführung zu halten haben, stellt die Befragung eine untergeordnete Hilfstätigkeit bei der Erhebung von Daten dar, die für die Durchführung des Steuerverfahrens erforderlich sind.

Datenschutzrechtlich beanstandungsfrei können private Unternehmen mit der Durchführung von Hundebestandsaufnahmen also nur beauftragt werden,

wenn die Gemeinde mit der Beauftragung eine präzise Beschreibung dessen vornimmt, was und auf welche Weise erfragt werden soll, außerdem bestimmt, daß die Mitarbeiterinnen und Mitarbeiter des beauftragten Unternehmens den Weisungen der Gemeinde unterliegen und zur Verschwiegenheit verpflichtet sind, sowie deren Tätigkeit auch überwacht.

Darüber hinaus sind mindestens folgende Vorgaben festzuschreiben:

- Die Bürgerinnen und Bürger der Gemeinde werden vor Durchführung der Hundebestandsaufnahme in angemessener Weise unterrichtet; auch darüber, wer die Befragung durchführt.
- Die Mitarbeiterinnen und Mitarbeiter erhalten einen Vordruck, in dem lediglich die Straßen und Hausnummern angegeben und allenfalls folgende Felder von ihnen auszufüllen sind: angetroffene Person (Name) bzw. nicht angetroffen, Angabe über Hundehaltung und gegebenenfalls Änderungen. Eine Rubrik "eigene Wahrnehmungen" ist nicht vorzusehen, weil dies als Aufforderung zu einer unzulässigen Ausforschung mißverstanden werden könnte.
- Vor der Befragung müssen sich die Mitarbeiterinnen und Mitarbeiter ausweisen und darauf hinweisen, daß die Beantwortung der gestellten Fragen freiwillig ist.
- Eine Befragung minderjähriger Kinder und nicht zum Haushalt gehörender Personen erfolgt nicht. Die Frage nach der Hundehaltung darf sich nur auf den jeweiligen Haushalt beziehen.
- Nachkontrollen finden nicht statt.
- Eine erneute Hundebestandsaufnahme erfolgt nicht im jährlichen Turnus, sondern erst nach längerem Zeitablauf.

15. Universitäten und Hochschulen

Die Novelle des Universitätsgesetzes hat die Macht der Dekaninnen und Dekane - nicht nur als Vorgesetzte - wachsen lassen, so daß auch in diesem Bereich ein Regelungsbedarf für den Umgang mit den Daten der Studierenden und der Hochschulbeschäftigten entstanden ist. Initiativen zur Durchführung von **Lehrveranstaltungskritik** und Beurteilungen der Lehrenden durch die Studierenden sind bislang bei der Verarbeitung personenbezogener Daten auf die Einwilligung der Betroffenen angewiesen. Sofern die Hochschulverwaltungen solche Beurteilungsaktionen künftig regelmäßig mit dem Ziel der Verbesserung der Lehre durchzuführen beabsichtigen, wären hierfür ebenfalls gesetzliche Regelungen zu treffen.

Die Unsitte, Leistungsergebnisse von Studierenden, deren Prüfungszulassungen und die Prüfungsergebnisse durch Aushänge in der Hochschule mit dem Namen und der Matrikelnummer bekanntzugeben, lebt leider immer noch weiter, obwohl es sich eindeutig um eine unzulässige personenbezogene Bekanntgabe handelt. Es gibt bereits Anfragen, ob Prüfungsergebnisse - wenn auch nur mit der Matrikelnummer - in das Internet eingestellt werden dürfen oder die Anmeldung zu Seminaren darüber abgewickelt werden kann. Ohne die vorherige **Information** der Betroffenen über die mit dem **Internet** verbundenen **Datenschutz- und Datensicherheitsrisiken** und ohne die vorherige ausdrückliche **Einwilligung** der Betroffenen können personenbezogene Daten allerdings nicht in das Internet eingegeben werden.

Der jüngst erfolgte Anschluß aller nordrhein-westfälischen Hochschulen an das Deutsche Breitband-Wissenschaftsnetz verbessert die bisherigen Verbindungskapazitäten um ein Vielfaches. Die neuen Bandbreiten ermöglichen multimediale Funktionen und fördern die verstärkte Nutzung von Internet-Zugängen durch Studierende. So soll in einigen Universitäten neu immatrikulierten Studierenden eine Internet-Zugangskennung angeboten werden, mit der sie über die Universitäts-Rechenzentren in das Netz gelangen können. Nach den bisher vorliegenden Informationen sollen dabei die Diensteanbieter zwar nur die Kennung des Universitätsservers erfassen, aber die Netznutzung selbst wird mit der persönlichen Benutzerkennung (User-ID) im Rechenzentrum der Universität protokolliert. Diese Protokolldaten dürfen unter Datenschutzgesichtspunkten kurzfristig aufbewahrt, aber keinesfalls zu Verhaltensprofilen zusammengestellt werden.

15.1 Chipkarten für Studierende

Bequeme Welt oder gläserne Studierende?

Die an einer Universität in der Erprobung befindliche UniversCard soll multifunktional Studierendenausweis und Nahverkehrsticket sein, zur Vereinfachung des Immatrikulations- und Rückmeldeverfahrens dienen, den Ausweis zur Identifikation bei allen benutzerrelevanten Vorgängen in der Bibliothek darstellen, eine elektronische Geldbörse zur Bezahlung in der Mensa und den Cafeterien enthalten sowie Anmeldungen zu Seminaren, Übungen und Prüfungen ermöglichen. Ob die damit verbundenen Erleichterungen im Alltag die **datenschutzrechtlichen Risiken** überwiegen, kann mit guten Gründen bezweifelt werden. Sofern nach Abschluß der Erprobungsphase beabsichtigt werden sollte, allen Studierenden solche Karten zugänglich zu machen, bedarf es angesichts der damit entstehenden Datenmengen unterschiedlichster Art einer gesetzlichen Regelung, die datenschutzrechtlichen Anforderungen genügt und denjenigen Studierenden, die lieber auf eine solche Karte **verzichten** möchten, auch diese Möglichkeit beläßt. Dabei muß sichergestellt werden, daß der Kartenverzicht nicht mit Benachteiligungen verbunden ist.

Eine gesetzliche Regelung muß mindestens folgende Festlegungen treffen:

- Den Studierenden ist ein Wahlrecht einzuräumen; sie müssen ohne Benachteiligung auf die Chipkarte insgesamt oder auf einzelne Funktionen verzichten können.
- Die von der Chipkarte umfaßten Funktionen müssen abschließend festgelegt sein.
- Bestimmt werden muß, wer verarbeitende Stelle und verantwortlich für Speicherung, Veränderung und Löschung der Daten auf der Chipkarte sein soll.
- Festzulegen ist, wer auf die Daten lesend zugreifen und Daten aus der Chipkarte für eigene Zwecke speichern und nutzen können soll; die jeweiligen Zwecke müssen im einzelnen bestimmt werden.
- Die Studierenden müssen die Möglichkeit haben, die auf der Chipkarte gespeicherten Daten an dafür bereitgestellten Lesegeräten kostenlos und jederzeit überprüfen zu können.
- Es sind Regelungen über die technischen und organisatorischen Maßnahmen zu treffen, mit denen die datenschutzgerechte Datenverarbeitung gewährleistet wird. Vor allem betrifft dies die fälschungssichere Authentifizierung der Karteninhaberin oder des Karteninhabers, die Steuerung der

Zugriffs- und Nutzungsberechtigung sowie die Vertraulichkeit und Integrität der gespeicherten Daten.

- Die Erstellung von Nutzungsprofilen ist zu verbieten.
- Aufzunehmen sind Vorschriften zum Schutz gegen mißbräuchliche Verwendung der Daten durch Dritte bei Verlust der Chipkarte.

Die gesetzliche Festlegung der Bedingungen für die Datenverarbeitung mit der UniversCard bedeutet natürlich keinen absoluten Schutz vor Mißbrauch der gewonnenen Daten oder auch nur vor Versehen bei der Datenverarbeitung. Wer sich freiwillig für den Kartengebrauch mit allen oder auch nur einigen Funktionsmöglichkeiten entscheiden möchte, muß - um eine wirksame Einwilligungserklärung abgeben zu können - vorher umfassend unterrichtet sein über Art, Umfang und Zweck der mit der UniversCard möglichen Datenverarbeitung und die beteiligten Stellen. Je **komplexer** die Chipkarte gestaltet ist, desto **unüberschaubarer** wird die damit erfolgende Datenverarbeitung. Problematisch sind insbesondere alle Online-Nutzungen, eine größere Zahl unterschiedlicher lese- und schreibberechtigter Stellen sowie umfangreiche Datensätze. Wird nicht bei jeder Nutzung für die Betroffenen erkennbar, welche Daten an einer Stelle gespeichert und eventuell weitergegeben sowie welche Daten neu auf der Chipkarte gespeichert werden, sind erteilte Einwilligungen unwirksam; die Datenverarbeitung ist dann unzulässig.

Nach Abschluß des Modellversuchs ist zu prüfen, ob die UniversCard mit welchen Funktionen und welchen Zugriffsberechtigungen auf freiwilliger Basis überhaupt eingeführt werden soll. Dem Sicherungskonzept muß besondere Aufmerksamkeit gewidmet werden (vgl. 2.1.5).

15.2 Videoeinsatz in der Psychiatrie

Im Zentrum für Psychiatrie einer Universität werden Patientengespräche mit Mikrofonen und Videokameras aufgezeichnet. Soweit die Aufzeichnung im Rahmen einer therapeutischen Behandlung vorgenommen wird, ist sie im Behandlungsvertrag zu vereinbaren. Werden allerdings bereits vor Abschluß des Behandlungsvertrags Vorgespräche mit Ton und Bild aufgezeichnet, muß hierzu in jedem Falle die Einwilligung der Patientin oder des Patienten eingeholt werden. Vor Ort mußte festgestellt werden, daß die verwendeten Informationsblätter und Einwilligungserklärungen unzureichend sind, insbesondere erweckte der Text der Einverständniserklärung den Eindruck, daß die sensiblen Patientendaten anonymisiert gespeichert würden. Zu berücksichtigen ist:

- Zur Aufzeichnung von Ton und Bild bedarf es keiner Einwilligung, wenn der Behandlungsvertrag die Aufzeichnung als vertragsgemäße Dokumentation und Nutzung umfaßt.
- Soweit die Aufzeichnung außerhab der Behandlung auch für eine wissenschaftliche Auswertung oder zu Lehrzwecken für die Ausbildung von Studierenden genutzt werden soll, ist dafür die Einwilligung der Patientin oder des Patienten einzuholen.
- Auch wenn Patientendaten statt mit Namen nur mit einer Nummer gespeichert werden, sind die Daten nicht anonymisiert, sondern personenbezogen gespeichert, solange über die Nummer ein Personenbezug - etwa über eine Namensliste - herstellbar ist. Da außerdem Unterlagen zur Dokumentation der Behandlung aufbewahrt werden müssen, ist auch über eine Zusammenführung der Daten aus den Unterlagen mit denen aus der Aufzeichnung eine Deanonymisierung möglich.
- Eine Einwilligung kann nur dann wirksam sein, wenn sie nach umfassender Information und auf der Grundlage der Freiwilligkeit erklärt worden ist. Soll sich die Einwilligung auf mehrere Verwendungsmöglichkeiten beziehen, muß den Patientinnen und Patienten die Möglichkeit gegeben werden, sich auch nur für einzelne Verwendungen zu entscheiden. Schließlich muß darauf hingewiesen werden, daß die Einwilligung jederzeit widerrufbar ist. In einem solchen Falle muß die gespeicherte Aufzeichnung gelöscht werden.

16. Schule und Weiterbildung

Mit dem Projekt "NRW-Schulen ans Netz - Verständigung weltweit" hält ein neues Medium Einzug in die Schulen. Der Anschluß ans Internet zu Unterrichtszwecken ist aber nur dann uneingeschränkt zu begrüßen, wenn von den Schulen sichergestellt wird, daß die Schülerinnen und Schüler möglichst keine personenbezogenen **Datenspuren** hinterlassen und die Gefahren, denen das Recht auf informationelle Selbstbestimmung bei der Netznutzung ausgesetzt ist, sowie der Datenschutz Gegenstand des Unterrichts sind.

Im Berichtszeitraum sind zwei Verordnungen ergangen, die die Datenverarbeitung im Schulbereich betreffen und dem Datenschutz sehr weitgehend Rechnung tragen. An beiden Verordnungen hat meine Dienststelle intensiv beratend mitgewirkt. Die Verordnung über die zur Verarbeitung zugelassenen Daten von **Schülerinnen, Schülern und Erziehungsberechtigten** (VO-DV I) vom 24.03.1995 (GV. NW. S. 356) regelt die automatisierte Datenverarbeitung und schreibt beispielsweise die Trennung der zum Unterricht genutzten ADV-Anlage vom Verwaltungscomputer vor (§ 2 Abs. 1 VO-DV I). Ebenso ist eine Genehmigungspflicht für die Verarbeitung von Schülerinnen- und Schülerdaten auf privaten PCs der Lehrkräfte am heimischen Schreibtisch festgelegt (§ 2 Abs. 2 VO-DV I).

Die Verordnung über die zur Verarbeitung zugelassenen Daten der **Lehrerinnen und Lehrer** (VO-DV II) vom 22.07.1996 (GV. NW. S. 310) regelt zusammen mit § 19 a Schulverwaltungsgesetz die Verarbeitung der Daten der Lehrkräfte abschließend, so daß die bisher geltende Regelung zur Personaldatenverarbeitung in § 29 DSG NW verdrängt wird. Allerdings gelten die Vorschriften über die Personalaktenführung nach dem Landesbeamtengesetz zusätzlich. Die Verordnung läßt auch bis auf wenige in ihr bezeichnete Ausnahmen eine automatisierte Verarbeitung der Daten zu. Sie unterscheidet im wesentlichen zwischen der Datenverarbeitung in der Schule und der in den Schulaufsichtsbehörden und beschreibt die wesentlichen Datenflüsse zwischen beiden Ebenen.

Das immer wieder auftauchende Problem der Führung von - datenschutzrechtlich unzulässigen - **Zensuren- und Krankenstatistiken** durch manche Schulleitungen erledigt sich nunmehr hoffentlich endgültig. Derartige Statistiken läßt die Verordnung bei der abschließenden Aufzählung des zulässigen Datenbestands in der Schule nämlich nicht zu (Anlage 1 zu § 5 Abs. 1 VO-DV II). Die dort genannte Übersicht der an der Schule Beschäftigten erstreckt sich weder auf eine allgemeine Zensurenstatistik noch auf eine Krankenstatistik. Von der Unzulässigkeit solcher generellen Statistiken unberührt bleibt

allerdings die Möglichkeit der Schulleitung, im Einzelfall anzuordnen, daß die Benotung durch eine bestimmte Lehrkraft über eine bestimmte Zeitdauer erfaßt und ausgewertet werden soll, wenn dies aus gegebener Veranlassung erforderlich ist.

Im Weiterbildungsbereich wurde mehrfach der Umgang von **Volkshochschulen** mit den Anmeldedaten der Kursteilnehmerinnen und Kursteilnehmer thematisiert. Hier ist festzuhalten, daß die Anmeldedaten die Öffentlichkeit nichts angehen und im wesentlichen nur für interne Verwaltungszwecke der Volkshochschulen genutzt werden können. Eine über die rechtmäßige Aufgabenerfüllung der Volkshochschulen hinausgehende Datenverarbeitung ist nur mit der Einwilligung der Betroffenen zulässig.

16.1 Schule und Jugendamt

Hält eine Schule wegen der Verhaltensauffälligkeiten einer Schülerin oder eines Schülers die Einschaltung des Jugendamtes für geboten, so darf sie dem Jugendamt nicht gleich ihr gesamtes Wissen über das Verhalten und die Persönlichkeit des Kindes sowie über seine Erziehung und sein Elternhaus offenbaren.

In solchen Fällen besteht die Wahrnehmung der Jugendhilfe in erster Linie darin, beratend an die Erziehungsberechtigten heranzutreten und durch fachlich geschulte Sozialarbeiterinnen und Sozialarbeiter Angebote zur Hilfestellung zu unterbreiten. Die dafür notwendigen **Daten** müssen grundsätzlich **bei den Betroffenen** unmittelbar erhoben werden (§ 62 Abs. 2 SGB VIII). Deshalb muß es zunächst genügen, dem Jugendamt nur die erforderliche Information zu übermitteln, die es in die Lage versetzt, einen Bedarf für Jugendhilfe festzustellen. Das Jugendamt selbst hat hierzu ausgeführt, daß ein genereller Hinweis der Schule über das Bestehen einer Problemlage bei dem betreffenden Schüler zunächst ausgereicht hätte. Erst wenn die Betroffenen ihre Mitwirkung verweigern, die Kenntnis näherer Angaben aber für die Erbringung bestimmter Jugendhilfeleistungen erforderlich ist, kann das Jugendamt diese Daten bei der Schule erheben (§ 62 Abs. 3 SGB VIII).

Zusätzlich wurde der Schulaufsichtsbehörde empfohlen, in Dienstbesprechungen mit den Schulleitungen darauf hinzuwirken, daß in solchen Fällen dem Jugendamt nur diejenigen Daten übermittelt werden, die das Bestehen einer Problemlage bei einer Schülerin oder einem Schüler aufzeigen, und erst auf Nachfrage des Jugendamtes notwendige weitere Auskünfte zu erteilen.

16.2 Datensammlung für Schulfahrten

Die zur Vorbereitung von Schulfahrten zu erhebenden Datenbestände dürfen nicht ausufern.

Verbunden mit der elterlichen Einverständniserklärung zur Teilnahme des Kindes an einer mehrtägigen Schulwanderung wurden an einer Schule eine Reihe von personenbezogenen Daten abgefragt, insbesondere medizinische Daten des Kindes, bestehende Kranken- und Haftpflichtversicherung der Erziehungsberechtigten, der Name der Versicherung, der Arbeitgeber der hauptversicherten Person sowie Anschrift und Telefonnummer der Erziehungsberechtigten. Wenn auch die Befragung erkennbar dazu dienen sollte, rechtzeitig Hinweise auf gesundheitliche Risiken bei den teilnehmenden Schülerinnen und Schülern zu erhalten, sind gleichwohl nicht alle erfragten Angaben zu diesem Zweck erforderlich, wie zum Beispiel die Frage nach dem Arbeitgeber.

Vordrucke zur Erhebung personenbezogener Daten sind vor ihrer Verwendung auf die datenschutzrechtliche Zulässigkeit ihres Inhalts zu überprüfen.

16.3 Fehlzeiten auf Bewerbungszeugnissen

Schülerinnen und Schüler der 9. Klasse einer Realschule fragen sich stellvertretend für viele andere, die sich bewerben wollen, was geht es meinen zukünftigen Arbeitgeber an, wie oft ich in der Schule gefehlt habe?

Nach den Vorgaben des Ministeriums für Schule und Weiterbildung des Landes Nordrhein-Westfalen ist bei Zeugnissen der Klassen 9 und 10 jeweils für das 1. Halbjahr der Realschule anzugeben: "Versäumte Stunden, davon unentschuldigt." Dagegen ist die Angabe von Fehlzeiten bei Überweisungs-, Abgangs- und Abschlußzeugnissen nicht vorgesehen. Dies entspricht auch den **Anforderungen des Datenschutzes**. Die derzeitige Regelung läßt jedoch zum Nachteil der Schülerinnen und Schüler außer acht, daß Halbjahreszeugnisse vor dem eigentlichen Abschluß der Schullaufbahn ausgestellt und als sogenannte Bewerbungszeugnisse verwendet werden. Für die Bewerbungszeugnisse hat aus datenschutzrechtlichen Gründen wie für die Abgangszeugnisse zu gelten, daß Fehlzeiten darin nicht aufzunehmen sind. Diese Überlegungen gelten selbstverständlich auch für die Sekundarstufen I und II in anderen Schulformen. Dem Ministerium für Schule und Weiterbildung sind die bestehenden datenschutzrechtlichen Bedenken mit der Empfehlung mitgeteilt worden, die einschlägigen Verwaltungsvorschriften entsprechend zu überarbeiten.

Unabhängig von einer ministeriellen Regelung sollte jede Schulleitung bereits jetzt denjenigen Schülerinnen und Schülern, die sich bewerben wollen, ein Zeugnis ohne Angabe der Fehlstunden ausstellen.

16.4 Schulmitwirkung

Datenflüsse zwischen den Mitwirkungsberechtigten

Grundsätzlich gilt, daß die Mitwirkungsberechtigten im Rahmen ihrer Beteiligung an den Aufgaben der Schule, insbesondere ihrer Teilnahme an der Bildungs- und Erziehungsarbeit der Schule, auch personenbezogene Daten von Schülerinnen und Schülern, Erziehungsberechtigten sowie von Lehrkräften zur Kenntnis erhalten, speichern und weitergeben dürfen. Da diese Datenverarbeitung der Schule zuzurechnen ist, trägt die Schulleitung insoweit die Verantwortung für die Einhaltung der Datenschutzvorschriften durch die Mitwirkungsorgane.

Welche Informationen mit personenbezogenen Daten den Klassen- und Schulpflegschaften weitergegeben werden dürfen und welche Beratungen untereinander einen Informationsaustausch erlauben, bestimmt sich nach der **Aufgabenstellung** des jeweiligen **Mitwirkungsorgans**. Die im Schulmitwirkungsgesetz vorgesehene Beteiligung setzt Informations-, Anhörungs- und Beratungsrechte voraus. Soweit beispielsweise die Schulpflegschaft Interessen der Erziehungsberechtigten bei der Gestaltung der Bildungs- und Erziehungsarbeit der Schule vertritt und Angelegenheiten berät, wie sie in § 5 Abs. 1 und 2 Schulmitwirkungsgesetz (SchMG) aufgezählt sind, steht einem Umgang mit personenbezogenen Daten nichts entgegen, wenn die Kenntnis solcher Daten für die Aufgabenwahrnehmung unbedingt erforderlich ist. Dies im Einzelfall zu beurteilen, ist nicht immer einfach. Was schiefgehen kann, zeigt das folgende Beispiel:

Eine Schulpflegschaftsvorsitzende hatte sich aktiv in eine Auseinandersetzung zwischen Erziehungsberechtigten und der Schulleitung sowie den betroffenen Lehrkräften eingeschaltet, die zunächst nur auf der Ebene der Klassenpflegschaft ausgetragen worden war. Die Schulpflegschaftsvorsitzende ist mit den ihr - entgegen § 18 Abs. 9 SchMG - zugetragenen Angaben über den Schüler und dessen Erziehungsberechtigte in die Schulpflegschaftsversammlung gegangen, ohne daß die Beratung der Angelegenheit den Aufgaben der Schulpflegschaft nach § 5 Abs. 2 SchMG entsprochen hätte. Sie hat darüber hinaus in der Schulpflegschaftsversammlung Ordnungsmaßnahmen gegen den Schüler erörtern lassen, deren Beratung ausschließlich Aufgabe der Lehrerkonferenz (§ 15 Allgemeine Schulordnung, § 6 Abs. 4 Nr. 7 SchMG) gewesen wäre.

Wenn es um Beratungen in Angelegenheiten geht, die einzelne Lehrkräfte, Erziehungsberechtigte, Schülerinnen oder Schüler persönlich betreffen, besteht die Verpflichtung von Mitgliedern der Schulmitwirkungsorgane zur Verschwiegenheit auch gegenüber Mitgliedern der anderen Mitwirkungsorgane. Überdies darf in diesen Angelegenheiten auch die Schulöffentlichkeit nicht hergestellt werden (§ 18 Abs. 4 und 9 SchMG).

17. Öffentlicher Dienst

Kaum eine Verwaltungseinheit weiß so viel über einzelne Personen wie die Personalstelle. Der Umgang mit Beschäftigtendaten ist trotz der erweiterten bereichspezifischen gesetzlichen Regelungen immer noch verbesserungsbedürftig - nicht nur im öffentlichen Dienst. Im Berichtszeitraum haben unter anderem folgende Themen eine Rolle gespielt: Neuregelung der amtsärztlichen Untersuchungen, Organisationsuntersuchungen durch Beratungsunternehmen, Datenschutz bei Personalvertretungen, Datenerhebungen im Übermaß bei polizeiärztlichen Einstellungsuntersuchungen. Zunehmende Bedeutung gewinnt bei der Modernisierung der Verwaltung das Personalkosten-Controlling. Gegen eine **dezentrale Ressourcenverantwortung** bestehen grundsätzlich keine datenschutzrechtlichen Bedenken, wenn der Grundsatz beachtet wird, daß der Kreis der mit Personalaktendaten befaßten Beschäftigten aus Gründen der Fürsorgepflicht des Dienstherrn möglichst eng zu halten ist. Allerdings dürfen die Fachvorgesetzten die Personalkosten nur ohne die Beihilfeaufwendungen für die Beschäftigten planen. Diese Daten unterliegen einer besonderen Zweckbindung (§ 102 a Satz 4 LBG) und dürfen anderen als mit der Beihilfebearbeitung betrauten Beschäftigten nicht zur Kenntnis gelangen.

Für die im 12. Tätigkeitsbericht (S. 87 f.) ausführlich behandelte Problematik, die nach § 102 a Satz 3 LBG gebotene **Abschottung der Beihilfebearbeitung** von der Personalverwaltung auch in kleineren Gemeinden zu gewährleisten, wird es künftig eine **zufriedenstellende Lösungsmöglichkeit** geben. Durch das Erste Gesetz zur Änderung des Gesetzes über die kommunalen Versorgungskassen und Zusatzversorgungskassen im Lande Nordrhein-Westfalen vom 18.12.1996 (GV. NW. 1996 S. 567) wurde den Kommunen der Weg eröffnet, die **Bearbeitung der Beihilfeanträge** ihrer Beschäftigten den **Versorgungskassen** zu übertragen. Es bedarf allerdings noch einer entsprechenden Änderung der Zuständigkeitsregelung in der Beihilfenverordnung. Mit der gesetzlichen Neuregelung kann dem Wunsch zahlreicher Gemeinden nach Kosteneinsparung Rechnung getragen und zugleich sichergestellt werden, daß dem gesetzlichen Abschottungsgebot genügt wird. Demgegenüber ist die **Übertragung** der Beihilfebearbeitung auf ein **privates Versicherungsunternehmen** nach wie vor datenschutzrechtlich **unzulässig**. Ein solches Vorgehen einer Gemeinde mußte im Dezember 1995 förmlich beanstandet werden. Die Übermittlung sensibler Gesundheitsdaten von Beschäftigten an eine nichtöffentliche Stelle ist ohne bereichspezifische gesetzliche Grundlage unzulässig. Das Innenministerium teilt diese Rechtsauffassung und hat die Bezirksregierungen, Kreise und kreisfreien Städte mit **Erlaß** vom 22.01.1996 - III A 4 - 37.45.10 - 3/96 - davon unterrichtet sowie darum gebeten, eventuell bereits abgeschlossene Verträge mit Versicherungen zum nächstmöglichen Zeitpunkt

zu kündigen. Das **VG Aachen** hat jüngst zudem in einem einstweiligen Rechtsschutzverfahren einer Gemeinde die Weitergabe von Beihilfeakten zur Bearbeitung durch ein Privatunternehmen **vorläufig untersagt**.

Durch die in der **Verordnung über amtsärztliche Untersuchungen** für den öffentlichen Dienst (GDSG-VO) vom 31. 07. 1996 (GV. NW. S. 296) getroffenen Regelungen verfügen die Gesundheitsämter nunmehr über klare Vorgaben bei Erstellung amtsärztlicher **Gesundheitszeugnisse** über Bedienstete oder Bewerberinnen und Bewerber für eine Tätigkeit im öffentlichen Dienst. Zu begrüßen ist, daß das Ministerium für Arbeit, Gesundheit und Soziales meinen zu dem Verordnungsentwurf geäußerten Bedenken und Anregungen im wesentlichen gefolgt ist. So wurde insbesondere auf unter persönlichkeitsrechtlichen Gesichtspunkten bedenkliche, den Rahmen einer amtsärztlichen Untersuchung überschreitende Erhebungen von Gesundheitsdaten Betroffener und Dritter verzichtet. Auch sind die der GDSG-VO beigefügten Formblätter nunmehr datenschutzfreundlich gestaltet und mit den notwendigen Bearbeitungshinweisen versehen. Allerdings bleibt zu bemängeln, daß bei jeder amtsärztlichen Begutachtung im Rahmen von Zurruhesetzungsverfahren von Beamtinnen und Beamten wegen Dienstunfähigkeit ungeachtet der gesetzlichen, auf die Erforderlichkeit im Einzelfall abstellenden Regelung (§ 24 Abs. 3 Satz 2 GDSG NW) die pauschale Angabe der **Diagnose** und deren Übermittlung an die die Untersuchung veranlassende Stelle vorgesehen ist.

Verschiedene Anfragen zu datenschutzrechtlichen Erfordernissen bei der Gesprächsdatenerfassung und -auswertung dienstlicher und privater Telefonate zeigen, daß die bei **Telefonkostenabrechnungen** zu beachtenden Vorschriften und Verfahrensregeln nicht überall hinreichend bekannt sind. Der die Dienstanschlußvorschriften betreffende Runderlaß des Finanzministeriums vom 22. 9. 1986 (MBl. NW. 1986, S. 1538), der sich zur Zeit in der Überarbeitung befindet, ist im 8. Tätigkeitsbericht ausführlich (S. 82 bis 84) behandelt worden. Nach wie vor gilt, daß bei privaten Telefonaten von Beschäftigten sowie bei dienstlichen Telefongesprächen in sensiblen Bereichen die **beiden letzten Ziffern** der Telefonnummern der Angerufenen auf der Telefonkostenabrechnung **nicht ausgewiesen** werden dürfen.

17.1 Datenschutz bei Bewerbungen

Seit Jahren wurde bei hausinternen sowie den nachgeordneten Bereich betreffenden Stellenausschreibungen eines Ministeriums darauf hingewiesen, daß **Bewerbungen** "auf dem Dienstweg", also **über die Vorgesetzten**, an das Personalreferat zu richten seien. Diese Verfahrensweise läßt sich auf keine gesetzliche Grundlage stützen. **Bei Bewerbungen gibt es keinen Dienstweg**.

Dieser ist nach § 179 LBG nur für Anträge und Beschwerden vorgeschrieben, ansonsten ist der Kreis der mit Personalakten und Personalaktendaten befaßten Beschäftigten möglichst eng zu halten. Nach Erörterung der Problematik mit dem Ministerium wird die Vorlage von Bewerbungen in dieser Form künftig nicht mehr verlangt.

Die Praxis, **vor dem Vorstellungsgespräch Personalbögen** ausfüllen zu lassen, begegnet erheblichen datenschutzrechtlichen Bedenken. Der Personalbogen ist, worauf bereits im 10. Tätigkeitsbericht (S. 95/96) hingewiesen wurde, als Vorblatt Bestandteil der Personalakte. Erst **nach** der getroffenen Personalauswahlentscheidung werden in ihm die für das Dienst- oder Arbeitsverhältnis erforderlichen Personalaktendaten gespeichert. Demnach ist die Erhebung und Speicherung personenbezogener Daten von Bewerberinnen und Bewerbern, deren **Einstellung noch nicht feststeht**, auf einem Personalbogen nicht erforderlich. Sie entspricht nicht dem Verhältnismäßigkeitsgrundsatz und ist damit **datenschutzrechtlich unzulässig**. Die auf diese Problematik hingewiesene Dienststelle hat mitgeteilt, daß Personalbögen künftig erst dann ausgefüllt werden, wenn die Einstellung der Bewerberin oder des Bewerbers definitiv feststeht.

Anläßlich **polizeiärztlicher Einstellungsuntersuchungen** haben sich Bewerberinnen und Bewerber umfangreichen Untersuchungen durch Polizeiärztinnen und Polizeiärzte zu unterziehen. Hierbei wird eine Vielzahl von teilweise intimen Gesundheitsdaten nicht nur über sie, sondern auch über Angehörige erfragt. Das Ausmaß der Untersuchungen ist in der bundesweit geltenden Polizeidienstvorschrift "Ärztliche Beurteilung der Polizeidiensttauglichkeit und der Polizeidienstfähigkeit" (PDV 300) festgelegt. Gegen einige der in dieser Verwaltungsvorschrift vorgesehenen Untersuchungsmaßnahmen habe ich **datenschutzrechtliche Bedenken**, so beispielsweise gegen überschießende Datenerhebungen und -weitergaben, gegen die unzureichende Formulierung der Einverständniserklärung und gegen Inhalt wie Form der im nordrhein-westfälischen Formularvordruck enthaltenen Frage nach dem Bestehen einer Schwangerschaft. Die Beauftragten für den Datenschutz streben an, gemeinsam für Nachbesserung zu sorgen.

17.2 Organisationsuntersuchungen durch Beratungsunternehmen

Im Berichtszeitraum führten private Beratungsunternehmen bei verschiedenen öffentlichen Stellen Organisationsuntersuchungen durch, um deren Aufgabenbereiche einer kritischen Überprüfung zu unterziehen. Trotz der Vielzahl der abgeschlossenen und zum Teil noch andauernden Untersu-

chungen gab es erfreulicherweise bislang nur vereinzelt Anlaß für datenschutzrechtliche Kritik.

Was aus datenschutzrechtlicher Sicht bei der Durchführung einer Organisationsuntersuchung durch ein privates Beratungsunternehmen und auch damit gegebenenfalls verbundener Mitarbeiterbefragungen zu beachten ist, soll im folgenden kurz dargestellt werden: Die Verarbeitung von Beschäftigtendaten durch das Beratungsunternehmen unterliegt **denselben Anforderungen** wie die Datenverarbeitung durch die öffentliche Stelle selbst. Hierzu sollte die Einhaltung der datenschutzrechtlichen Erfordernisse **vertraglich** im einzelnen **vereinbart** werden.

- Organisationsuntersuchungen bedürfen klarer, für den Auftragnehmer verbindlicher vertraglicher **Festlegungen**, inwieweit und unter welchen eindeutig zu bestimmenden Voraussetzungen im Rahmen der Organisationsuntersuchung die **Verarbeitung von Beschäftigtendaten** in Betracht kommt. Sollen Mitarbeiterbefragungen durchgeführt werden, sind besondere datenschutzrechtliche Erfordernisse zu beachten und vertraglich festzulegen, so beispielsweise die **Freiwilligkeit** der Teilnahme an derartigen Befragungen.
- Die vertraglichen Regelungen sollen gewährleisten, daß bei jeder Einzeluntersuchung unzulässige Datenerhebungen, -speicherungen und -übermittlungen durch das beauftragte Beratungsunternehmen **vermieden** werden.
- Um die **Einhaltung** der datenschutzrechtlich bedeutsamen vertraglichen Regelungen in der Praxis **zu gewährleisten**, bietet sich zusätzlich die Aufnahme einer Bestimmung in den Vertrag an, nach der die für die Einzeluntersuchungen vorgesehenen Mitarbeiterinnen und Mitarbeiter über die datenschutzrechtlichen Bestimmungen eingehend zu unterrichten und zur strikten Beachtung aller vertraglichen Pflichten anzuhalten sind.

Das Innenministerium hat mitgeteilt, vor dem Abschluß künftiger, seinen Geschäftsbereich betreffender Organisationsuntersuchungsverträge im Rahmen seiner Beteiligung darauf hinzuwirken, daß entsprechende vertragliche Regelungen getroffen werden. Zudem ist auch der Arbeitsstab Aufgabenkritik der Landesregierung über die datenschutzrechtlichen Erfordernisse unterrichtet worden.

17.3 Datenschutz bei Personalvertretungen

Zur Speicherung und Löschung personenbezogener Daten enthält der **Runderlaß** des Innenministeriums zur "Durchführung des Landespersonalvertretungs-

gesetzes" vom 22.03.1996 - MBl. NW. 1996 S. 741 - nunmehr unter anderem folgende Anwendungsgrundsätze:

"Zur Person der oder des Beschäftigten dürfen personenbezogene Daten nicht zusammengefaßt und auf Dauer gespeichert werden. § 65 Abs. 3 Satz 1 bleibt unberührt. Unterlagen mit personenbezogenen Daten, die dem Personalrat aus Anlaß seiner Beteiligung an einer bestimmten Maßnahme zur Verfügung gestellt wurden, sind der Dienststelle nach Abschluß des Beteiligungsverfahrens zurückzugeben bzw. vom Personalrat zu vernichten. Andere Unterlagen des Personalrats, die personenbezogene Daten enthalten, insbesondere Niederschriften und Personallisten, dürfen für die Dauer der regelmäßigen Amtszeit des Personalrats aufbewahrt werden. Sie sind spätestens nach Ablauf einer weiteren Amtsperiode zu vernichten."

Aus der Gesetzesbegründung zu § 65 Abs. 3 LPVG, der seit 1994 eine Änderung des **Akteneinsichtsrechts** enthält, ergibt sich, welche Personaldaten von Mitgliedern des Personalrats auch **ohne Zustimmung** der Beschäftigten eingesehen werden können: Name, Vorname, Geburtsjahr, Hinweis auf Ausbildung (etwa Dipl.-Volkswirt), Eintritt in den Vorbereitungsdienst, Ernennungsdaten, Abteilungs-, Dezernatszugehörigkeit, Beurlaubung und Ermäßigung der Arbeitszeit (von - bis); zusätzlich bei Arbeitnehmerinnen und Arbeitnehmern: Datum der letzten Eingruppierung, Vergütungs- bzw. Lohngruppe und Fallgruppe, feste Zulagen. **Beurteilungsdaten** gehören **nicht** dazu.

Verwaltungsvorlagen zu Personalmaßnahmen, die zusammen mit Stellungnahmen des Personalrats in alphabetischer Reihenfolge abgeheftet und im Personalratsbüro aufbewahrt werden, sind **unzulässige nebenaktenähnliche Personalvorgänge**, besonders, wenn weitere Maßnahmen den Akten fortwährend zugeordnet werden. Für diese Speicherung gibt es keine gesetzliche Grundlage. Auch die jährliche Information von Personalräten durch Listen über anstehende **Jubiläen** und **Verabschiedungen** ist unzulässig, denn hier mangelt es ebenfalls an einer bereichspezifischen gesetzlichen Grundlage. Diese Beschäftigtendaten dürfen daher nur auf Grund einer den Erfordernissen des § 4 DSG NW genügenden **Einwilligung** der Beschäftigten an den Personalrat weitergegeben werden.

18. Verkehr

Im Vordergrund datenschutzrechtlich bedeutsamer Änderungen in diesem Bereich steht das im Gesetzgebungsverfahren befindliche neue Straßenverkehrsgesetz. Zum Teil sind gravierende Einschnitte in das Recht der Verkehrsteilnehmerinnen und -teilnehmer auf ihre informationelle Selbstbestimmung vorgesehen. So sollen durch die Einrichtung eines **Zentralen Fahrerlaubnisregisters** beim Kraftfahrt-Bundesamt künftig die Führerscheindaten der ca. 60 Millionen Autofahrerinnen und Autofahrer elektronisch verfügbar sein. Ein solches zentrales Register in "elektronischer Nähe" zu dem bestehenden Verkehrszentralregister - der sogenannten Flensburger Kartei - und dem Zentralen Fahrzeugregister läßt es zu, daß in Sekundenschnelle die dort jeweils gespeicherten Daten aller Verkehrsteilnehmerinnen und -teilnehmer zur Verfügung stehen. Eine erst einmal so geschaffene zentrale Erfassung des größten Teils der Bevölkerung läßt weitergehende Verwendungen eines solchen Registers befürchten, also einen weiteren Schritt in Richtung Überwachungsstaat.

Die **elektronische Überwachung** an allen **Autobahnen** - zur Bezahlung einer Autobahngebühr - scheint im übrigen erfreulicherweise vorerst gescheitert zu sein, nachdem sich herausgestellt hatte, daß keines der erprobten technischen Verfahren den Schutz der dabei erhobenen personenbezogenen Daten gewährleistet, das heißt die Anforderungen wie Anonymisierung, Trennung von Zahlungs- und Nutzungsdaten und Transparenz der Erhebungs- und Kontrollvorgänge erfüllen konnte.

Informations- und Kontrollbesuche bei mehreren örtlichen Führerscheinstellen ergaben etliche **Datenschutzmängel**. In einigen Punkten ist das Verkehrsministerium der Anregung gefolgt, den Datenschutz durch verbindliche Erlaßregelungen zu verbessern. Dies betrifft beispielsweise die Festlegung von Prüfungsterminen zur Löschung automatisiert gespeicherter Führerscheindaten, der Vernichtung alter Karteibestände und - bis zur Einführung bundeseinheitlicher Anträge - der Verwendung datenschutzkonformer Antragsformulare.

Aus guten Gründen der Information und Beteiligung der Bevölkerung an Straßenplanungen sind in verschiedenen Stadien der straßenrechtlichen **Planfeststellungsverfahren** öffentliche Auslegungen geboten. Welche personenbezogenen Daten dabei in welchem Umfang bekanntzugeben sind, um einerseits der Informations- und Anstoßwirkung der Planunterlagen, andererseits aber auch dem Datenschutz gerecht zu werden, war Gegenstand einer grundsätzlichen Erörterung mit dem Verkehrsministerium, den Landschaftsverbänden und den Bezirksregierungen. Die Erörterung war notwendig geworden, nachdem im Rahmen einer Auslegung die Namen, Anschriften und Grund-

stücksbezeichnungen aller von der Planung betroffenen Grundstückseigentümerinnen und -eigentümer sowie die Liste von ungefähr 5000 Einwenderinnen und Einwendern veröffentlicht worden waren. Es konnten dabei folgende Ergebnisse erzielt werden:

- Planungsphase: In den auszulegenden Planungsunterlagen entfällt künftig die Angabe von Namen und Anschriften der Grundstückseigentümerinnen und -eigentümer.
- Anhörungsphase: In dem Erörterungstermin soll darauf hingewiesen werden, daß über den Termin eine Niederschrift gefertigt wird, in der die Einwenderinnen und Einwender mit Namen und Adresse bezeichnet werden. Alle Personen, die mit der Angabe ihrer persönlichen Daten nicht einverstanden sind, werden in der Niederschrift anonymisiert.
- Beschlußphase: Die namentliche Nennung von Einwenderinnen und Einwendern im Planfeststellungsbeschluß soll entfallen; statt dessen wird jede Einwendung mit einer Schlüsselnummer bezeichnet. Bei der Übersendung des Beschlusses wird der Einwenderin oder dem Einwender die entsprechende Schlüsselnummer mitgeteilt. Wird der Planfeststellungsbeschluß durch öffentliche Auslegung bekanntgemacht, können die Einwendungen anhand einer Schlüsselungsliste auf den jeweiligen Einwendungsfall bezogen und berechtigten Personen mitgeteilt werden.

Darüber hinaus will das Ministerium die Planfeststellungsrichtlinien überarbeiten.

19. Wirtschaft und öffentliche Unternehmen

Das Internet weckt viele Begehrlichkeiten. So wollten die Industrie- und Handelskammern die aus dem Handelsregister im automatisierten Verfahren erhaltenen **Daten der eingetragenen Unternehmen ins Netz einstellen**. Diesem Anliegen steht jedoch **entgegen**, daß die Bekanntgabe von Handelsregistereintragungen nicht ohne weiteres beliebig an private Dritte oder nichtöffentliche Stellen erfolgen kann, sondern nach dem Handelsgesetzbuch nur unter besonderen Anforderungen und Kontrollen möglich ist. Im übrigen würde durch eine Veröffentlichung im Internet aus der bisher nur zulässigen Einzelabfrage aus dem Handelsregister ein umfassender Online-Zugriff auf alle Eintragungen des beim jeweiligen Amtsgericht geführten Handelsregisters. Wenn dies alle Industrie- und Handeskammern anböten, wäre dann auch ein bundesweiter Zugriff auf alle Handelsregister denkbar. Da außerdem derzeit noch nicht bewältigte Gefahren für die Datensicherheit - mögliche Veränderungen und Löschungen der Daten auf dem Internet-Server - bestehen, sprechen alle datenschutzrechtlichen Anforderungen gegen die Zulässigkeit des Vorhabens.

19.1 Zuverlässigkeitsüberprüfung von Gewerbetreibenden

Seit Februar 1995 regelt § 11 der Gewerbeordnung (GewO) als datenschutzrechtliche Generalklausel die Verarbeitung personenbezogener Daten in allen gewerberechtlichen Verfahren. Bislang sind lediglich geringfügige Probleme bei Art und Umfang der Erhebung von Daten zur Überprüfung der Zuverlässigkeit der Gewerbetreibenden bekanntgeworden.

So fürchten die Gewerbebehörden auf Grund von Erfahrungen beispielsweise, daß sie in den Erteilungsverfahren für Gaststättenerlaubnisse im sogenannten Rotlichtmilieu, das den Betrieb von Pornokinos und ähnlichem einschließt, oder in Gebieten, deren Straßenbild stark vom Rauschgifthandel geprägt ist, nicht immer **vollständig** von den Betroffenen selbst über die Tatsachen **informiert** werden, die für die Zuverlässigkeitsbeurteilung eine Rolle spielen. In diesen Fällen fragen sie daher in aller Regel bei der örtlich zuständigen Polizeibehörde an, ob ein Ermittlungsverfahren anhängig ist oder war. Ich habe insoweit empfohlen, die Betroffenen vor Antragstellung auf diese Praxis hinzuweisen.

Eine andere Möglichkeit, sich über die Zuverlässigkeit von Gewerbetreibenden ein Bild zu machen, bietet die Einsichtnahme in **Schuldnerverzeichnisse** bei den Amtsgerichten. In diese Verzeichnisse werden Personen eingetragen, die

eine eidesstattliche Versicherung über ihre Vermögenslage abgegeben haben oder gegen die eine Haftanordnung zur Abgabe der eidesstattlichen Versicherung erlassen wurde. Von den Verzeichnissen können auch Abdrucke in der Form von **Schuldnerlisten** bezogen werden. Soweit Gewerbebehörden sich solche Listen - wie geschehen - regelmäßig übermitteln lassen wollen, ist darauf zu achten, daß die Listen von den in ihnen enthaltenen Daten anderer Personen als den Gewerbetreibenden bereinigt sind. Es kommt aus datenschutzrechtlichen Gründen also nur die Übersendung eines Auszugs der Liste in Betracht, der allein die Daten der Gewerbetreibenden ausweist. Dies sicherzustellen ist Aufgabe der Justizverwaltung.

19.2 Zuverlässigkeitsüberprüfung nach dem Atomgesetz

Wer in der Atomindustrie arbeiten will, wird "zum Schutz gegen Entwendung oder erhebliche Freisetzung radioaktiver Stoffe" besonders charakterlich durchleuchtet.

Die Überprüfung erfolgt auf der Grundlage von Auskünften von Landespolizei- und Landesverfassungsschutzbehörden, vom Generalbundesanwalt - Dienststelle Bundeszentralregister - sowie im Einzelfall vom Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik ("Gauck-Behörde"). Ergeben sich aus den von den Sicherheitsbehörden übermittelten Erkenntnissen Anhaltspunkte für die Unzuverlässigkeit der betroffenen Person, so kann die zuständige atomrechtliche Behörde auch bei anderen öffentlichen Stellen weitere Auskünfte einholen.

Das Überprüfungsverfahren ist in der bundeseinheitlichen "**Richtlinie** für die Überprüfung der Zuverlässigkeit der in kerntechnischen Anlagen, bei der Beförderung und Verwendung von Kernbrennstoffen und Großquellen tätigen Personen" geregelt. Dagegen spricht schon ein datenschutzrechtlicher Einwand grundsätzlicher Art, da § 12 b Abs. 2 des Atomgesetzes nicht nur eine Richtlinie, sondern den Erlaß einer **Rechtsverordnung** verlangt, die dann auch für die Atomindustrie bindende Wirkung entfalten würde.

Das Ministerium für Wirtschaft und Mittelstand, Technologie und Verkehr des Landes Nordrhein-Westfalen hatte den Richtlinienentwurf zur datenschutzrechtlichen Beurteilung vorgelegt. Die von mir benannten datenschutzrechtlichen Problempunkte - wie etwa die Einholung von unbeschränkten Bundeszentralregisterauszügen oder von Auskünften aus dem Gewerbezentralregister sowie die im Regelfall vorgesehene Anfrage an die "Gauck-Behörde" und die arbeitsrechtlich nicht vorgesehene Bekanntgabe bestimmter Angaben zur Per-

son an den Arbeitgeber - sind in der mittlerweile in Kraft getretenen Richtlinie nicht mehr vorhanden.

Die Bedenken gegen die Richtlinienform bestehen allerdings weiterhin, so daß das Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit aufgefordert bleibt, die notwendige Rechtsverordnung zu schaffen.

19.3 Korruptionsregister

Als Teil eines Maßnahmenbündels zur Korruptionsbekämpfung plant der Bund die Einrichtung einer zentralen Melde- und Informationsstelle für Vergabesperren. Damit soll verhindert werden, daß sich Unternehmen, die wegen Bestechung, Preisabsprachen oder ähnlichen Verfehlungen auffällig geworden sind, weiterhin ungehindert am Wettbewerb um öffentliche Aufträge beteiligen können.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Entschließung vom 9./10. November 1995 zu Planungen für ein Korruptionsbekämpfungsgesetz (Abdruck im Anhang) verlangt, daß der Gesetzgeber vor weiteren Eingriffen in die Freiheitsrechte eine sorgfältige Güter- und Risikoabwägung vornimmt und dabei insbesondere verantwortlich prüft, ob sich die innenpolitischen Ziele mit Mitteln erreichen lassen, welche die informationelle Selbstbestimmung der Bürgerinnen und Bürger schonen.

Auch auf **Länderebene** wird über die Errichtung derartiger Register nachgedacht. Auf eine entsprechende Anfrage des Wirtschaftsministeriums habe ich folgende **Bedenken** geäußert: Es ist gesetzlich nicht festgelegt, welche Behörde befugt sein soll und außerdem, welche Angaben über auffällige Firmen gesammelt sowie welche Angaben an die öffentlichen Vergabestellen übermittelt werden dürften. Darüber hinaus könnten wettbewerbs- und kartellrechtliche, aber auch europarechtliche Gesichtspunkte einem derartigen Meldesystem entgegenstehen. Im übrigen bestehen erhebliche Zweifel, ob eine auf das Land beschränkte Meldestelle für eine effiziente Kontrolle überhaupt geeignet sein könnte, da sich auch Unternehmen aus dem Bundesgebiet und dem europäischen Raum bewerben können.

19.4 Sparkassen

Multifunktionale Chipkarten, Internet, Homebanking und Datenübermittlung im Finanzverbund prägen auch in der Kreditwirtschaft die Entwicklungen mit datenschutzrelevanten Fragestellungen.

- Die notwendige Aufklärung der Kundinnen und Kunden über eine **Videokameraüberwachung** in Geldautomaten, die den Sparkassen bereits im 12. Tätigkeitsbericht (S. 128 f.) empfohlen wurde, ist immer noch nicht in die Tat umgesetzt, weil noch keine Abstimmung mit den privaten Banken über den Umfang der Information erreicht werden konnte. Nach dem derzeitigen Informationsstand soll auf allen Geldautomaten mit eingebauter Videokameraüberwachung mindestens der Hinweis gegeben werden, daß aus Sicherheitsgründen bei der Benutzung des Geldautomaten Bildaufnahmen erstellt und aufgezeichnet werden.

- Die Banken und Sparkassen wollen, daß die Kundinnen und Kunden bei Vertragsabschluß durch Unterzeichnung einer Klausel in die **Datenübermittlung innerhalb des Verbundes** der jeweiligen Finanzgruppe einwilligen, also bei den Sparkassen mit der Landesbausparkasse und den Provinzial-Versicherungen. Doch mit der inhaltlichen Ausgestaltung der Klausel hapert es noch. Sie muß aus der Sicht des Datenschutzes so präzise abgefaßt sein, daß vor Unterzeichnung der Einwilligungserklärung erkennbar ist, welcher Verbundpartner zu welchem Zweck welche Daten erhält und nutzen darf. Der ausdrücklichen **Einwilligungserklärung** bedarf es auch bei bestehenden Vertragsverhältnissen. Sollen also Daten der Kundinnen und Kunden für Angebote der Vertragspartner genutzt werden, muß die Einwilligung hierzu vorher eingeholt werden.

- **Girokonten für Sozialhilfeempfängerinnen und Sozialhilfeempfänger** müssen von den nordrhein-westfälischen Sparkassen grundsätzlich ohne Einschränkung eingerichtet werden. Die Einrichtung darf insbesondere nicht von der Unterzeichnung der Schufa-Erklärung, mit der in die Einholung einer Schufa-Auskunft eingewilligt wird, abhängig gemacht werden, wenn das Girokonto auf Guthabenbasis geführt werden soll. Nur dann, wenn eine Kundin oder ein Kunde beispielsweise die Teilnahme am Lastschriftverfahren wünscht, mit dem auch die Möglichkeit der Kontoüberziehung eingeräumt ist, bestehen gegen die Schufa-Erklärung keine Bedenken.

- Elektronische Geldbörse, Internetbanking oder Homebanking verändern den bargeldlosen Zahlungsverkehr und werfen neue Datenschutzprobleme auf. Beim elektronischen Bezahlen werden im Gegensatz zur Zahlung mit Bargeld Datenspuren gelegt, ohne daß dies den Betroffenen immer bewußt ist. Diese **Datenspuren** können gelesen, gesammelt und ausgewertet werden, so daß es technisch möglich ist, Nutzungsprofile zu gewinnen und diese für kommerzielle Zwecke zu verwenden.

  Im Hinblick auf diese technische Entwicklung haben es die Datenschutzbeauftragten des Bundes und der Länder in einer gemeinsamen Entschlie-

ßung vom 13. Oktober 1995 (Abdruck im Anhang) für dringend erforderlich gehalten, bei kartengestützten Zahlungssystemen **datenschutzfreundliche Verfahren** einzusetzen. Ein solches Verfahren stellt zum Beispiel die Verwendung von **Guthabenkarten** dar, die ohne personenbezogene Daten auskommen. Daneben können aber auch Verfahren entwickelt werden, die weder eine individuelle Kartennummer erfassen und speichern, noch einen anderen Bezug zur Karteninhaberin oder zum Karteninhaber herstellen. Vor allem im Kleingeldbereich ist die Nutzung von kontobezogenen Geldkarten entbehrlich, da fälschungssichere Guthabenkarten auf der Basis von Chipkarten mit integriertem Verschlüsselungsbaustein zur Verfügung stehen.

Die von den Sparkassen inzwischen eingeführte Geldkarte ermöglicht zumindest beim Aufladen des Chips mit Bargeld und bei der Nutzung von Automaten (öffentlicher Nahverkehr, Parkhäuser, Automatenverkauf) weiterhin den anonymen Zahlungsverkehr, bei dem keine auf die Betroffenen rückführbaren Einzeltransaktionen feststellbar sind. Bei größeren Geldbeträgen dagegen werden die einzelnen Zahlungsvorgänge im Verteilersystem, das heißt in den sogenannten Evidenzzentralen festgehalten, damit die erfolgten Abrechnungen mit den jeweiligen Banken nachvollzogen werden können. Die Evidenzzentralen speichern diese Einzeltransaktionen über einen längeren Zeitraum, in dem noch bestimmbar ist, welche Beträge mit der Geldkarte wann und wo abgebucht worden sind. Damit ist es auch wieder möglich, das Bewegungs- und Konsumverhalten der Betroffenen auszuwerten.

Anhang

Anlage 1

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995

zum Datenschutz bei elektronischen Mitteilungssystemen

Es ist damit zu rechnen, daß in Zukunft mit Hilfe elektronischer Mitteilungssysteme rechtsverbindliche bedeutsame Informationen und insbesondere personenbezogene Daten über Netze ausgetauscht werden.

Die zunehmende Nutzung von elektronischen Mitteilungssystemen (Electronic-Mail, Dokumentenaustausch über Datenfernübertragung, Message Handling Systems MHS/X.400) hat zur Folge, daß Bedrohungen wie Verlust von Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit verschärft werden, weil Unbefugte Zugriffe auf Daten und Programme erhalten können und die Übertragungswege vom Kommunikationspartner nicht sicher zu kontrollieren sind. Deshalb ist beim Einsatz solcher Systeme das Risikobewußtsein bei den Verantwortlichen sowie den Anwendern zu schärfen. In diesem Zusammenhang gewinnt der Schutz der elektronisch gespeicherten, verarbeiteten und übertragenen Information durch eine Vielzahl umfassender aufeinander abgestimmter Sicherheitsmaßnahmen an Bedeutung.

Die Datenschutzbeauftragten des Bundes und der Ländern fordern, daß den folgenden Sicherheitsaspekten beim Einsatz von elektronischen Mitteilungssystemen Rechnung getragen wird:

1. **Authentizität von Benutzern, Nachrichten und Systemmeldungen**

   Für den Empfänger einer Nachricht muß jederzeit die Möglichkeit bestehen, anhand bestimmter Kriterien die Authentizität des Absenders, der Nachricht sowie der an ihn gerichteten Systemmeldungen (z.B. Empfangs- und Weiterleitungsbestätigungen, Sendeanforderungen, Teilnehmerkennungen, Teilnehmereinstufungen) zu überprüfen.

2. **Vertraulichkeit von übertragenen Daten**

   Für alle Arten von Daten in elektronischen Mitteilungssystemen - Nachrichten sowie Verkehrs- und Verbindungsdaten - muß die Ver-

traulichkeit gewahrt bleiben. Sie ist durch geeignete Maßnahmen, z.B. kryptografische Verfahren, sicherzustellen.

3. Integrität von Nachrichten und Meldungen

Es ist zu gewährleisten, daß bei Speicherung und Weiterleitung von Daten keine unbefugte, unerkannte Veränderung erfolgen kann.

4. Fälschungssichere Kommunikationsnachweise

Die für die Anerkennung einer elektronischen Kommunikation erforderlichen fälschungssicheren Sende-, Empfangs- und Übertragungsnachweise müssen dem Anwender auf Wunsch zur Verfügung stehen.

5. Ausschluß von Kommunikationsprofilen

Die Erstellung von Kommunikationsprofilen muß verhindert werden. Gespeicherte Protokollierungsdaten dürfen nur zu Zwecken des Datenschutzes und der Datensicherung (§§ 14 Abs. 4, 31 BDSG bzw. landesgesetzliche Regelungen) verwendet werden.

Empfehlungen zum Einsatz von elektronischen Mitteilungssystemen:

Zum sicheren Einsatz von elektronischen Mitteilungssystemen sind als Grundschutzmaßnahmen folgende Empfehlungen zu beachten.

1. Grundsätzlich sind nur solche Produkte einzusetzen, die die Sicherheitsfunktionen der X.400-Empfehlung aus dem Jahre 1988 erfüllen. Vorhandene Systeme - insbesondere solche, die noch auf Empfehlungen von 1984 basieren - sollen künftig durch geeignete Zusatzprodukte hinsichtlich ihrer Sicherheit verbessert oder durch neuere Softwareversionen ersetzt werden.

2. Bei Übertragung von personenbezogenen Daten ist eine Verschlüsselung vorzusehen. Die Verschlüsselung der Daten muß mit einem hinreichend sicheren Verschlüsselungsverfahren erfolgen. Neben der Auswahl eines effektiven Verschlüsselungsalgorithmus (z.B. DES, IDEA) muß dabei insbesondere eine ordnungsgemäße Schlüsselerzeugung, -verwaltung und -verteilung gewährleistet sein. Verschlüsselungskomponenten sind durch technische, bauliche und organisatorische Maßnahmen vor dem Zugriff Unbefugter zu schützen.

3. Zur Absicherung der Integrität der Daten sollte auf Verfahren der "elektronischen Unterschrift" zurückgegriffen werden.

4. Nach Möglichkeit ist die Funktion des Systemverwalters von der des Netzwerkverwalters - insbesondere der Verwaltung des elektronischen Mitteilungssystems - aus Sicherheitsgründen zu trennen.

5. Es ist grundsätzlich separat administrierbare Hard- oder Software - z.B. in Form eines Kommunikationsservers - für das elektronische Mitteilungssystem vorzusehen.

6. Bei Verwendung von öffentlichen Übertragungswegen sind die vorhandenen Sicherheitsmechanismen dieser Netze z.B. geschlossene Benutzergruppen, Rufnummernidentifikation, Teilnehmerzeichengabe und automatische Rückruffunktion zur Abwehr des Zugriffs durch externe zu nutzen.

7. Zur Beweissicherung einer stattgefundenen Kommunikation sollte die eingesetzte Software folgende Funktionen beinhalten:

   - Zustellungs-/Empfangsnachweise

   - Sende-/Empfangsübergabenachweise.

Anlage 2

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 13. Oktober 1995

zum Datenschutz bei elektronischen Geldbörsen und anderen kartengestützten Zahlungssystemen

Die Datenschutzbeauftragten des Bundes und der Länder halten es für dringend erforderlich, daß bei kartengestützten Zahlungssystemen, die zunehmend in Konkurrenz zum Bargeld treten, datenschutzfreundliche Verfahren eingesetzt werden. Dabei bietet es sich an, vor allem Guthabenkarten zu verwenden. Es sollten nur solche Clearingverfahren eingesetzt werden, die weder eine individuelle Kartennummer benutzen noch einen anderen Bezug zum Karteninhaber herstellen.

Sowohl im öffentlichen Personennahverkehr als auch bei der Deutschen Bahn AG können Fahrscheine bargeldlos erworben werden. Auch Autofahrer können auf Bargeld verzichten: Beim Parken, beim Tanken, künftig auch bei der Benutzung von Autobahnen wird verstärkt auf elektronisches Bezahlen zurückgegriffen. Immer mehr Telefone und Warenautomaten werden auf bargeldlose Zahlungsverfahren umgestellt, so daß viele Artikel des täglichen Bedarfs elektronisch bezahlt werden können. Von Kreditinstituten wird die

Kombination verschiedener Anwendungen auf einer Karte angestrebt, z.B. mit einer Kombination der Bezahlung für den öffentlichen Nahverkehr, Parkgebühren und Benutzungsentgelte für öffentliche Einrichtungen.

Zum elektronischen Bezahlen werden entweder Kreditkarten, Debitkarten oder Guthabenkarten eingesetzt. Bei Kredit- und Debitkarten werden sämtliche Zahlungsbeträge verbucht, dem Käufer in Rechnung gestellt, auf den Kontoauszügen ausgedruckt und für mindestens 6 Jahre gespeichert. Dagegen wird bei Guthabenkarten im voraus ein Guthaben eingezahlt und bei jeder einzelnen Zahlung das Guthaben entsprechend herabgesetzt; die Zahlungsbeträge müssen keinem Käufer zugeordnet werden.

Beim elektronischen Bezahlen entstehen sehr unterschiedliche Datenschutzrisiken. Bei Kredit- und Debitkarten besteht die Gefahr, daß die aus Abrechnungsgründen gespeicherten personenbezogenen Daten ausgewertet und zweckentfremdet genutzt werden: Informationen über den Kauf von Fahrscheinen oder über die Nutzung von Autobahnen können zu Bewegungsprofilen verdichtet werden. Das Konsumverhalten des Einzelnen wird bis ins Detail nachvollziehbar, falls auch Kleineinkäufe am Kiosk nachträglich abgerechnet werden. Durch den Datenverkauf für Werbung und Marketing können sich weitere Risiken ergeben. Demgegenüber kann bei der Verwendung von Guthabenkarten auf das Speichern personen- oder kartenbezogener Daten aus erfolgten Zahlungen verzichtet werden.

Vor allem im Kleingeldbereich ist die Nutzung von Debit- und Kreditkarten entbehrlich, da fälschungssichere Guthabenkarten auf der Basis von Chipkarten mit integriertem Verschlüsselungsbaustein zur Verfügung stehen. Falls größere Geldbeträge nachträglich per Kredit- oder Debitkarte bezahlt werden, ist darauf zu achten, daß die Abrechnung zunächst über Konten erfolgt, deren Inhaber dem Zahlungsempfänger nicht namhaft gemacht wird. Erst bei Zahlungsunregelmäßigkeiten ist es notwendig, den Bezug zum Kontoinhaber herzustellen.

Angesichts der Risiken, aber auch der von Chipkarten ausgehenden Chancen, fordern die Datenschutzbeauftragten die Kartenherausgeber und die Kreditwirtschaft dazu auf, kartengestützte Zahlungssysteme zu entwickeln, die möglichst ohne personenbezogene Daten auskommen, und deren Anwendung so zu gestalten, daß ein karten- und damit personenbezogenes Clearing nicht erfolgt. Der Gesetzgeber muß sicherstellen, daß auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher anonym zu bleiben.

Anlage 3

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. November 1995

zur Weiterentwicklung des Datenschutzes in der Europäischen Union

Die Konferenz der Datenschutzbeauftragten der Europäischen Union hat am 08.09.1995 in Kopenhagen in einer Resolution im Hinblick auf die für 1996 geplante Regierungskonferenz dafür plädiert, anläßlich der Überarbeitung der Unions- und Gemeinschaftsverträge in einen verbindlichen Grundrechtskatalog ein einklagbares europäisches Grundrecht auf Datenschutz aufzunehmen. Die Schaffung rechtsverbindlicher Datenschutzregelungen für die Organe und Einrichtungen der Union sowie die Schaffung einer unabhängigen und effektiven Datenschutzkontrollinstanz der EU werden angemahnt. Dieser Resolution schließt sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an. Sie hält angesichts der fortschreitenden Integration und des zunehmenden Einsatzes von Informations- und Kommunikationstechnologien in der EU eine Weiterentwicklung des Datenschutzes im Rahmen der EU für geboten.

Sie fordert die zuständigen Politiker und insbesondere die Bundesregierung auf, dafür einzutreten, daß im EU-Vertragsrecht ein Grundrecht auf Datenschutz aufgenommen wird, die materiellen Datenschutzregelungen in der EU verbessert werden, das Amt eines Europäischen Datenschutzbeauftragten geschaffen wird sowie eine parlamentarische und richterliche Kontrolle der Datenverarbeitung der im EU-Vertrag vorgesehenen Instanzen sichergestellt wird.

Grundrecht auf Datenschutz

Bei einer Weiterentwicklung der Europäischen Union ist es unabdingbar, daß dem Grundrechtsschutz eine angemessene Bedeutung beigemessen wird. Dies sollte dadurch geschehen, daß die Verträge zur Europäischen Union mit einem Grundrechtskatalog ergänzt werden. Mit einer Entschließung vom 10.02.1994 hat das Europäische Parlament einen Entwurf zur Verfassung der Europäischen Union zur Erörterung gestellt, der unter anderem folgende Aussagen enthält: "Jeder hat das Recht auf Achtung und Schutz seiner Identität. Die Achtung der Privatsphäre und des Familienlebens, des Ansehens (...) wird gewährleistet".

Die Konferenz der Datenschutzbeauftragten ist mit ihrer Entschließung vom 28.04.1992 dafür eingetreten, daß in das Grundgesetz nach dem Vorbild ande-

rer europäischer Verfassungen ein Grundrecht auf Datenschutz aufgenommen wird. Sie hat hierfür einen Formulierungsvorschlag gemacht. Auf ihren Konferenzen am 16./17.02.1993 und 09./10.03.1994 bekräftigten die Datenschutzbeauftragten des Bundes und der Länder ihre Position. Diese Forderung wurde aber wegen des Nichterreichens der notwendigen qualifizierten Mehrheit durch den Gesetzgeber nicht umgesetzt.

In Wirtschaft, Verwaltung und Gesellschaft der Staaten der EU erhält der Dienstleistungs- und Informationssektor eine zunehmende Bedeutung. Dies hat zur Folge, daß mit hochentwickelten Informationstechnologien von privaten wie auch öffentlichen Stellen verstärkt personenbezogene Daten verarbeitet und auch grenzüberschreitend ausgetauscht werden. Diese Entwicklung wird gefördert durch die Privatisierung und den rasanten Ausbau transeuropäischer elektronischer Telekommunikations-Netze. Dadurch gerät das Grundrecht auf informationelle Selbstbestimmung in besonderem Maße auf der überstaatlichen Ebene in Gefahr. Dieser Gefahr kann dadurch entgegengetreten werden, daß in einen in den überarbeiteten EU-Vertrag aufzunehmenden Grundrechtskatalog das Grundrecht auf Datenschutz und zu dessen Konkretisierung ein Recht auf unbeobachtete Telekommunikation aufgenommen werden. Dies hätte folgende positive Auswirkungen:

- Anhand einer ausdrücklichen gemeinsamen Rechtsnorm kann sich eine einheitliche Rechtsprechung zum Datenschutz entwickeln, an die sowohl die EU-Organe wie auch die nationalen Stellen gebunden werden.
- Ein solches Grundrecht wäre die Basis für eine Vereinheitlichung des derzeit noch sehr unterschiedlichen nationalen Datenschutzrechts auf einem hohen Niveau.
- Den Bürgerinnen und Bürgern wird deutlich erkennbar, daß ihnen in einklagbarer Form der Datenschutz in gleicher Weise garantiert wird wie die traditionellen Grundrechte.
- Das grundlegende rechtsstaatliche Prinzip des Datenschutzes wird dauerhaft, auch bei Erweiterung der EU, gesichert.
- Mit der rechtlichen Konkretisierung eines Rechts auf unbeobachtete Telekommunikation würde der zunehmenden Registrierung des Verhaltens der Bürgerinnen und Bürger in der multimedialen Informationsgesellschaft entgegengewirkt und der Schutz des Fernmeldegeheimnisses auch nach dem Abbau der staatlichen Monopole im Sprachtelefondienst sichergestellt.

Materielle Datenschutzregelungen

Mit der kürzlich verabschiedeten EU-Datenschutzrichtlinie wird ein großer Fortschritt für den Datenschutz auf europäischer Ebene erreicht. Dies darf aber nicht den Blick dafür verstellen, daß in einzelnen Bereichen spezifische, dringend nötige Datenschutzregelungen fehlen. Insbesondere sind folgende Bereiche regelungsbedürftig:

- Es bedarf eines für die EU-Institutionen verbindlichen eigenen Datenschutzrechts. Die datenschutzrechtliche Verantwortung der Mitgliedstaaten einschließlich ihrer Datenschutzkontrolle der Übermittlung von Daten an EU-Institutionen bleibt dabei unberührt.
- Die geplante ISDN-Datenschutzrichtlinie darf weder einer völlig falsch verstandenen Subsidiarität zum Opfer fallen noch in unzureichender Form verabschiedet werden.
- Die im Bereich der Statistik bestehenden datenschutzrechtlichen Defizite sind abzubauen.
- Es soll eine Technikfolgenabschätzung bei der Förderung und Einführung neuer Informationstechniken mit Personenbezug durch die EU obligatorisch eingeführt werden.
- In den Bereichen Inneres und Justiz sind aufeinander abgestimmte verbindliche Regelungen mit hohem Datenschutzstandard, die die Datenverarbeitung in Akten und die Sicherung der Datenschutzkontrolle mit umfassen, zu schaffen.
- Es bedarf der Harmonisierung des Arbeitnehmerdatenschutzes auf hohem Niveau in den Staaten der EU.
- Für das Personal der EU-Organe ist der Arbeitnehmerdatenschutz sicherzustellen, was zum Beispiel bei der Durchführung von Sicherheitsüberprüfungen insbesondere unter Beteiligung von Behörden der Heimatstaaten von großer Bedeutung ist.

Es ist zu prüfen, inwieweit Informationszugangsrechte in weiteren Bereichen eingeführt werden sollen.

Europäischer Datenschutzbeauftragter

Die Konferenz der EU-Datenschutzkontrollinstanzen (25./26.05.1994, 08.09.1995) und die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (25.08.1994) haben darauf hingewiesen, daß es an einer unabhängigen und effektiven Datenschutzkontrollinstanz fehlt, an die sich jeder wen-

den kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der EU in seinen Rechten verletzt zu sein. Aufgabe eines Europäischen Datenschutzbeauftragten sollte die Behandlung aller Datenschutzbelange der EU sein. Dazu gehört nicht nur die Bearbeitung von Betroffeneneingaben, sondern auch die datenschutzrechtliche Beratung der EU-Organe und -Einrichtungen sowie deren anlaßunabhängige Kontrolle, die Begleitung informationstechnischer EU-Projekte und der entsprechenden EU-Normsetzung sowie die Zusammenarbeit mit den nationalen Kontrollinstanzen. Wegen der teilweise anders gelagerten Aufgaben sollen die Funktionen des Europäischen Datenschutzbeauftragten und des Bürgerbeauftragten nach den EG-Verträgen nicht vermengt werden. Die Bundesregierung sollte im Rahmen der Vorbereitung der Regierungskonferenz 1996 darauf hinwirken, daß ein unabhängiger Europäischer Datenschutzbeauftragter in den Verträgen über die Europäische Union institutionell abgesichert wird.

Parlamentarische und richterliche Kontrolle

Bei der Zusammenarbeit der EU-Staaten in den Bereichen Justiz und Inneres muß mit Besorgnis festgestellt werden, daß eine ausreichende parlamentarische und richterliche Kontrolle im EUV derzeit nicht gewährleistet ist. Die geplante Europol-Konvention ist hierfür ein Beispiel. Mit unbestimmten Formulierungen werden einem fast völlig freischwebenden Europäischen Polizeiamt informationelle Befugnisse eingeräumt, einem Amt, das keiner parlamentarischen Verantwortlichkeit und nur einer unzureichenden (teils nur nationalen) Rechtskontrolle unterworfen wird. Zur Wahrung des Datenschutzes bei der Umsetzung gemeinsamer Maßnahmen in den Bereich Justiz und Inneres muß daher - unbeschadet der Kontrolle durch die nationalen Datenschutzbehörden - auch eine im Rahmen ihrer jeweiligen Zuständigkeiten lückenlose Kontrolle durch die nationalen Parlamente und Gerichte sowie durch das Europäische Parlament und den Europäischen Gerichtshof sichergestellt werden.

Anlage 4

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. November 1995

zu datenschutzrechtlichen Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 47. Konferenz am 09./10 März 1994 kritisch zum Einsatz von Chipkarten im Gesundheitswesen Stellung genommen. In dem Beschluß wird die Nutzung

von Patientenkarten von mehreren Voraussetzungen zur Sicherung des Persönlichkeitsrechts abhängig gemacht.

Seitdem werden in mehreren Ländern Modellversuche und Pilotprojekte durchgeführt. Die Bandbreite reicht

- von allgemeinen Patientenkarten, die an möglichst viele Patienten/Versicherte ausgegeben werden, eine Vielzahl von Krankheitsdaten enthalten und von einem unbestimmten Kreis von Personen und Institutionen des Gesundheitswesens zu vielfältigen Zwecken verwendet werden können (zum Beispiel Vital-Card der AOK Leipzig, Persönliche Patientenkarte Neuwied, BKK-Patientenkarte Berlin)
- bis zu krankheitsspezifischen Karten für bestimmte Patientengruppen mit reduziertem Datensatz und einer Definition der Verwendung (zum Beispiel Dialyse-Card, Diab-Card, Krebsnachsorgekarte, Defi-Card).

Datenschutzrechtlich stellen sich vor allem folgende Probleme:

- Die massenhafte Einführung der Karten erzeugt einen sozialen Druck auf die Betroffenen, sie mitzuführen und vorzuzeigen. Diesen Erwartungen wird sich der Betroffene vielfach nur unter Befremden des Arztes oder sogar der Gefahr, daß dieser die Behandlung ablehnt, verweigern können.
- Die Verwendung von allgemeinen Patientenkarten bringt die Gefahr einer pauschalen Offenbarung von medizinischen Daten mit sich.
- Dem Patienten wird die Last aufgebürdet, für die Sicherheit seiner medizinischen Daten selbst zu sorgen.

Die Datenschutzbeauftragten fordern alle für Kartenprojekte im Gesundheitswesen Verantwortlichen in Politik, Industrie, Ärzteschaft, Wissenschaft und in den Krankenversicherungen auf, das Recht auf informationelle Selbstbestimmung der betroffenen Patienten bzw. Versicherten zu gewährleisten. Die 50. Konferenz hält folgende Voraussetzungen für elementar:

1. Besondere Schutzwürdigkeit medizinischer Daten

Medizinische Daten sind besonders schutzwürdig, unabhängig davon, welche Technologien eingesetzt werden, ob die Patientendaten beim Arzt gespeichert und versandt oder über ein Netz abgerufen werden oder ob der Patient die Daten auf einer Chipkarte bei sich hat. Es handelt sich oftmals um belastende, schicksalhafte Daten. Zudem geht es nicht nur um Daten des Patienten, sondern auch um fremde Einblicke in die ärztliche Tätigkeit.

2. Wirksame Entscheidung der Betroffenen über die Verwendung einer Karte

Die freie Entscheidung der Betroffenen (Patienten/Versicherten), eine Chipkarte zu verwenden, muß gewährleistet sein. Dies umfaßt die Entscheidung,

- ob Daten auf einer Chipkarte gespeichert werden,
- welche der Gesundheitsdaten auf die Karte aufgenommen werden,
- ob die Karte bei einem Arztbesuch bzw. einem Apothekenbesuch vorgelegt wird und
- welche Daten im Einzelfall zugänglich gemacht werden.

Ein Widerruf der Entscheidung muß ohne Nachteile für den Betroffenen möglich sein. Die gleiche Freiheit der Entscheidung für oder gegen die Verwendung der Chipkarte muß für Ärzte und Apotheker gewährleistet sein. Eine wirksame Entscheidung für oder gegen die Verwendung einer Chipkarte setzt eine schriftliche, objektive, vollständige und nachvollziehbare Information über Zweck, Art, Umfang und Beteiligte der Chipkarten-Kommunikation voraus. Das Gesamtkonzept des Chipkarteneinsatzes und der damit verbundenen Datenverarbeitung muß für die Betroffenen überschaubar sein.

Auf der Karte darf nicht der Datensatz der Krankenversichertenkarte nach § 291 Abs. 2 SGB V, insbesondere nicht die Krankenversicherung und die Krankenversicherungsnummer, gespeichert werden, da andernfalls - zumal bei allgemeinen Patientenkarten mit hohem Verbreitungsgrad - die Krankenversichertenkarte verdrängt und deren Nutzungsbeschränkungen umgangen werden.

3. Freiheit der Entscheidung

Die uneingeschränkte Freiheit der Entscheidung der Betroffenen für oder gegen die Verwendung einer Chipkarte muß gewährleistet sein, denn der Einsatz von Chipkarten im Gesundheitswesen führt keineswegs zwangsläufig zu größerer Autonomie der Patienten. Neue Technologien können sich auch als Verführung erweisen, deren Preis erst langfristig erkennbar wird. Die individuelle Entscheidung des Bürgers über die Verarbeitung seiner Daten war und bleibt ein zentrales Recht gegenüber Eingriffen in seine Freiheitssphäre. Mit der Chipkarte können sich jedoch Situationen ergeben, in denen wirkliche Freiheit, tatsächliche Wahlmöglichkeit der Betroffenen nicht mehr gewährleistet sind und durch technische und or-

ganisatorische, rechtliche und soziale Rahmenbedingungen wiederhergestellt werden müssen.

Dem Staat kommt hier eine veränderte Rolle zu: Freiheitsrechte nicht einzuschränken, sondern sie zu sichern, wo Entwicklungen des Marktes und der Technologien sowie Gruppeninteressen die Entscheidungsfreiheit des Bürgers bedrohen. Die Technologie selbst kann für die Sicherung der Freiheitsrechte ein wertvolles Hilfsmittel sein. Darüber hinaus kommt der Informiertheit der Betroffenen ein zentraler Stellenwert zu. Ihre Kompetenz zur Entscheidung und zum praktischen Umgang mit der Karte muß gestärkt werden, damit sie auch langfristig die größtmöglichen Chancen haben, ihre Interessen durchzusetzen.

Mit der Ausstellung der Karte dürfen nur die Vorteile verknüpft werden, die sich unmittelbar aus den Nutzungspraktiken der Karte selbst ergeben. Die freie Entscheidung der Betroffenen, eine Karte zu nutzen oder dies abzulehnen, darf nicht durch einen Nutzungszwang oder eine Bevorzugung von Karten-Nutzern (zum Beispiel durch Bonuspunkte) bzw. von Karten-Verweigerern eingeschränkt werden.

4. Keine Verschlechterung der Situation der Betroffenen

Durch die Einführung von Kommunikationssystemen mit Chipkarten dürfen die Betroffenen nicht schlechter gestellt werden als im konventionellen Verfahren. Die medizinische Versorgung, der Schutz der Gesundheitsdaten und die Mitentscheidungsrechte der Betroffenen müssen in Umfang und Qualität erhalten bleiben.

Das therapeutische Verhältnis Arzt/Patient darf sich durch den Einsatz von Chipkarten nicht verschlechtern. Freiheit und Vertrauen innerhalb des Arzt-Patienten-Verhältnisses sowie der Grundsatz der Abschottung der dem Arzt anvertrauten Informationen und der ärztlichen Erkenntnisse nach außen, gegen die Kenntnisnahme durch Dritte, müssen erhalten bleiben. Insbesondere muß der Gesetzgeber sicherstellen, daß die auf der beim Patienten befindlichen Chipkarte gespeicherten medizinischen Daten ebenso gegen Beschlagnahme und unbefugte Kenntnisnahme geschützt sind wie die beim Arzt gespeicherten Daten. Eine Kommunikation unter Vorlage der Karte mit Personen oder Stellen außerhalb des Arzt-Patienten-Verhältnisses, zum Beispiel Arbeitgebern oder Versicherungen, muß vom Gesetzgeber untersagt werden.

Das sich im Gespräch entwickelnde Vertrauensverhältnis zwischen Arzt und Patient darf nicht durch eine Chipkarten-vermittelte Kommunikation verdrängt werden. Verkürzte Darstellungen medizinischer Sachverhalte auf der Chipkarte - zum Beispiel mit Hilfe von Schlüsselbegriffen - dür-

fen nicht zu einer Minderung der Qualität des therapeutischen Verhältnisses führen; das liegt auch im Interesse des Arztes. Der Patient muß auch weiterhin die Möglichkeit des individuellen Dialogs wählen können. Dies schließt insbesondere die Freiheit des Betroffenen ein, eine Chipkarte im Einzelfall nicht vorzulegen, auf der Chipkarte nur einen begrenzten Datensatz speichern zu lassen oder zu entscheiden, welchem Arzt welche Informationen oder Informationsbereiche offenbart werden. Der Patient darf durch die Ausgestaltung und den Verwendungszusammenhang der Chipkarte nicht zur pauschalen Offenbarung seiner Daten gezwungen sein. So sind Daten auf der Chipkarte so zu ordnen, daß zum Beispiel beim Zahnarzt die gynäkologische Behandlung geheim bleiben kann.

Es darf keine "Einwilligung" in Chipkarten und Chipkartensysteme mit verminderter Datensicherheit geben. Der Gesetzgeber muß die Patientinnen und Patienten vor "billigen Gesundheitskarten" ohne ausreichende Sicherung vor einer Nutzung durch Dritte schützen.

5. Sicherstellung der Integrität und Authentizität der Daten

Zur Sicherstellung der Vertraulichkeit, Integrität und Authentizität der Daten auf Chipkarten im Gesundheitswesen und zur Differenzierung der Zugriffsmöglichkeiten nach dem Grundsatz der Erforderlichkeit in unterschiedlichen Situationen sind kryptographische Verfahren sowie geeignete Betriebssysteme zur Abschottung unterschiedlicher Anwendungsbereiche nach dem Stand der Technik in Chipkarten und Schreib/Lese-Terminals zu implementieren. Eine Protokollierung der Lösch- und Schreibvorgänge auf der Karte ist unverzichtbar.

Darüber hinaus ist für das infrastrukturelle Kartenumfeld (Herstellung, Verteilung, Personalisierung, ..., Rücknahme) sicherzustellen, daß ausreichende technische und organisatorische Maßnahmen Berücksichtigung finden. Für die zur Erstellung und Personalisierung von Gesundheits-Chipkarten dienenden Systeme sowie die informationstechnischen Systeme und Verfahren, mit denen Daten auf der Chipkarte gelesen, eingetragen, verändert, gelöscht oder verarbeitet werden, muß der gleiche hohe Sicherheitsstandard erreicht werden.

6. Keine neuen zentralen medizinischen Datensammlungen

Der Einsatz von Chipkarten im Gesundheitswesen darf nicht zur Entstehung neuer zentraler Dateien von Patientendaten bei Kassenärztlicher Vereinigung, Krankenkassen, Kartenherstellern oder sonstigen Stellen führen. Dies gilt auch für das Hinterlegen von Sicherungskopien der auf der Karte gespeicherten medizinischen Daten. Es steht in der freien Ent-

scheidung der Betroffenen, ob sie dem Arzt ihres Vertrauens eine umfassende Pflege aller Chipkarten-Daten - einschließlich der Sicherungskopien - übertragen oder nicht.

7. Leserecht des Karteninhabers

Der Karteninhaber muß das Recht auf die Möglichkeit haben, seine auf der Chipkarte gespeicherten Daten vollständig zu lesen.

8. Suche nach datenschutzfreundlichen Alternativen

Angesichts der aufgezeigten Gefährdungen der informationellen Selbstbestimmung im Gesundheitswesen muß die Suche nach datenschutzfreundlichen Alternativen zur Chipkarte fortgesetzt werden.

Vorstehende Kriterien sind der Maßstab für die datenschutzrechtliche Bewertung von Projekten für die Einführung von Chipkarten im Gesundheitswesen.

Die Datenschutzbeauftragten von Bund und Ländern fordern die Gesetzgeber auf, die dringend notwendigen Regelungen zur Sicherung der Rechte von Patienten und Ärzten zu schaffen. Ebenso ist durch die Gesetzgeber von Besonderheiten der Datenverarbeitung auf Chipkarten durch bereichspezifische Regelungen Rechnung zu tragen.

Anlage 5

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. November 1995

zu Planungen für ein Korruptionsbekämpfungsgesetz

Derzeit gibt es Vorschläge, die Bekämpfung der Korruption durch Verschärfungen des Strafrechts und des Strafprozeßrechts mit weiteren Eingriffen in das Grundrecht auf informationelle Selbstbestimmung zu organisieren. Ein Beispiel dafür ist der Beschluß des Bundesrates vom 3. November 1995 zur Einbringung eines Korruptionsbekämpfungsgesetzes.

Nach dem vom Bundesrat beschlossenen Gesetzentwurf sollen Bestechlichkeit und Bestechung in den Kreis derjenigen Tatbestände aufgenommen werden, bei deren Verdacht die Überwachung des Fernmeldeverkehrs und der Einsatz technischer Mittel ohne Wissen des Betroffenen (§§ 100a, 100c StPO) angeordnet werden dürfen.

Die Datenschutzbeauftragten weisen demgegenüber darauf hin, daß es vorrangig um Prävention, nicht um Repression geht. Die Datenschutzbeauftragten treten für eine entschlossene und wirksame Bekämpfung der Korruption mit rechtsstaatlichen Mitteln unter strikter Beachtung der Freiheitsrechte ein.

Sie wenden sich zugleich gegen eine Rechtspolitik, welche - noch bevor sie sich darüber im klaren ist, was die bisherigen Verschärfungen und Eingriffe an Vorteilen und an Nachteilen gebracht haben - auf weitere Verschärfungen und Eingriffe setzt.

Gerade gegenüber der Korruption gibt es Möglichkeiten, welche Effektivität versprechen und gleichwohl die Privatsphäre der unbeteiligten und unschuldigen Bürgerinnen und Bürger nicht antasten:

- Rotation derjenigen Mitarbeiterinnen und Mitarbeiter einer Behörde, deren Position und Aufgaben erfahrungsgemäß für Bestechungsversuche in Betracht kommen;
- Vier- und Sechsaugenprinzip bei bestimmten Entscheidungen;
- Trennung von Planung, Überwachung und Ausführung, von Ausschreibung und Vergabe;
- Prüfverfahren und Innenrevision;
- Codes of Conduct (formalisierte "Ethikprogramme") im Bereich der Wirtschaft;
- verbesserte Transparenz von Entscheidungsprozessen in der Verwaltung.

Die in den Gesetzentwürfen vorgesehene weitere Einschränkung von Grundrechten, die mit einer abermaligen Erweiterung der Telefonüberwachung verbunden wäre, ist nur vertretbar, wenn sie nach einer sorgfältigen Güter- und Risikoabwägung zusätzlich zu den oben genannten Verfahrens- und Verhaltensmaßregeln als geeignet und unbedingt erforderlich anzusehen wäre.

Die Datenschutzbeauftragten verlangen, daß vor einer zusätzlichen Aufnahme von Straftatbeständen in den Katalog der Abhörvorschrift des § 100a StPO diese Abwägung durchgeführt wird.

Die Datenschutzbeauftragten fordern weiterhin, daß eine Erweiterung des genannten Straftatenkataloges nur befristet vorgenommen wird, damit sich vor einer Verlängerung die Notwendigkeit stellt, auf der Grundlage einer sorgfältigen Erfolgs- und Effektivitätskontrolle erneut die Erforderlichkeit und Ver-

hältnismäßigkeit einer solchen Erweiterung des Grundrechtseingriffs zu überprüfen.

Die Datenschutzbeauftragten verlangen, daß der Gesetzgeber vor weiteren Eingriffen in Freiheitsrechte eine sorgfältige Güter- und Risikoabwägung vornimmt und dabei insbesondere verantwortlich prüft, ob sich die innenpolitischen Ziele mit Mitteln erreichen lassen, welche die informationelle Selbstbestimmung der Bürgerinnen und Bürger schonen.

Schließlich gibt die anstehende erneute Erweiterung des Katalogs von § 100a StPO Veranlassung, den Umfang der darin genannten Straftaten so bald wie möglich grundlegend zu überprüfen.

Anlage 6

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996

zur Modernisierung und europäischen Harmonisierung des Datenschutzrechts

Die Datenschutzrichtlinie der Europäischen Union vom Oktober 1995 verpflichtet alle Mitgliedstaaten, ihr Datenschutzrecht binnen drei Jahren auf europäischer Ebene zu harmonisieren. Die Richtlinie geht zu Recht von einem hohen Datenschutzniveau aus und stellt fest: "Die Datenverarbeitungssysteme stehen im Dienste des Menschen".

Die Datenschutzbeauftragten begrüßen diesen wichtigen Schritt zu einem auch international wirksamen Datenschutz. Sie appellieren an den Gesetzgeber in Bund und Ländern, die Umsetzung der Richtlinie nicht nur als Beitrag zur europäischen Integration zu verstehen, sondern als Aufforderung und Chance, den Datenschutz fortzuentwickeln. Die Datenschutzbeauftragten sprechen sich für eine umfassende Modernisierung des deutschen Datenschutzrechts aus, damit der einzelne in der sich rapide verändernden Welt der Datenverarbeitung, der Medien und der Telekommunikation über den Umlauf und die Verwendung seiner persönlichen Daten soweit wie möglich selbst bestimmen kann.

Die wichtigsten Ziele sind:

1. Weitgehende Vereinheitlichung der Vorschriften über den öffentlichen und privaten Bereich mit dem Ziel eines hohen, gleichwertigen Schut-

zes der Betroffenen, beispielsweise bei der Datenerhebung und bei der Zweckbindung bis hin zur Verarbeitung in Akten

2. Erweiterung der Rechte der Betroffenen auf Information durch die datenverarbeitenden Stellen über die Verwendung der Daten, auf Auskunft, auf Widerspruch und im Bereich der Einwilligung

3. Verpflichtung zu Risikoanalyse, Vorabkontrolle, Technikfolgenabschätzung und zur Beteiligung der Datenschutzbeauftragten bei der Vorbereitung von Regelungen mit Auswirkungen auf den Datenschutz

4. Verbesserung der Organisation und Stärkung der Befugnisse der Datenschutzkontrolle unter den Gesichtspunkten der Unabhängigkeit und der Effektivität

5. Einrichtung und effiziente Ausgestaltung des Amtes eines internen Datenschutzbeauftragten in öffentlichen Stellen

6. Weiterentwicklung der Vorschriften zur Datensicherheit, insbesondere im Hinblick auf Miniaturisierung und Vernetzung

Darüber hinaus machen die Datenschutzbeauftragten folgende Vorschläge:

7. Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen und Regelung der Video-Überwachung

8. Stärkere Einbeziehung von Presse und Rundfunk in den Datenschutz, Aufrechterhaltung von Sonderregelungen nur, soweit dies für die Sicherung der Meinungsfreiheit notwendig ist

9. Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren

10. Sicherstellung der informationellen Selbstbestimmung bei Multimedia-Diensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsformen anzubieten, durch den Schutz vor übereilter Einwilligung, zum Beispiel durch ein Widerrufsrecht, und durch strenge Zweckbindung für die bei Verbindung, Aufbau und Nutzung anfallenden Daten

11. Besondere Regelungen für Chipkarten-Anwendungen, um die datenschutzrechtliche Verantwortung aller Beteiligten festzulegen und den einzelnen vor unfreiwilliger Preisgabe seiner Daten zu schützen

12. Schutz bei Persönlichkeitsbewertungen durch den Computer, insbesondere durch Beteiligung des Betroffenen und Nachvollziehbarkeit der Computerentscheidung

13. Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing

14. Verbesserung des Datenschutzes bei grenzüberschreitender Datenverarbeitung; Datenübermittlung ins Ausland nur bei angemessenem Datenschutzniveau

Anlage 7

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 29. April 1996

zu Eckpunkten für die datenschutzrechtliche Regelung von Mediendiensten

In letzter Zeit finden Online-Dienste und Multimedia-Anwendungen zunehmend Verbreitung. Mit den - häufig multimedialen - Angeboten, auf die interaktiv über Telekommunikationsnetze zugegriffen werden kann, sind besondere Risiken für das Recht auf informationelle Selbstbestimmung der Teilnehmer verbunden; hinzuweisen ist insbesondere auf die Gefahr, daß das Nutzerverhalten unbemerkt registriert und zu Verhaltensprofilen zusammengeführt wird. Das allgemeine Datenschutzrecht reicht nicht aus, die mit den neuen technischen Möglichkeiten und Nutzungsformen verbundenen Risiken wirkungsvoll zu beherrschen.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für dringend erforderlich, durch bereichsspezifische Regelungen technische und rechtliche Gestaltungsanforderungen für die elektronischen Dienste zu formulieren, die den Datenschutz sicherstellen. Leitlinie sollte hierbei der Grundsatz der Datenvermeidung bzw. -minimierung sein. Die Datenschutzbeauftragten haben dazu in einer Entschließung vom 14./15. März 1996 zur Modernisierung und zur europäischen Harmonisierung des Datenschutzrechts vorgeschlagen, daß die informationelle Selbstbestimmung bei Multimediadiensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsverfahren anzubieten, durch den Schutz vor übereilter Einwilligung, zum Beispiel durch ein Widerspruchsrecht, und durch strenge Zweckbindung für die bei der Verbindung, Nutzung und Abrechnung anfallenden Daten sichergestellt wird.

Die Datenschutzbeauftragten weisen darauf hin, daß auch mit Inhalten, die durch Mediendienste verbreitet werden, datenschutzrechtliche Probleme verbunden sein können. Auf diese Probleme wird im folgenden jedoch - ebenso wie auf die Datenschutzaspekte der Telekommunikation - nicht näher eingegangen. Bei den datenschutzrechtlichen Eckpunkten wird ferner bewußt darauf verzichtet, den Regelungsort - etwa einen Länder-Staatsvertrag oder ein Bundesgesetz - anzugeben. Die Datenschutzbeauftragten appellieren an die Gesetzgeber in Bund und Ländern, eine angemessene datenschutzgerechte Regulierung der neuen Dienste nicht an Kompetenzstreitigkeiten scheitern zu lassen.

1. **Anonyme bzw. datensparsame Nutzung:** Die Dienste und Multimedia-Einrichtungen sollten so gestaltet werden, daß keine oder möglichst wenige personenbezogene Daten erhoben, verarbeitet und genutzt werden; deshalb sind auch anonyme Nutzungs- und Zahlungsformen anzubieten. Auch zur Aufrechterhaltung und zur bedarfsgerechten Gestaltung von Diensten und Dienstleistungen (Systempflege) sind soweit wie möglich anonymisierte Daten zu verwenden. Soweit eine vollständig anonyme Nutzung nicht realisiert werden kann, muß jeweils geprüft werden, ob durch andere Verfahren, zum Beispiel die Verwendung von Pseudonymen, ein unmittelbarer Personenbezug vermieden werden kann. Die Herstellung des Personenbezugs sollte bei diesen Nutzungsformen nur dann erfolgen, wenn hieran ein begründetes rechtliches Interesse besteht.

2. **Bestandsdaten:** Bestandsdaten dürfen nur in dem Maße erhoben, verarbeitet und genutzt werden, soweit sie für die Begründung und Abwicklung eines Vertragsverhältnisses sowie für die Systempflege erforderlich sind. Die Bestandsdaten dürfen zur bedarfsgerechten Gestaltung von Diensten und Dienstleistungen sowie zur Werbung und Marktforschung genutzt werden, soweit der Betroffene dem nicht widersprochen hat. Für die Werbung und Marktforschung durch Dritte dürfen Bestandsdaten nur mit der ausdrücklichen Einwilligung des Betroffenen verarbeitet werden.

3. **Verbindungs- und Abrechnungsdaten:** Verbindungs- und Abrechnungsdaten dürfen nur für Zwecke der Vermittlung von Angeboten und für Abrechnungszwecke erhoben, gespeichert und genutzt werden. Sie sind zu löschen, wenn sie für die Erbringung der Dienstleistung oder für Abrechnungszwecke nicht mehr erforderlich sind. Soweit Verbindungsdaten ausschließlich zur Vermittlung einer Dienstleistung gespeichert werden, sind sie spätestens nach Beendigung der Verbindung zu löschen. Die Speicherung der Abrechnungsdaten darf den Zeitpunkt, die Dauer, die Art, den Inhalt und die Häufigkeit bestimmter

von den einzelnen Teilnehmern in Anspruch genommener Angebote nicht erkennen lassen, es sei denn, der Teilnehmer beantragt eine dahingehende Speicherung. Verbindungs- und Abrechnungsdaten sind einer strikten Zweckbindung zu unterwerfen. Sie dürfen über den hier genannten Umfang hinaus nur mit der ausdrücklichen Einwilligung des Betroffenen erhoben, verarbeitet und genutzt werden. Unberührt hiervon bleibt die Speicherung von Daten von Verantwortlichen für Angebote im Zusammenhang mit Impressumspflichten.

4. **Interaktionsdaten:** Werden im Rahmen von interaktiven Dienstleistungen darüber hinaus personenbezogene Daten erhoben, die nachweisen, welche Eingaben der Teilnehmer während der Nutzung des Angebots zur Beeinflussung des Ablaufs vorgenommen hat (Interaktionsdaten; hierzu gehören zum Beispiel Daten, die bei lexikalischen Abfragen in interaktive Suchsysteme - etwa elektronische Fahrpläne und Telefonverzeichnisse - und bei Online-Spielen eingegeben werden), darf dies nur in Kenntnis und mit ausdrücklicher Einwilligung des Betroffenen geschehen. Interaktionsdaten dürfen nur unter Beachtung einer strikten Zweckbindung verarbeitet und genutzt werden. Sie sind grundsätzlich zu löschen, wenn der Zweck, zu dem sie erhoben wurden, erreicht wurde (so müssen Daten über die interaktive Suche von Angeboten unmittelbar nach Beendigung des Suchprozesses gelöscht werden). Eine weitergehende Verarbeitung dieser Daten ist nur auf Grundlage einer ausdrücklichen Einwilligung des Betroffenen zulässig.

5. **Einwilligung:** Der Abschluß oder die Erfüllung eines Vertragsverhältnisses dürfen nicht davon abhängig gemacht werden, daß der Betroffene in die Verarbeitung oder Nutzung seiner Daten außerhalb der zulässigen Zweckbestimmung eingewilligt hat. Soweit Daten aufgrund einer Einwilligung erhoben werden, muß diese jederzeit widerrufen werden können. Für die Form und Dokumentation elektronisch abgegebener Einwilligungen und sonstiger Willenserklärungen ist ein Mindeststandard zu definieren, der einen fälschungssicheren Nachweis über die Tatsache, den Zeitpunkt und den Gegenstand gewährleistet. Dabei ist sicherzustellen, daß der Teilnehmer bereits vor der Einwilligung soweit wie möglich über den Inhalt und die Folgen seiner Einwilligung und über sein Widerrufsrecht informiert ist. Deshalb müssen die Betroffenen sowohl vor als auch nach Eingabe der Erklärung die Möglichkeit haben, auf Einwilligungen, Verträge und sonstige Informationen über die Bedingungen der Nutzung von Diensten, Multimedia-Einrichtungen und Dienstleistungen zuzugreifen und diese auch in schriftlicher Form zu erhalten. Da Verträge oder andere rechtswirksame Erklärungen, die in einer Fremdsprache verfaßt sind, unter Um-

Zahlreiche Rechtsvorschriften gebieten, das Grundrecht auf informationelle Selbstbestimmung auch während der automatisierten Verarbeitung personenbezogener Daten zu sichern (z.B. § 78 a SGB X mit Anlage, § 10 Abs. 8 Btx-Staatsvertrag, § 9 BDSG nebst Anlage und entsprechende landesgesetzliche Regelungen).

Kryptographische Verfahren (z.B. symmetrische und asymmetrische Verschlüsselung, digitale Signatur) sind besonders geeignet, um Verletzungen des Datenschutzes beim Transport schutzwürdiger elektronisch gespeicherter Daten zu verhindern. Mit ihrer Hilfe lassen sich Manipulationen und Übertragungsfehler nachweisen und die unberechtigte Kenntnisnahme verhindern. Derartige Verfahren sind heute Stand der Technik und können in vielen Anwendungsfällen mit vertretbarem Aufwand eingesetzt werden.

Angesichts der beschriebenen Situation und der vorhandenen technischen Möglichkeiten fordern die Datenschutzbeauftragten des Bundes und der Länder, geeignete, sichere kryptographische Verfahren beim Transport elektronisch gespeicherter personenbezogener Daten unter Berücksichtigung ihrer Schutzwürdigkeit anzuwenden.

Anlage 9

Kurzbericht zum "Datenschutz durch Technik" für die Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. Oktober 1996

zu Datensparsamkeit durch moderne Informationstechnik - Datenvermeidung, Anonymisierung und Pseudonymisierung -

Die zunehmende Verbreitung, Nutzung und Verknüpfbarkeit von Informations- und Kommunikationstechnik bringt mit sich, daß jeder Benutzer immer mehr elektronische Spuren hinterläßt. Das wird dazu führen, daß er über Art, Umfang, Speicherort, Speicherdauer und Verwendungszweck der vielen über ihn gespeicherten Daten keine Kontrolle mehr hat, so daß die Gefahr des Mißbrauchs und der Zusammenführung zu komplexen Persönlichkeitsprofilen ständig zunimmt.

Dieser Gefahr kann dann begegnet werden, wenn in Zukunft die Frage nach der Erforderlichkeit personenbezogener Daten im Vordergrund steht, wobei Datensparsamkeit bis hin zur Datenvermeidung angestrebt werden muß. Durch die Nutzung neuer Möglichkeiten der modernen Informations- und Kommunikationstechnik (IuK-Technik) ist es in vielen Anwendungsfällen möglich, den

Umgang mit personenbezogenen Daten zu reduzieren bis hin zur vollständigen Vermeidung. Auf diese Weise kann das Prinzip **"Datenschutz durch Technik"** umgesetzt werden. Datensparsamkeit und Datenvermeidung werden sich dabei auch zunehmend als Wettbewerbsvorteil erweisen.

Ausgehend von einer Untersuchung des niederländischen Datenschutzbeauftragten und des Datenschutzbeauftragten von Ontario/Kanada zum sogenannten **Identity Protector** beschäftigen sich derzeit die Datenschutzbeauftragten des Bundes und der Länder intensiv mit der Formulierung von Anforderungen zur datenschutzfreundlichen Ausgestaltung von IuK-Technik. Schon die Sommerakademie in Kiel zeigte unter dem Motto "Datenschutz durch Technik - Technik im Dienste der Grundrechte" Wege zur Wahrung der Persönlichkeitsrechte der Bürger auf. Einige datenvermeidende Technologien wie die anonyme, vorausbezahlte Telefonkarte, sind bereits seit längerer Zeit allgemein akzeptiert. Erste Ansätze der Datenvermeidung auf gesetzgeberischer Ebene sind im Entwurf zum Teledienstegesetz und zum Mediendienstestaatsvertrag enthalten.

Der Arbeitskreis "Technische und organisatorische Datenschutzfragen" erarbeitet im Auftrag der Konferenz der Datenschutzbeauftragten des Bundes und der Länder einen Bericht mit Vorschlägen und Empfehlungen, wie unter Nutzung der modernen Datenschutztechnik das Prinzip der Datenvermeidung umgesetzt werden kann. Neben der Entwicklung entsprechender Hard- und Software werden Anonymisierung und Pseudonymisierung eine zentrale Rolle spielen. Bei der Erarbeitung des Berichtes werden Experten aus Wissenschaft und Forschung hinzugezogen, um die technische Entwicklung berücksichtigen zu können. Auch Vertreter der Wirtschaft als Entwickler und Anwender werden einbezogen, damit die Umsetzung der Vorschläge der Datenschutzbeauftragten als zukünftiger Wettbewerbsvorteil erkannt wird.

Während der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder wird vom Arbeitskreis "Technische und organisatorische Datenschutzfragen" ein Zwischenbericht zum Thema vorgelegt. Der umfassenden Darstellung des gesamten Problemkreises wird eine so große Bedeutung beigemessen, daß noch weitere Recherchen und die intensive Einbeziehung externer Fachleute erforderlich sind, um zukunftsweisende realistische Empfehlungen geben zu können.

Anlage 10

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. Oktober 1996

zum Datenschutz bei der Vermittlung und Abrechnung digitaler Fernsehsendungen

Mit der Markteinführung des digitalen Fernsehens eröffnen sich für die Anbieter - neben einem deutlich ausgeweiteten Programmvolumen - neue Möglichkeiten für die Vermittlung und Abrechnung von Sendungen. Hinzuweisen ist in erster Linie auf Systeme, bei denen die Kunden für die einzelnen empfangenen Sendungen bezahlen müssen. Dort entsteht die Gefahr, daß die individuellen Vorlieben, Interessen und Sehgewohnheiten registriert und damit Mediennutzungsprofile einzelner Zuschauer erstellt werden. Die zur Vermittlung und zur Abrechnung verfügbaren technischen Verfahren können die Privatsphäre des Zuschauers in unterschiedlicher Weise beeinträchtigen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter und Progammlieferanten auf, den Nutzern zumindest alternativ auch solche Lösungen anzubieten, bei denen die Nutzung der einzelnen Programmangebote nicht personenbezogen registriert werden kann, wie es der Entwurf des Mediendienste-Staatsvertrages bereits vorsieht. Die technischen Voraussetzungen für derartige Lösungen sind gegeben.

Die technischen Verfahren sind so zu gestalten, daß möglichst keine personenbezogenen Daten erhoben, gespeichert und verarbeitet werden (Prinzip der Datensparsamkeit). Verfahren, die im voraus bezahlte Wertkarten - Chipkarten - nutzen, um die mit entsprechenden Entgeltinformationen ausgestrahlten Sendungen zu empfangen und zu entschlüsseln, entsprechen weitgehend dieser Forderung. Allerdings setzt eine anonyme Nutzung voraus, daß beim Zuschauer gespeicherte Informationen über di gesehenen Sendungen nicht durch den Anbieter abgerufen werden können.

Die Datenschutzbeauftragten sprechen sich außerdem dafür aus, daß für die Verfahren auf europäischer Ebene Vorgaben für eine einheitliche Architektur mit gleichwertigen Datenschutzvorkehrungen entwickelt werden.

Anlage 11

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. Oktober 1996

zu Eingriffsbefugnissen zur Strafverfolgung im Informations- und Telekommunikationsbereich

Die Entwicklung moderner Informations- und Telekommunikationstechniken führt zu einem grundlegend veränderten Kommunikationsverhalten der Bürger.

Die Privatisierung der Netze und die weite Verbreitung des Mobilfunks geht einher mit einer weitreichenden Digitalisierung der Kommunikation. Mailboxen und das Internet prägen die Informationsgewinnung und -verbreitung von Privatleuten, von Unternehmen und öffentlichen Institutionen gleichermaßen.

Neue Dienste wie Tele-Working, Tele-Banking, Tele-Shopping, digitale Videodienste und Rundfunk im Internet sind einfach überwachbar, weil personenbezogene Daten der Nutzer in digitaler Form vorliegen. Die herkömmlichen Befugnisse zur Überwachung des Fernmeldeverkehrs erhalten eine neue Dimension; weil immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden, können sie mit geringem Aufwand kontrolliert und ausgewertet werden. Demgegenüber stehen jedoch auch Gefahren durch die Nutzung der neuen Technik zu kriminellen Zwecken. Die Datenschutzbeauftragten erkennen an, daß die Strafverfolgungsbehörden in die Lage versetzt werden müssen, solchen mißbräuchlichen Nutzungen der neuen Techniken zu kriminellen Zwecken wirksam zu begegnen.

Sie betonen jedoch, daß die herkömmlichen weitreichenden Eingriffsbefugnisse auch unter wesentlich veränderten Bedingungen nicht einfach auf die neuen Formen der Individual- und Massenkommunikation übertragen werden können. Die zum Schutz der Persönlichkeitsrechte des einzelnen gezogenen Grenzen müssen auch unter den geänderten tatsächlichen Bedingungen der Verwendung der modernen Informationstechnologien aufrechterhalten und gewährleistet werden. Eine Wahrheitsfindung um jeden Preis darf es auch insoweit nicht geben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher Thesen zur Bewältigung dieses Spannungsverhältnisses entwickelt.

Sie hebt insbesondere den Grundsatz der spurenlosen Kommunikation hervor. Kommunikationssysteme müssen mit personenbezogenen Daten möglichst sparsam umgehen. Daher verdienen solche Systeme und Technologien Vor-

rang, die keine oder möglichst wenige Daten zum Betrieb benötigen. Ein positives Beispiel ist die Telefonkarte, deren Nutzung keine personenbezogenen Daten hinterläßt und die deshalb für andere Bereiche als Vorbild angesehen werden kann. Daten allein zu dem Zweck einer künftig denkbaren Strafverfolgung bereitzuhalten ist unzulässig.

Bei digitalen Kommunikationsformen läßt sich anhand der Bestands- und Verbindungsdaten nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und damit wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Eine staatliche Überwachung dieser Vorgänge greift tief in das Persönlichkeitsrecht der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse (zum Beispiel Arztgeheimnis, anwaltliches Vertrauensverhältnis). Die Datenschutzbeauftragten fordern daher, daß der Gesetzgeber diesen Gesichtspunkten Rechnung trägt.

Die Datenschutzbeauftragten wenden sich nachhaltig dagegen, daß den Nutzern die Verschlüsselung des Inhalts ihrer Nachrichten verboten wird. Die Möglichkeit für den Bürger, seine Kommunikation durch geeignete Maßnahmen vor unberechtigten Zugriffen zu schützen, ist ein traditionelles verfassungsrechtlich verbürgtes Recht.

Aus Sicht des Datenschutzes besteht andererseits durchaus Verständnis für das Interesse der Sicherheits- und Strafverfolgungsbehörden, sich rechtlich zulässige Zugriffsmöglichkeiten nicht dadurch versperren zu lassen, daß Verschlüsselungen verwandt werden, zu denen sie keinen Zugriff haben. Eine Reglementierung der Verschlüsselung, zum Beispiel durch Schlüsselhinterlegung, erscheint aber aus derzeitiger technischer Sicht kaum durchsetzbar, da entsprechende staatliche Maßnahmen - insbesondere im weltweiten Datenverkehr - ohnehin leicht zu umgehen und kaum kontrollierbar wären.

Stichwortverzeichnis

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z

chen. Bei elektronischen Diensten, für die das Medienprivileg gilt, ist die externe Datenschutzkontrolle entsprechend zu beschränken.

9. **Geltungsbereich:** Der Geltungsbereich der jeweiligen Regelungen ist eindeutig festzulegen. Es ist sicherzustellen, daß die Datenschutzbestimmungen auch gelten, sofern personenbezogene Daten nicht in Dateien verarbeitet werden.

10. **Internationale Datenschutzregelung:** Im Hinblick auf die zunehmende Bedeutung grenzüberschreitender elektronischer Dienste und Dienstleistungen ist eine Fortentwicklung der europäischen und internationalen Rechtsordnung dringend erforderlich, die auch bei ausländischen Diensten, Dienstleistungen und Multimedia-Angeboten ein angemessenes Datenschutzniveau gewährleistet. Die Verabschiedung der sogenannten ISDN-Datenschutzrichtlinie mit einem europaweiten hohen Schutzstandard ist überfällig. Kurzfristig ist es notwendig, den Betroffenen angemessene Mittel zur Durchsetzung ihrer Datenschutzrechte gegenüber ausländischen Betreibern und Dienstleistern in die Hand zu geben. Die in Deutschland aktiven Dienste aus Nicht-EG-Staaten haben im Sinne der EG-Datenschutzrichtlinie (95/46/EG) vom 24.10.1995 einen verantwortlichen inländischen Vertreter zu benennen.

Anlage 8

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9. Mai 1996

zu Forderungen zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten

Der Schutz personenbezogener Daten ist während der Übertragung oder anderer Formen des Transportes nicht immer gewährleistet. Elektronisch gespeicherte, personenbezogene Daten können sowohl auf leitungsgebundenen oder drahtlosen Übertragungswegen als auch auf maschinell lesbaren Datenträgern weitergegeben werden. Oft sind die Eigenschaften des Transportweges dem Absender und dem Empfänger weder bekannt noch durch sie beeinflußbar. Vor allem die Vertraulichkeit, die Integrität (Unversehrtheit) und die Zurechenbarkeit der Daten (Authentizität) sind nicht sichergestellt, solange Manipulationen, unbefugte Kenntnisnahme und Fehler während des Transportes nicht ausgeschlossen werden können. Die Verletzung der Vertraulichkeit ist möglich, ohne daß Spuren hinterlassen werden.

ständen juristische Fachbegriffe enthalten, die nur vor dem Hintergrund der jeweiligen Rechtsordnung zu verstehen sind, sollten zumindest diejenigen Dienste, die eine deutschsprachige Benutzeroberfläche anbieten, derartige Unterlagen auch in deutscher Sprache bereitstellen.

6. **Transparenz der Dienste und Steuerung der Datenübertragung durch die Teilnehmer:** Die automatische Übermittlung von Daten durch die beim Betroffenen eingesetzte Datenverarbeitungsanlage ist auf das technisch für die Vertragsabwicklung notwendige Maß zu beschränken. Eine darüber hinausgehende Übermittlung ist nur aufgrund einer besonderen Einwilligung zulässig. Im Hinblick darauf, daß die Teilnehmer bei der eingesetzten Technik nicht erkennen können, in welchem Dienst sie sich befinden und welche Daten bei der Nutzung von elektronischen Diensten bzw. bei der Erbringung von Dienstleistungen automatisiert übertragen und gespeichert werden, ist sicherzustellen, daß die Teilnehmer vor Beginn der Datenübertragung hierüber informiert werden und die Möglichkeit haben, den Prozeß jederzeit abzubrechen. Die zur Nutzung vom Anbieter oder Netzbetreiber bereitgestellte Software muß eine vom Nutzer aktivierbare Möglichkeit enthalten, den gesamten Strom der ein- und ausgehenden Daten vollständig zu protokollieren. Bei einer Durchschaltung zu einem anderen Dienst bzw. zu einer anderen Multimedia-Einrichtung müssen die Teilnehmer über die Durchschaltung und damit mögliche Datenübertragungen informiert werden. Diensteanbieter haben zu gewährleisten, daß sie keine erkennbar unsicheren Netze für die Übertragung personenbezogener Daten nutzen bzw. den Schutz dieser Daten durch angemessene Maßnahmen sicherstellen. Entsprechend dem Stand der Technik sind geeignete (zum Beispiel kryptographische) Verfahren anzuwenden, um die Vertraulichkeit und Integrität der übertragenen Daten sowie eine sichere Identifizierung und Authentifikation zwischen Teilnehmern und Anbietern zu gewährleisten.

7. **Rechte von Betroffenen:** Die Rechte von Betroffenen auf Auskunft, Sperrung, Berichtigung und Löschung sind auch bei multimedialen und sonstigen elektronischen Diensten zu gewährleisten. Soweit personenbezogene Daten im Rahmen eines elektronischen Dienstes veröffentlicht wurden, der dem Medienprivileg unterliegt, ist das Gegendarstellungsrecht der von der Veröffentlichung Betroffenen sicherzustellen.

8. **Datenschutzkontrolle:** Eine effektive, unabhängige und nicht anlaßgebundene Datenschutzaufsicht ist zu gewährleisten. Den für die Kontrolle des Datenschutzes zuständigen Behörden ist ein jederzeitiger kostenfreier elektronischer Zugriff auf die Dienste und Dienstleistungen und der Zugang zu den eingesetzten technischen Einrichtungen zu ermögli-