LANDTAG RHEINLAND-PFALZ
12. Wahlperiode

Drucksache 12/3858
12. 11. 1993

158 Seiten

Unterrichtung

durch den Landesbeauftragten für den Datenschutz

Vierzehnter Tätigkeitsbericht nach § 21 des Landesdatenschutzgesetzes – LDatG – für die Zeit vom 1. Oktober 1991 bis 30. September 1993

Inhaltsverzeichnis

Dem Präsidenten des Landtags mit Schreiben vom 10. November 1993 zugeleitet.

Druck: Landtag Rheinland-Pfalz, 12. Januar 1994

Anlagen

Abkürzungen

AO	Abgabenordnung
BDSG	Bundesdatenschutzgesetz
BKA	Bundeskriminalamt
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
DOG	Dienstordnungsgesetz
Drs.	Drucksache
DSK	Datenschutzkommission
GG	Grundgesetz
HochschG	Landeshochschulgesetz
Kfz	Kraftfahrzeug
LDatG	Landesdatenschutzgesetz
LG	Landgericht
LfD	Landesbeauftragter für den Datenschutz
LKA	Landeskriminalamt
LKG	Landeskrankenhausgesetz
MG	Meldegesetz
MRRG	Melderechtsrahmengesetz
MS-DOS	Microsoft-Disk-Operating-System
NJW	Neue Juristische Wochenschrift
PC	Personal-Computer
PVG	Polizeiverwaltungsgesetz
Rdnr	Randnummer
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
Tb	Tätigkeitsbericht
TEMEX	Fernmeß- und Fernwirkdienst
Tz	Textziffer

Tätigkeitsberichte der Datenschutzkommission und des Landesbeauftragten für den Datenschutz

1.	Tätigkeitsbericht	Drs. 7/3342	vom 17. Oktober	1974
2.	Tätigkeitsbericht	Drs. 8/350	vom 1. Oktober	1975
3.	Tätigkeitsbericht	Drs. 8/1444	vom 1. Oktober	1976
4.	Tätigkeitsbericht	Drs. 8/2470	vom 10. Oktober	1977
5.	Tätigkeitsbericht	Drs. 8/3492	vom 12. Oktober	1978
6.	Tätigkeitsbericht	Drs. 9/253	vom 15. Oktober	1979
7.	Tätigkeitsbericht	Drs. 9/970	vom 15. Oktober	1980
8.	Tätigkeitsbericht	Drs. 9/1869	vom 28. Oktober	1981
9.	Tätigkeitsbericht	Drs. 10/270	vom 26. Oktober	1983
10.	Tätigkeitsbericht	Drs. 10/1922	vom 8. November	1985
11.	Tätigkeitsbericht	Drs. 11/710	vom 11. November	1987
12.	Tätigkeitsbericht	Drs. 11/3427	vom 21. Dezember	1989
13.	Tätigkeitsbericht	Drs. 12/800	vom 16. Dezember	1991

1 Vorbemerkung

Mit der Vorlage dieses 14. Tätigkeitsberichts ist an zwei Ereignisse zu erinnern, die für den Datenschutz von herausragender Bedeutung sind: Vor fast zwanzig Jahren hat der Landesgesetzgeber mit der Verabschiedung des „Gesetzes gegen mißbräuchliche Datennutzung" den Grundstein für die Datenschutzarbeit im Lande Rheinland-Pfalz gelegt und vor zehn Jahren hat das Bundesverfassungsgericht in einer Grundsatzentscheidung, die in ihrer Bedeutung weit über den Anlaß der Verfassungsbeschwerde – die Volkszählung – hinausreichte, klargestellt, daß Datenschutz Verfassungsrang hat. Das höchste deutsche Gericht hat ein „Recht auf informationelle Selbstbestimmung" definiert, in das nur durch Gesetz oder aufgrund eines Gesetzes und nur im überwiegenden Allgemeininteresse eingegriffen werden darf.

Die beiden Ereignisse kennzeichnen eine höchst bedeutsame Akzentverschiebung des Datenschutzes. Vor zwanzig Jahren war es das Ziel des Datenschutzes zu vermeiden, daß der informationelle Status quo durch den Einsatz der automatisierten Datenverarbeitung zum Nachteil des Bürgers verändert wird. Im Blick des Gesetzgebers waren nur die Folgen des Technikeinsatzes im Rahmen der Befriedigigung traditioneller staatlicher Informationsansprüche. Heute ist dies anders. Längst ließ die Entwicklung der Informationstechnik, insbesondere die vor zwanzig Jahren nicht einmal ansatzweise vorhersehbare Erweiterung der Speicherkapazitäten und die jetzt bestehenden Möglichkeiten der Datenverarbeitung (z. B. Recherche, Übermittlungen, Abgleiche) in einem Rückkoppelungseffekt gewissermaßen neue Informationsansprüche des Staates entstehen. So wird die Datenschutzdiskussion mehr und mehr durch die Probleme der Grenzziehung für staatliche Informationsansprüche bestimmt. Die Frage, ob weitere Eingriffe in das informationelle Selbstbestimmungsrecht im überwiegenden Allgemeininteresse hinzunehmen sind, steht heute im Vordergrund.

Die Datenerhebung für die Erfüllung öffentlicher Aufgaben hat eine Dimension erreicht, die größte Aufmerksamkeit verdient und die in einzelnen Bereichen staatlichen Handelns Anlaß zur Besorgnis gibt. Die Verteilung staatlicher Leistungen ist eine zentrale Staatsaufgabe; angesichts knapper Mittel differenzieren die gesetzlichen Bestimmungen immer stärker nach individuellen Einzelfallbedingungen. Sie verlangen umfangreichere Datenerhebungen und Datenzugriffe im Rahmen einer komplexeren zentralen oder vernetzten Informationsverarbeitung – auch um die mißbräuchliche Inanspruchnahme öffentlicher Leistungen zu begrenzen. So stellt sich die Frage, ob der Gesetzgeber immer neue Eingriffsgrundlagen schaffen darf für die Datenerhebung durch Sicherheitsbehörden unter Einsatz neuer Techniken (Lauschangriff), für die Kontrolle von Sozialleistungsempfängern oder für die Überwachung von Landwirten aufgrund EG-Rechts. Entspricht es noch dem Menschenbild des Grundgesetzes, daß der Staat Wanzen oder Videokameras im engsten Wohnungsbereich für die Datenerhebung nutzt, daß er dem Bürger, der auf Sozialleistungen angewiesen ist, immer stärker mit Mißtrauen entgegentritt, indem er durch Eröffnung von Zugriffsmöglichkeiten und durch Datenabgleiche ein noch dichteres Kontrollnetz knüpft, und daß er existentiell notwendige Leistungen an die Landwirtschaft davon abhängig macht, daß sich die Leistungsempfänger mit der Überwachung ihres Betriebs unter Einsatz der Satellitentechnik einverstanden erklären?

Der Katalog denkbarer Überwachungsmaßnahmen unter Nutzung der automatisierten Datenverarbeitung läßt sich beliebig erweitern. Stehen heute Sicherheitsfragen und die staatliche Leistungsgewährung im Vordergrund, so kann es morgen die verstärkte Kontrolle der öffentlichen Einnahmen sein. Oder gibt es hier vielleicht im Blick auf die Betroffenen größere Hemmnisse? Wer diesen Tätigkeitsbericht aufmerksam liest, wird manche Besorgnis teilen.

Wenig gewandelt hat sich in den zwanzig zurückliegenden Jahren die Einstellung mancher Behörden zum Datenschutz. „Datenschutz ist Tatenschutz!" Mit dieser bösen Redensart wird noch allzu oft versucht, den Datenschutz zu diskreditieren.

Es gibt indessen nicht nur Anlaß zur Kritik; auch über Erfreuliches ist zu berichten. Das Änderungsgesetz zum Landesdatenschutzgesetz ist auf den Weg gebracht und die Bemühungen, die Beratungsarbeit der Datenschutzkontrollbehörde zu intensivieren, waren wohl insgesamt erfolgreich. Erfreulich ist auch die Zusammenarbeit mit der Kommission beim Landesbeauftragten für den Datenschutz, die die Datenschutzarbeit mit sachbezogenem Rat begleitet.

2 Novellierung des Landesdatenschutzgesetzes

Auf die Notwendigkeit, auch das allgemeine Datenschutzrecht des Landes den Forderungen aus dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 entsprechend neu zu gestalten, hatten sowohl die Datenschutzkommission wie auch der LfD in der Vergangenheit mehrfach, zuletzt in den beiden vorangehenden Tätigkeitsberichten, eindringlich hingewiesen (vgl. 12. Tb., Tz. 2.2 und 13. Tb., Tz. 2). Es ist deshalb zu begrüßen, daß nunmehr der Referentenentwurf eines Landesdatenschutzgesetzes vorliegt, in dem die Folgerungen aus der neueren verfassungs- und datenschutzrechtlichen Diskussion sowie der inzwischen gefestigten Rechtsprechung des Bundesverfassungsgerichts zum informationellen Selbstbestimmungsrecht gezogen werden. Es darf allerdings nicht unerwähnt bleiben, daß Rheinland-Pfalz nunmehr das letzte Bundesland ist, das sein Datenschutzgesetz noch nicht novelliert hat.

Es ist zu begrüßen, daß schon die erste Fassung des Referentenentwurfs die Datenverarbeitung in Akten sowohl in den Anwendungsbereich des Gesetzes wie auch in die Kontrollzuständigkeit des LfD uneingeschränkt einbezog. Im BDSG ist dies nicht zufriedenstellend geregelt.

Der LfD bedankt sich an dieser Stelle für die umfassende und frühzeitige Beteiligung schon im Stadium der Abstimmung zwischen den Ressorts der Landesregierung. Etwa die Hälfte seiner Vorschläge wurde in dem jetzt vorliegenden Entwurfstext berücksichtigt. Darunter befinden sich normenklarere Regelungen zum Geltungsbereich des Gesetzes einschließlich der Kontrollbefugnisse gegenüber den Staatsanwaltschaften, Regelungen über technische und organisatorische Maßnahmen sowie eine Auffangnorm für die Allgemeine Verwaltungstätigkeit. Hierzu gehören auch die Wiederaufnahme des bewährten Begriffs der automatisierten Anwendung wie der Wegfall des Ordnungswidrigkeitentatbestandes, der die Zusammenarbeit der Behörden mit dem LfD nachhaltig beeinträchtigt hätte.

In einer Reihe von Punkten konnte sich die Auffassung des LfD nicht durchsetzen; sie betreffen im wesentlichen die folgenden Bereiche:

Mit dem Entwurf in seiner jetzigen Fassung wird der bundesweit bewährte funktionale Behördenbegriff aufgegeben. Dies ergibt sich aus der Begründung des Entwurfs. Der funktionale Behördenbegriff bietet aber einen wichtigen Schutz vor zweckwidriger Verwendung personenbezogener Daten, indem er innerhalb einer Verwaltungseinheit diejenigen Stellen, die unterschiedliche gesetzliche Aufgaben wahrnehmen, hinsichtlich der Datenübermittlung wie dritte datenverarbeitende Stellen behandelt. Dies zwingt bei jeder Datenübermittlung zu einer Prüfung der datenschutzrechtlichen Zulässigkeit und macht dies damit auch dem Bearbeiter in besonderer Weise bewußt. So wird den Forderungen aus dem Volkszählungsurteil des Bundesverfassungsgerichts angemessen und wirksam Rechnung getragen. Dasselbe kann mit der jetzigen Konstruktion des Entwurfs nicht geleistet werden, die ohne Anknüpfung an die Organisationsstruktur allein auf die Zweckbindung abstellt. Dies ist schon deshalb nicht möglich, weil bei der Weitergabe personenbezogener Daten innerhalb einer organisatorischen Gesamtheit (z. B. einer großen Stadtverwaltung) die Zweckbindung oft ausgeklammert werden kann, indem der Erhebungszweck der Daten fallweise entsprechend übergreifend durch Oberbegriffe ersetzt wird.

Die Abwendung von dem im Lande durchweg akzeptierten funktionalen Behördenbegriff, den das Bundesverfassungsgericht in seinem Kammerbeschluß vom 18. Dezember 1987 (NJW 1988 S. 959, 961) als einen das Datenschutzrecht prägenden Begriff bezeichnet, bringt darüber hinaus unnötige Unsicherheiten in den praktischen Verwaltungsablauf. Das Meldegesetz von Rheinland-Pfalz ebenso wie das Sozialgesetzbuch gehen vom funktionalen Behördenbegriff aus. Würde die im Entwurf vorgesehene Regelung Gesetz, müßten viele Behörden im Lande für vergleichbare Verarbeitungsvorgänge unterschiedliches Recht anwenden. Bei den Bearbeitern vor Ort wird schließlich – auch im Vergleich mit anderen Ländern – der falsche Eindruck erweckt, daß für den Anwendungsbereich des Landesdatenschutzgesetzes der Datenfluß innerhalb einer Gesamtbehörde nunmehr prinzipiell erleichtert sei. Die erforderliche Aufklärungsarbeit würde sehr viel Verwaltungsaufwand erfordern.

Ein weiterer strittiger Punkt ist das vorgesehene automatisierte Übermittlungsverfahren.
Im Gegensatz zu mehreren anderen Landesdatenschutzgesetzen läßt der Entwurf die Einrichtung automatisierter Übermittlungsverfahren zu, ohne dies einer jeweils gesonderten Rechtsvorschrift vorzubehalten. Schon in seiner ersten Stellungnahme hatte der LfD dargelegt und begründet, daß dies aus der Sicht des Datenschutzes nur dann vertreten werden kann, wenn besondere Sicherungen für das Recht auf informationelle Selbstbestimmung vorgesehen werden. Hier kämen zusätzliche technische Anforderungen ebenso in Frage wie der Ausschluß der Übermittlung an private Nutzer, eine Sonderregelung besonderer Berufs- oder Amtsgeheimnisse, eine rechtzeitige Anhörung des LfD und eine präzisere Ausgestaltung der Anordnung durch den zuständigen Minister. Von den entsprechenden Vorschlägen wurde kein einziger übernommen.

Angesichts der allgemein anerkannten erhöhten Gefährdungen des Rechts auf informationelle Selbstbestimmung beim Betrieb automatisierter Übermittlungsverfahren entspricht dieses Ergebnis nicht dem hohen Schutzstandard, den der Entwurf ansonsten anstrebt.

Auf den Vorschlag des LfD wurde der Gesetzesaufbau in der Abfolge von Erhebung, Speicherung und Übermittlung dem Bundesdatenschutzgesetz und den Datenschutzgesetzen anderer Länder stärker angepaßt. In diesem Zusammenhang besteht jedoch noch Erörterungsbedarf hinsichtlich der Regelung für die Zulässigkeit der Erhebung und der Erforderlichkeit einer eigenen Bestimmung für die Zweckbindung als einem zentralen Institut des allgemeinen Datenschutzrechts.

Starken Bedenken begegnet ein Zustimmungsvorbehalt bei der Auskunftserteilung. Die Auskunft an betroffene Bürger wird von der Zustimmung der Verfassungsschutzes, der Gerichte, der Staatsanwaltschaft und der Polizei sowie von Behörden der Finanzverwaltung abhängig gemacht, soweit sie sich auf die Herkunft der Daten von ihnen bezieht. Angesichts der weitgefaßten allgemeinen Verweigerungsgründe und im Blick auf den ganz erheblichen Verwaltungsaufwand, der mit der Einholung der Zustimmung verbunden ist, hatte der LfD hiergegen von Anfang an Bedenken geltend gemacht. Betroffen sind nämlich pauschal alle Daten, die von den genannten Behörden stammen, also auch solche, für die die vorerwähnten allgemeinen Verweigerungsgründe überhaupt nicht zutreffen. Nachdem das Zustimmungserfordernis auch auf solche Auskünfte ausgedehnt ist, die sich auf Übermittlungen an die o. g. Stellen beziehen, bestehen weiterhin große Bedenken gegen die Regelung.

Der LfD hofft auf eine möglichst zügige Verabschiedung des Gesetzes, das, wenn weitere inhaltliche Forderungen übernommen werden, die Rechte des einzelnen gegenüber dem Staat deutlich verstärkt.

3 Die Datenschutzrichtline der EG

Am 15. Oktober 1992 hat die Kommission der Europäischen Gemeinschaften den geänderten Vorschlag für eine allgemeine Datenschutzrichtlinie vorgelegt. Deren Titel lautet nunmehr: Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (KOM 8 [92] 422 ENDG.-SYN 287, ABl. EG C 311 vom 27. November 1992) – zur ersten Fassung vgl. 13. Tb., Tz. 3 –. Dies ist die Reaktion auf die etwa 120 Änderungsanträge des Europäischen Parlaments zum ersten Entwurf aus dem Jahre 1990. Der geänderte Vorschlag bildet gegenwärtig die Basis für die weiteren Verhandlungen in der Arbeitsgruppe „Wirtschaftsfragen" des Rates zur Vorbereitung des gemeinsamen Standpunktes.

Es geht um den Versuch einer Harmonisierung des Datenschutzrechts in den EG-Mitgliedstaaten. Dem Binnenmarkt entspricht der freie Informationsaustausch. Allerdings fehlen bislang in Italien und Griechenland gesetzliche Regelungen zum Datenschutz. Bei jenen Mitgliedstaaten, die Datenschutzgesetze erlassen haben, finden sich recht unterschiedliche Ansätze, was Inhalt und Systematik anbelangt. So gehen beispielsweise der „Data Protection Act" des Vereinigten Königreichs – wie auch die französische Regelung – von einer umfassenden Registerpflicht aus. Das deutsche Datenschutzrecht ist wiederum durch das materiell-rechtliche Verbotsprinzip geprägt. Danach gilt für die Verarbeitung und Nutzung personenbezogener Daten als allgemeiner Grundsatz ein Verbot mit Erlaubnisvorbehalt: Die Verarbeitung und Nutzung von Daten ist verboten, es sei denn, sie ist durch das Datenschutzgesetz oder eine andere Rechtsvorschrift ausdrücklich erlaubt oder angeordnet oder der Betroffene hat dazu seine Einwilligung erklärt.

Die Meldepflichten bei der Kontrollbehörde gem. Artikel 18 bis 21 des geänderten Vorschlags haben wegen des befürchteten bürokratischen Aufwands Kritik hervorgerufen. Nach deutschem Recht ist bisher die Melde- und Registerpflicht im nichtöffentlichen Bereich lediglich bei Auftragsverarbeitung durch die Dienstleister und bei geschäftsmäßiger Verarbeitung zum Zweck der Übermittlung (z. B. durch Auskunfteien oder Adressenhändler) vorgesehen. Für die Briten wiederum ist der Begriff des „berechtigten Interesses" nach Artikel 7 f sowie deren Abwägung völlig fremd (vgl. den letzten Halbsatz: „ . . . , sofern nicht das Interesse der betroffenen Person überwiegt."). Die Regelung mittels Generalklausel ist aus britischer Sicht kein brauchbares Werkzeug zur Problemlösung.

In diesem Zusammenhang ist mithin die Frage nach dem Spielraum, der bei der Umsetzung einer EG-Richtlinie dem nationalen Gesetzgeber eingeräumt ist, von entscheidender Bedeutung. Es ist gegenwärtig nicht recht erkennbar, welche Regelungsspielräume den Mitgliedstaaten konkret verbleiben. Für den deutschen Datenschutz gilt, sich dennoch darauf einzustellen, daß der aktuelle Entwurf nicht mehr zwischen öffentlichem und nichtöffentlichem Bereich unterscheidet und im Gegensatz zur deutschen Regelung auch nicht von einem Verbot mit Erlaubnisvorbehalt ausgeht.

Der Richtlinienvorschlag betrifft (u. a.) die öffentlichen Verwaltungen, deren Tätigkeit unter das Gemeinschaftsrecht fällt. Einige Gesetzesänderungen werden unumgänglich sein; insbesondere wohl im Bereich der Unterrichtungspflichten und der Meldevorschriften. Was die Stellung der Aufsichtsbehörden anbelangt, ist derzeit nach Einschätzung des LfD noch Klärungsbedarf vorhanden. So ist ein wesentlicher Punkt des aktuellen Richtlinienentwurfs die Notwendigkeit der Schaffung einer unabhängigen Kontrollinstanz, und zwar sowohl für den öffentlichen wie für den nichtöffentlichen Bereich. Artikel 30 des Richtlinienvorschlags macht deutlich, daß dessen wortgetreue Umsetzung für die deutschen Datenschutzgesetze einen totalen Umstrukturierungsbedarf zur Folge hätte. Im ersten Absatz ist davon die Rede, daß jeder Mitgliedstaat eine unabhängige staatliche Behörde benennt, die für die Gewährleistung des Schutzes personenbezogener Daten zuständig ist. Im zweiten Absatz, zweiter Spiegelstrich, werden effektive Eingriffsbefugnisse gefordert. Diese Regelungen werfen eine Menge Fragen auf. So ist z. B. nicht klar, was mit Unabhängigkeit gemeint ist. Aus deutscher Sicht kommt hier nur die Unabhängigkeit gegenüber den zu Kontrollierenden in Frage. Ansonsten müßte man die Aufsichtsbehörden für den nichtöffentlichen Bereich, in Rheinland-Pfalz die Bezirksregierungen und das Innenministerium, in den für den Datenschutz zuständigen Organisationseinheiten der Eingriffsverwaltung umstrukturieren und ihnen gleichzeitig beispielsweise die Unabhängigkeit des LfD geben. Es entstünde ein nicht nur kontrollierendes, sondern entscheidungsbefugtes Gebilde, das zwischen den Staatsgewalten angeordnet wäre und sich keiner von ihnen zuordnen ließe. Tatsächlich sind die Bezirksregierungen indes gegenüber den zu kontrollierenden Privatfirmen absolut unabhängig. Man müßte also diesen Zusatz, „von den zu Kontrollierenden unabhängig", in den Richtlinientext aufnehmen. Fernerhin sollte das Wort „Gewährleistung" in Artikel 30 Abs. 1 durch das Wort „Kontrolle" ersetzt werden. Denn naturgemäß kann eine Kontrollbehörde den Datenschutz nicht gewährleisten, sondern die Einhaltung der datenschutzrechtlichen Bestimmungen lediglich kontrollieren. Den Datenschutz zu gewährleisten hat vielmehr der Datenverarbeiter selbst.

Der LfD hat auch gefordert, auf den Begriff der „effektiven Eingriffsbefugnisse" zu verzichten, da er ansonsten mit exekutiven Kompetenzen ausgestattet werden müßte. Diese wiederum sind dem deutschen Beauftragtenmodell fremd.

Nach allem würde der Richtlinien-Vorschlag bei wortgetreuer Umsetzung in einer nicht zu akzeptierenden Art und Weise in das Organisationsrecht der Mitgliedstaaten eingreifen.

Demnächst wird der EG-Ministerrat im Rahmen des europäischen Gesetzgebungsverfahrens auf der Grundlage des zweiten Kommissionsentwurfs einen gemeinsamen Standpunkt festlegen. Dann wird das Richtlinienvorhaben vom Europäischen Parlament in zweiter Lesung beraten. Erst danach kann der EG-Ministerrat die Richtlinie endgültig verabschieden. Nach den ursprünglichen Planungen sollte das Vorhaben mit der Vollendung des Binnenmarktes Anfang des Jahres 1993 abgeschlossen sein, nun wird Ende 1994 als frühester Zeitpunkt genannt.

Es ist zu hoffen, daß die verbleibende Zeit von allen Beteiligten genutzt wird, um die vorgenannten, nach Auffassung des LfD besonders wichtigen Punkte verbindlich zu klären. Gegenüber der Presse hat die EG-Kommission erklärt, daß die Richtlinie nur die großen Leitlinien eines Gesetzes festlege, ansonsten aber viel Freiraum eingeräumt werde. Gleichwohl sollte eine verbindliche Klärung herbeigeführt werden.

In diesem Zusammenhang enthält die Regelung in Artikel 3 des Richtlinienvorschlags, wonach die Bestimmungen der Richtlinie keine Anwendung finden auf Verarbeitungen für die Ausübung von Tätigkeiten, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, noch viel Streitstoff. Zu denken ist hier an das mit dem Vertrag von Maastricht in den EG-Vertrag (Artikel 3 b) aufgenommene Subsidiaritätsprinzip. So werden wohl künftig in Bund und Ländern jeweils zwei Datenschutzgesetze erforderlich sein; eines für die EG-Regelungsbereiche, das andere für jene Tätigkeiten, die nicht von der Regelungskompetenz der EG umfaßt sind. Zum Beispiel ist für den Datenschutz in den Bundesländern die Frage nach der Speicherung und Übermittlung der Religionsmerkmale durch die Meldebehörden von Bedeutung. Nach Auffassung des LfD fällt das Melderecht nicht in den Anwendungsbereich des Gemeinschaftsrechts. Mithin können die Meldebehörden auch nach Erlaß der EG-Richtlinie – entgegen den vorgesehenen Bestimmungen in Artikel 8 – das Religionsmerkmal speichern und an die Kirchen übermitteln; sozusagen auf der Grundlage des „landesspezifischen Datenschutzgesetzes".

Letztlich wird die Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr durch die Rechtsprechung des Europäischen Gerichtshofes entscheidend konturiert werden.

4 Meldewesen

4.1 Novellierung der Meldedaten-Übermittlungsverordnung (MeldDÜVO) vom 7. Februar 1984 (GVBl. S. 36)

Seit dem Erlaß der Meldedaten-Übermittlungsverordnung 1984 ist bei weiteren Behörden ein Bedarf an regelmäßigen Datenübermittlungen erkennbar geworden. Dieser ist zum einen auf Rechtsänderungen und zum anderen auf den zunehmenden Einsatz von Informationstechnik in den Behörden zurückzuführen. Deshalb ist eine Novellierung dieser Verordnung erforderlich. Die DSK und der LfD haben in der Vergangenheit wiederholt Änderungen und Ergänzungen angeregt.

Das Ministerium des Innern und für Sport hat dem LfD Ende Juli 1993 den Entwurf einer Ersten Änderungsverordnung zur Meldedaten-Übermittlungsverordnung zur Stellungnahme zugeleitet. Der LfD hat hierzu eine Stellungnahme mit folgenden Schwerpunkten vorgelegt:

a) Regelmäßige Datenübermittlung innerhalb der Verwaltungseinheit, der die Meldebehörde angehört

In der Frage, unter welchen Voraussetzungen Meldedaten innerhalb der Verwaltungseinheit, der die Meldebehörde angehört, regelmäßig (on-line) übermittelt werden dürfen, vertritt das Ministerium des Innern und für Sport seit langem die Auffassung, daß kein Erfordernis für eine Regelung in der MeldDÜVO bestehe. Diese Auffassung stützt sich auf den Wortlaut des § 31 Abs. 7 Meldegesetz (MG):
„Innerhalb der Verwaltungseinheit, der die Meldebehörde angehört, dürfen unter den in Absatz 1 genannten Voraussetzungen sämtliche der in § 3 Abs. 1 genannten Daten und Hinweise weitergegeben werden. Für die Weitergabe und Einsichtnahme der in § 3 Abs. 2 genannten Daten und Hinweise gelten die Absätze 2 und 6 entsprechend."

Die DSK hingegen war der Meinung, daß diese Vorschrift nur für die Einzeldatenübermittlung, also nicht für die regelmäßige Datenübermittlung, gelte. Dies folge aus dem Vorhandensein besonderer Regelungen für die regelmäßige Datenübermittlung. Die Übermittlungsempfänger innerhalb der Verwaltungseinheit seien Behörden oder Stellen i. S. des § 31 Abs. 4; die regelmäßige Datenübermittlung stehe daher unter Gesetzes-/Verordnungsvorbehalt. Die Absätze 4 und 5 des § 31 MG enthielten gegenüber Absatz 7 die spezielleren Regelungen; die Verweisung in Absatz 7 auf den Erforderlichkeitsgrundsatz in Absatz 1 verdeutliche, daß die Vorschrift gerade nicht für die regelmäßige Datenübermittlung gelten könne, denn hier sei eine Erforderlichkeitsprüfung im Einzelfall nicht möglich.

Auch der LfD vertritt diese Auffassung. Bei der Beantwortung von Anfragen haben die DSK ebenso wie seine Behörde auf die abweichende Rechtsauffassung hingewiesen.

Aus einer Stellungnahme zu dem o. a. Entwurf kann dieser Dissens nicht ausgeklammert bleiben. Der LfD tritt dafür ein, die Novellierung der MeldDÜVO für eine angemessene Lösung der Übermittlungsproblematik zu nutzen. Hierfür sprechen im übrigen keineswegs nur formale Gesichtspunkte. Bei örtlichen Prüfungen wird immer wieder festgestellt, daß Direktzugriffsverfahren eingerichtet wurden, die eindeutig nicht dem Verhältnismäßigkeitsgrundsatz entsprechen. So räumte beispielsweise die Vollstreckungsstelle einer Verbandsgemeindeverwaltung ein, daß wöchentlich höchstens fünf On-line-Abrufe durchgeführt werden. Den Prüfungsfeststellungen des LfD wurde entgegengehalten, daß die Einschränkungen des § 31 Abs. 5 Satz 3 keine Geltung hätten.

Selbstverständlich ist zu berücksichtigen, daß es sich um verhältnismäßig unsensible Daten handelt und daß das Bundesdatenschutzgesetz ebenso wie – de lege ferenda – das novellierte Landesdatenschutzgesetz für die Einrichtung eines automatisierten Abrufverfahrens keinen Gesetzesvorbehalt statuiert. Es ist aber auch zu berücksichtigen, daß, geht man von der Richtigkeit der von zuständigen Ressorts vertretenen Rechtsauffassung aus, die Einrichtung von On-line-Zugriffen uneingeschränkt zulässig wäre, denn nicht einmal die Regelungen des künftigen Landesdatenschutzgesetzes wären wegen des Vorhandenseins einer speziellen Regelung in § 31 Abs. 7 anwendbar. Die Verweisung auf den Erforderlichkeitsgrundsatz kann jedenfalls nicht verhindern, daß Abrufverfahren auch dort eingerichtet werden, wo die Zahl der Abrufe und deren grundsätzliche Geeignetheit für die Aufgabenerfüllung außer Verhältnis zu dem Informationseingriff steht.

Der LfD empfahl, in einer Ergänzung der MeldDÜVO die Einrichtung regelmäßiger Datenübermittlungen innerhalb der Verwaltungseinheit, der die Meldebehörde angehört, zuzulassen, soweit

- die zum Abruf bereitgehaltenen Daten ihrer Art nach für den Empfänger erforderlich sind und
- das Bereithalten der Daten zum Abruf durch den Empfänger unter Berücksichtigung der schutzwürdigen Belange der Betroffenen, der Aufgaben der beteiligten Stellen und der zu erwartenden Zahl der Abrufe angemessen ist.

Auf die formalen Voraussetzungen für die Einrichtung automatisierter Übermittlungsverfahren nach dem LDatG (künftig § 7 Abs. 2) sollte hingewiesen werden.

b) Verfahren der regelmäßigen Datenübermittlung

§ 1 Abs. 2 MeldDÜVO nennt als Form der regelmäßigen Datenübermittlung u. a. die Übertragung von Daten oder Übersendung von maschinell lesbaren Datenträgern (Nr. 3) und das Bereithalten von Daten zum Abruf (Nr. 4). Die Vorschrift soll nach dem o. a. Entwurf keine Veränderung erfahren.

Nach Auffassung des LfD fordert aber die seit 1984 – dem Verkündungsjahr der Verordnung – eingetretene Entwicklung der Datenverarbeitungstechnik die Prüfung, ob nicht eine Klarstellung vorzunehmen ist. Vor der Einführung und Anwendung von Arbeitsplatzcomputern (z. B. PC) bedeutete „Bereithalten von Daten zum Abruf", daß Meldedaten an unintelligente Terminals (Bildschirme oder Drucker) übermittelt wurden. Sie konnten von dem Übermittlungsempfänger nur gelesen oder ausgedruckt werden. Die Verwendung intelligenter Systeme als Endgeräte ermöglicht, abgerufene Daten zu speichern und weiter zu verarbeiten. Diese Nutzung der nach § 1 Abs. 2 Nr. 4 übermittelten Daten sollte in der MeldDÜVO grundsätzlich untersagt werden, soweit es für die Erfüllung der verschiedenen in der Verordnung genannten Aufgaben ausreichend ist, daß die Übermittlungsempfänger auf die jeweils aktuellen Meldedaten zugreifen können. Kommt eine Weiterverarbeitung übermittelter Daten in automatisierten Verfahren in Betracht, so ist § 1 Abs. 2 Nr. 3 – Übertragung von Daten oder Übersendung von maschinell lesbaren Datenträgern – einschlägig. Diese Form der regelmäßigen Datenübermittlung sollte jedoch ebenfalls unter einen ausdrücklichen Zulassungsvorbehalt (wie Nummern 4 und 5, mit Anschlußänderungen in den nachfolgenden Vorschriften) gestellt werden.

4.2 Veröffentlichung von Hinweisen auf Widerspruchsrechte nach dem Meldegesetz (MG)

Nach § 35 MG darf die Meldebehörde an jedermann Auskunft über Alters- oder Ehejubiläen von Einwohnern erteilen, wenn der Betroffene nicht widersprochen hat. Das Widerspruchsrecht kann innerhalb von zwei Monaten vor dem Jubiläum nicht mehr ausgeübt werden. Die Meldebehörde hat auf das Widerspruchsrecht wie auch auf andere Widerspruchsrechte nach dem Meldegesetz bei der Anmeldung sowie mindestens einmal jährlich durch öffentliche Bekanntmachung hinzuweisen.

Im Berichtszeitraum wurde bei 26 Verbandsgemeinden überprüft, ob dieser Verpflichtung zur öffentlichen Bekanntmachung der Widerspruchshinweise entsprochen wurde. Sechs Verbandsgemeinden (hiervon fünf aus dem Regierungsbezirk Rheinhessen-Pfalz) mußten einräumen, daß dies nicht geschehen war. Es war zu rügen, daß damit gegen melderechtliche Bestimmungen verstoßen wurde.

Aufgrund einer Anfrage hatte der LfD zu prüfen, ob der folgende Text, der mit der Überschrift „Veröffentlichung von Daten über Altersjubiläen im Amtsblatt der Verbandsgemeinde" veröffentlicht wurde, mit den melderechtlichen Vorschriften zu vereinbaren ist: „Die Veröffentlichung von Altersjubilaren wird nur dann vorgenommen, wenn der Jubilar dem nicht ausdrück-

lich widersprochen hat. Wird von dem Widerspruchsrecht Gebrauch gemacht, darf die Meldebehörde, z. B. der Presse, keine Auskunft über den Geburtstag oder das Ehejubiläum der betroffenen Person geben. Wenn auch von dem Widerspruchsrecht Gebrauch gemacht worden ist, darf z. B. der Ortsbürgermeister, der Bürgermeister oder der Landrat von dem Jubiläum unterrichtet werden. Wir bitten alle Bürgerinnen und Bürger, die im Jahre 1993 70 Jahre oder älter werden oder ein Ehejubiläum feiern, mit der Veröffentlichung ihrer Daten (Name, Vorname, Geburtsdatum, Datum des Jubiläums und Anschrift) einverstanden zu sein."

In seiner Stellungnahme wies der LfD darauf hin, daß der veröffentlichte Text unrichtig ist, sofern der Eindruck erweckt wird, eine Datenübermittlung aufgrund § 35 MG an Ortsbürgermeister, Bürgermeister oder den Landrat sei auch dann zulässig, wenn ihr widersprochen wurde. Tatsächlich sind die Genannten häufig aufgrund anderer Meldedatenübermittlungen (beispielsweise nach § 31 MG i. V. mit § 8 Meldedatenübermittlungsverordnung) über Jubiläen unterrichtet. Sie werden auf diesem Weg aber auch über den Widerspruch unterrichtet und dadurch in die Lage versetzt zu entscheiden, ob die Gratulation vollkommen unterbleiben oder aber nur unter Ausschluß der Öffentlichkeit erfolgen soll. Auch inhaltlich ist der Hinweis auf die Widerspruchsmöglichkeit verbesserungsbedürftig. So deckt beispielsweise die Überschrift „Veröffentlichung von Daten über Altersjubiläen" nicht den übrigen Text der Bekanntmachung, soweit er sich auch auf Ehejubiläen erstreckt. Widerspruchsberechtigt sind auch nicht nur solche Bürgerinnen und Bürger, die 70 Jahre und älter werden oder bei denen ein Jubiläum bevorsteht, sondern alle Einwohner, unabhängig von ihrem Alter. Da im übrigen nur die „Veröffentlichung der Daten im Amtsblatt" angesprochen ist, müßte nach den gesetzlichen Bestimmungen eine weitere Bekanntmachung erfolgen, die auch auf die Widerspruchsmöglichkeit gegen die Erteilung von Auskünften über Jubiläumsdaten für andere Zwecke – beispielsweise zur Gratulation durch Mandatsträger – hinweist.

Üblicherweise wird auf die Widerspruchsmöglichkeit gegen die Erteilung von Auskünften über Alters- und Ehejubiläen zusammen mit den nach dem Meldegesetz bestehenden anderen Widerspruchsmöglichkeiten hingewiesen. Der hierfür vom Ministerium des Innern und für Sport vorgeschlagene Text ist als Anlage 2 zur Verwaltungsvorschrift des Ministeriums des Innern und für Sport vom 30. September 1988, MinBl. S. 464, veröffentlicht.

4.3 Übermittlung von Einwohnerdaten an Ortsbürgermeister

Auf Anfrage äußerte sich die DSK wiederholt zu der Frage, ob und ggf. welche Melderegisterdaten an Ortsgemeinden weitergegeben werden dürfen. Eine zusammenfassende Darstellung der hierzu vertretenen Rechtsauffassung enthält der 13. Tätigkeitsbericht (Tz. 4.3): Es wurde für zulässig gehalten, einem Ortsbürgermeister auf Anforderung im Einzelfall nach § 31 Abs. 1 MG einer Einwohnerbestandsliste mit den Vor- und Familiennamen, etwaigen akademischen Graden und der Anschrift der Einwohner zu überlassen. Aufgrund der regelmäßigen Übermittlung von Meldedaten nach § 8 der Meldedaten-Übermittlungsverordnung (MeldDÜVO) kann eine derartige Liste vom Ortsbürgermeister ergänzt und fortgeschrieben werden.

Das Geburtsdatum war in den Stellungnahmen als übermittlungsfähiges Datum nicht erwähnt. Dies war nicht etwa deshalb unterblieben, weil es grundsätzlich nicht als übermittlungsfähig angesehen wird, sondern deshalb, weil seine Einbeziehung in die Einwohnerlisten in den Fällen, die an die DSK mit der Bitte um Stellungnahme herangetragen wurden, keine Rolle spielte.

Auf eine Anfrage, die die Einbeziehung des Geburtsdatums in die Einwohnerliste betraf, äußerte sich der LfD wie folgt:

„§ 8 Abs. 2 der MeldDÜVO läßt zu, daß die Meldebehörden an Ortsgemeinden zur Aufgabenerfüllung aus Anlaß der Anmeldung eines Einwohners regelmäßig die in der Vorschrift im einzelnen genannten Meldedaten übermitteln. Zu diesen Meldedaten gehört auch das Geburtsdatum. Um welche Aufgaben der Ortsgemeinden es sich hierbei handelt, ist nicht bestimmt. Der Verordnungsgeber ging davon aus, daß zu dem Grundbestand der bei einer Ortsgemeinde vorhandenen Informationen über einen neu zugezogenen Einwohner das Geburtsdatum gehört. Tatsächlich wird das Geburtsdatum in der Praxis außer zur eindeutigen Identifikation zur Erfüllung vielfältiger Aufgaben verwandt, so z. B. auch zu Gratulationszwecken.

Die zitierte Vorschrift setzt voraus, daß die Ortsgemeinde auch für die Einwohner, die nicht zuziehen – und sich deshalb zum Melderegister anmelden –, sondern schon in der Gemeinde wohnen, aufgrund einer Datenübermittlung aus dem Melderegister bestimmte Grundinformationen besitzt. Der Gesetzgeber sah es wohl als selbstverständlich an, daß den Ortsgemeinden auf der Grundlage des § 31 MG zur Aufgabenerfüllung einmalig eine Einwohnerliste zur Verfügung gestellt wird. Die Regelung in § 8 Abs. 2 Meldedaten-Übermittlungsverordnung wurde geschaffen, damit die Ortsgemeinden in der Lage sind, diese Liste bezüglich der Anmeldungen zum Melderegister zu aktualisieren. Eine spezielle Übermittlungsregelung für die erwähnte Einwohnerliste war deshalb nicht erforderlich, weil eine regelmäßige Datenübermittlung nicht in Rede steht und deshalb der Verordnungsvorbehalt des § 31 Abs. 5 nicht zu beachten ist.

Bezüglich des Inhalts der Einwohnerliste gilt der Erforderlichkeitsgrundsatz nach § 31 Abs. 1 MG. Eine Orientierung an den in § 8 Abs. 2 Nummern 1 bis 5 der Meldedaten-Übermittlungsverordnung genannten Merkmalen ist nicht nur zugelassen, sondern nach Auffassung des LfD geradezu geboten. Zu diesen Merkmalen gehört auch der Tag der Geburt."

4.4 Nutzung von Meldedaten für den Rundfunkgebühreneinzug

Gestützt auf das rechtswissenschaftliche Gutachten von Universitätsprofessor Dr. Jarass zur „Verfassungsmäßigkeit der regelmäßigen Nutzung von Einwohnermeldedaten für den Rundfunkgebühreneinzug" drängen die Rundfunkanstalten auf Schaffung einer Rechtsgrundlage für die regelmäßige Übermittlung von Meldedaten aus Anlaß der An- und Abmeldung von Einwohnern sowie von Sterbefällen. Durch eine Ergänzung der MeldDÜVO in der Weise, wie dies in Nordrhein-Westfalen und Hessen bereits geschehen ist und in anderen Ländern – z. B. Baden-Württemberg und Bayern – vorbereitet wird, sollen die Voraussetzungen geschaffen werden, um eine „effektivere Ausschöpfung des Gebührenpotentials durch die Landesrundfunkanstalten zu ermöglichen".

Der LfD bezweifelt, daß die von den Rundfunkanstalten angestrebte Ergänzung der MeldDÜVO vor dem Hintergrund der Regelungen im Rundfunkgebührenstaatsvertrag und im Meldegesetz Rheinland-Pfalz zulässig ist:

Nach § 3 Abs. 2 des Rundfunkgebührenstaatsvertrages haben die Rundfunkteilnehmer der Landesrundfunkanstalt die für die Gebührenerhebung benötigten Daten mitzuteilen. Die Erteilung von Auskünften durch Meldebehörden ist nach § 4 Abs. 6 Satz 1 des Rundfunkgebührenstaatsvertrages nur über Personen zulässig, bei denen tatsächliche Anhaltspunkte vorliegen, daß sie ein Rundfunkempfangsgerät zum Empfang bereit halten und dies nicht oder nicht umfassend nach § 3 angezeigt haben. Ferner ist bestimmt, daß die Einholung von Auskünften nur zulässig ist, soweit dies zur Überwachung der Rundfunkgebührenpflicht erforderlich und die Erhebung der Daten beim Betroffenen nicht möglich ist oder einen unverhältnismäßigen Aufwand erfordern würde. Obwohl § 4 Abs. 6 Satz 2 darauf hinweist, daß besondere melderechtliche Regelungen zur Unterrichtung der Landesrundfunkanstalten unberührt bleiben, ist davon auszugehen, daß damit keine über Satz 1 hinausgehende Befugnisnorm zur Einholung von Auskünften geschaffen wurde.

Bestehen bereits erhebliche Zweifel, ob die Vorschriften des Rundfunkgebührenstaatsvertrages eine Lösung in der von den Rundfunkanstalten angestrebten Weise zulassen, so gilt dies in noch stärkerem Maße für das Meldegesetz Rheinland-Pfalz. Nach § 31 Abs. 5 i.V.m. Abs. 1 dieses Gesetzes darf der Minister des Innern und für Sport die regelmäßige Übermittlung von Meldedaten nur dann zulassen, wenn diese Daten für die Aufgabenerfüllung erforderlich sind und die Übermittlung unter Berücksichtigung der schutzwürdigen Belange der Betroffenen und der Aufgabe der beteiligten Stellen angemessen ist. Bei den Personen, die kein Rundfunkgerät zum Empfang bereithalten und der großen Mehrzahl der Bürger, die ihrer Gebührenpflicht nachkommen, liegen diese Voraussetzungen nicht vor.

Der Landesbeauftragte für den Datenschutz Nordrhein-Westfalen verweist in seinem 10. Tätigkeitsbericht – S. 37 – auf zahlreiche Anfragen und Eingaben die deutlich machten, daß die regelmäßige Datenübermittlung an den Westdeutschen Rundfunk von den Bürgern als problematisch angesehen werde. Die Bürger empfänden eine derartige „Raster"-Fahndung nach Schwarzhörern und -sehern als unnötigen Eingriff in das Recht auf informationelle Selbstbestimmung der überwiegenden Mehrheit derjenigen, die ordnungsgemäß ihre Rundfunk- und Fernsehgeräte angemeldet haben.

4.5 Meldedatenübermittlung an den Internationalen Suchdienst Arolsen (ISD)

Der Internationale Suchdienst bemüht sich im Rahmen seiner Aufgabenstellung um die Erlangung von Unterlagen aus der Kriegszeit und unmittelbar danach, soweit sich diese Unterlagen auf ausländische Zivilpersonen beziehen. Er folgt damit einer von der Bundesrepublik Deutschland im Deutschlandvertrag aus dem Jahre 1955 übernommenen völkerrechtlichen Verpflichtung gegenüber den drei westlichen Siegermächten aus dem Zweiten Weltkrieg.

Unter Hinweis auf seine Aufgabenstellung ersuchte der ISD mehrere Verbandsgemeinden, die Durchsicht und Auswertung der noch vorhandenen Meldebücher und -karteien durch seine Mitarbeiter zu gestatten.

Die Verbandsgemeinden äußerten in einer Anfrage an den LfD Zweifel an der Zulässigkeit dieser Vorgehensweise. Sie begründeten diese Zweifel damit, daß den Auskunftsersuchen keine Ersuchen der Betroffenen im Einzelfall zugrunde lägen, sondern Globalauskünfte begehrt würden, die zwangsläufig auch Daten von Personen umfaßten, für die der ISD keinen konkreten Auftrag habe. Im datenschutzrechtlichen Sinne handele es sich um eine Vorratsspeicherung des ISD zumindest bis zu dem Zeitpunkt, zu dem die übermittelten Daten daraufhin ausgewertet werden, ob sich Anhaltspunkte finden, die für die Bearbeitung von Suchaufträgen hilfreich sind.

Im Sinne des § 11 MG, der strenge Verwendungsbeschränkungen für archivierte Meldedaten statuiert, kann nur dann von einer zulässigen Übermittlung zur Behebung einer Beweisnot gesprochen werden, wenn eine Datenübermittlung an den ISD durch die konkrete Anfrage eines Betroffenen veranlaßt ist.

Die in diesem Zusammenhang auch zu prüfende Frage, ob § 11 MG auf die früher manuell geführten Meldekarteien anzuwenden ist, wurde vom Ministerium des Innern und für Sport bejaht. Im Ergebnis ist also eine Durchsicht und Auswertung der Meldekarteien durch Mitarbeiter des ISD nicht zulässig.

Im Blick auf die große humanitäre Bedeutung der Arbeit des ISD bedauert der LfD, daß dessen Anliegen nicht entsprochen werden kann. Er wird im Rahmen einer Novellierung des Melderechts auf eine Übermittlungsregelung drängen, welche die Interessen des ISD berücksichtigt.

4.6 Kirchenaustritte

Im Berichtszeitraum beschwerten sich mehrere Bürger beim LfD über die öffentliche Bekanntmachung von Kirchenaustritten in den Pfarrgemeindenachrichten oder durch Bekanntgabe in den Gottesdiensten. In allen diesen Fällen war darauf hinzuweisen, daß der LfD mangels einer eigenen Zuständigkeit für den Bereich der Kirchen inhaltlich zu den Eingaben nicht Stellung nehmen kann. Kirchen können zwar öffentlich-rechtliche Körperschaften sein, sie werden jedoch auch dann vom Anwendungsbereich der staatlichen Datenschutzgesetze (des Bundesdatenschutzgesetzes oder des jeweiligen Landesdatenschutzgesetzes) nicht erfaßt. Dies ergibt sich aus der verfassungsrechtlich begründeten Sonderstellung der Kirchen, die auch in den Datenschutzgesetzen selbst Ausdruck gefunden hat. So folgt aus § 15 Abs. 4 BDSG, daß öffentlich-rechtliche Religionsgesellschaften nicht als öffentliche Stellen im Sinne des BDSG anzusehen sind. Gleiches ergibt sich für den Bereich der öffentlich-rechtlichen Religionsgesellschaften des Landes aus § 6 Abs. 4 Landesdatenschutzgesetz. Dies ist einhellige Ansicht und wird nicht bestritten (vgl. zu diesem Problembereich Schatzschneider, Wolfgang, Kirchenautonomie und Datenschutzrecht, Heidelberg 1984; Hoeren, Thomas, Kirchen und Datenschutz, Essen 1986).

Eine Strafbarkeit nach § 43 Abs. 2 Nr. 2 BDSG scheidet also schon mangels der Anwendbarkeit dieses Gesetzes auf die Kirchen und ihre Mitarbeiter aus. Gleiches gilt für die Strafvorschrift des § 27 LDatG. Ob und inwieweit die Verfahrensweisen der örtlichen Pfarreien gegen kirchliches Datenschutzrecht verstoßen, ist vom LfD nicht zu beurteilen. Aufgrund der Presseberichterstattung ist jedoch bekanntgeworden, daß sich die nach kirchlichem Datenschutzrecht eingesetzten Datenschutzbeauftragten gegen eine Beibehaltung der Praxis ausgesprochen haben.

Der Kontrollzuständigkeit des LfD unterliegende Behörden sind indessen an den Datenübermittlungsvorgängen beteiligt: Kirchenaustritte werden den örtlichen Pfarreien aufgrund von Meldedatenübermittlungen bekannt. Rechtsgrundlage der regelmäßigen Datenübermittlung durch Meldebehörden an öffentlich-rechtliche Religionsgemeinschaften ist § 32 MG, der es zuläßt, daß Daten der Mitglieder und die sich hierauf beziehenden Veränderungen übermittelt werden. Die Information über die Zugehörigkeit zu einer Religionsgemeinschaft betrifft unmittelbar das Verhältnis zwischen dieser und den Betroffenen. Die Verwendung dieser Information im kirchlichen Bereich hat keine Rückwirkung auf die Beurteilung der Zulässigkeit der Datenübermittlung nach der erwähnten Vorschrift des Meldegesetzes. Vor diesem Hintergrund besteht also ebenfalls kein Ansatzpunkt für ein Tätigwerden des LfD.

5 Polizei

5.1 Täterschutz?

Mit der ansteigenden Kriminalität und den in der öffentlichen Diskussion beklagten Defiziten bei ihrer Bekämpfung häufen sich auch die Vorwürfe gegen den Datenschutz. Dieser behindere die innere Sicherheit und führe zu einer Datenschutzlawine, die die Sacharbeit ersticke.

Diese Art von Vorwürfen kommt weniger aus den Länderpolizeien. Als Quelle derartiger Unmutsäußerungen ist zunehmend das Bundeskriminalamt auszumachen, dem offenbar die auf Länderebene über weite Strecken sachliche Zusammenarbeit zwischen Datenschützern und Polizei verborgen geblieben ist.

Die Kritik äußert sich häufig in allgemeinen Behauptungen, die wegen ihrer Pauschalität schwer widerlegbar sind; wird sie hingegen konkreter, dann offenbaren sich häufig Mißverständnisse über Fakten oder im Blick auf das anzuwendende Recht. So wurde auf der Herbsttagung 1992 des BKA u. a. der Vorwurf erhoben, Sozialhilfebehörden wären durch den Datenschutz gehindert, in Fällen des Verdachts von Sozialhilfebetrug durch Asylbewerber die erforderlichen Daten der Polizei zu übermitteln. Die Rechtsgrundlagen für diese Übermittlungen im SGB X konnten jedoch demgegenüber unmittelbar und ausführlich dargelegt werden (vgl. Tz. 5.6). Ein weiterer Vorwurf: Den Gewerbebehörden dürften keine Erkenntnisse über die Zuverlässigkeit von Personen im Sinne des Gewerberechts mehr übermittelt werden. Dem konnte ebenfalls an Ort und Stelle die Praxis in den Ländern entgegengehalten werden, die teilweise in Landespolizeigesetzen bereits festgeschrieben ist.

Der Hinweis auf die Vielzahl der Datenschutzbestimmungen im Sicherheitsbereich, insbesondere deren Unübersichtlichkeit und Regelungsdichte, trifft zwar – insbesondere für die Bundesgesetzgebung – im Ergebnis zu. Die Ursache hierfür ist aber weniger in konkreten Empfehlungen der Datenschutzbeauftragten zu sehen, als in dem offensichtlichen Bestreben, die jeweils bestehende Praxis rechtlich abzudecken und mögliche „datenschutzrechtliche Risiken" von vornherein auszuschalten. Nur in diesem Zusammenhang ist es zu erklären, wenn wichtige Gesetzentwürfe, wie der für ein neues Gesetz über das Bundeskriminalamt, so lange wie möglich vor den Landesdatenschutzbeauftragten wie aber auch vor den Landesregierungen geradezu

geheimgehalten werden. Während Vertreter des BKA auf Tagungen bereits über den Entwurf referieren, ist dessen Text auf Länderebene so gut wie unbekannt, obwohl gerade dort die Erfahrungen aus der Praxis vorhanden sind, die sich dann auch in der zu regelnden Zusammenarbeit mit dem BKA niederschlagen. Bei rechtzeitiger Beteiligung der Länderebene bestünde mit Sicherheit eine größere Chance, Strukturen zu konzipieren und den Regelungen zugrunde zu legen, die übersichtlicher und damit für Anwender und Betroffene transparenter sind.

Ein beliebtes Beispiel für Vorwürfe an die Adresse des Datenschutzes ist die Sachfahndung des BKA nach gestohlenen Kraftfahrzeugen (vgl. Tz. 5.18). Hier hat es insbesondere wegen der erstmaligen Übermittlung ganzer Datenbestände an Private zunächst Diskussionsbedarf bei den Datenschützern sowie dann zwischen diesen und dem BKA gegeben – eine ganz natürliche Sache. Schließlich kann es im Sinne eines rechtsstaatlichen Verfahrens doch nur nützlich sein, wenn eine neue Maßnahme zunächst einmal aus verschiedenen Positionen heraus sachlich diskutiert wird. Am Ende gab es keine überzeugende Gegenposition mehr aus der Sicht des Datenschutzes. Warum dieser Ablauf als Argument gegen den Datenschutz verwendet wird, ist nicht erkennbar. Das BKA selbst hat indessen während der Verhandlungen eine nicht unwesentliche Komplikation eingebracht, indem es die Maßnahme auf seine im Umfang des Anwendungsbereichs nicht abschließend geklärte Zentralstellenkompetenz stützte, obwohl zu Beginn der Erörterungen von einer Tätigkeit im Auftrag der Länderpolizeien ausgegangen wurde, um gerade in der wichtigen und eiligen Angelegenheit diese störende Problematik auszuklammern. Demgegenüber konnte der LfD auf Einladung der Polizeipräsidenten bei ihrer Tagung in Münster im Juni 1993 die Erfordernisse des Datenschutzes im Polizeibereich darstellen und gleichzeitig erfahren, welche konkreten Probleme wiederum die Praxis bereitet. Die Verstärkung des gegenseitigen Verständnisses hat auch hier die Bereitschaft zum vorbehaltsfreien Austausch gefördert und Wege aufgezeigt, wie auch gemeinsam effektive Lösungen zur Grundrechtsverwirklichung gesucht und gefunden werden können.

All dies zeigt, wie wichtig gerade auf dem Gebiet der inneren Sicherheit die Sachlichkeit der Auseinandersetzung ist; Auseinandersetzung in Sachfragen aus verschiedener Aufgabenstellung ist notwendig und sogar unverzichtbarer Bestandteil jeder vertrauensvollen Zusammenarbeit. Nur so kann den Zielen einer effektiven Verbrechensbekämpfung und dem Schutz der Individualrechte gleichermaßen und in jeweils angemessener Weise gedient werden. Vor allem sollte eines beherzigt werden: Offenheit erzeugt mehr Verständnis!

5.2 INPOL-Neukonzeption

Das BKA und die für die Polizei zuständigen obersten Landesbehörden arbeiten daran, das gemeinsame polizeiliche Informationssystem INPOL neu zu konzipieren. INPOL wurde zu Beginn der siebziger Jahre entwickelt und kam erstmalig 1972 auf dem Flughafen Frankfurt zur Anwendung. Es umfaßt heute ca. 27 Anwendungen, davon fünf im Verbund. Sind die Daten einer Person in verschiedenen Anwendungen zu speichern, so müssen insbesondere die Personalien mehrfach erfaßt, der Bestand muß aber auch mehrfach gepflegt werden. Da ein im allgemeinen Zugriff stehender Index fehlt, sind in einschlägigen Fällen gesonderte Abfragen in den verschiedenen Anwendungen erforderlich. Bei der Fortentwicklung haben immer neue Hilfslösungen das System unübersichtlich und komplex gemacht. Die damit schwieriger gewordene Handhabung hat jetzt erkennbare Auswirkungen auf die Akzeptanz bei der polizeilichen Arbeit „vor Ort". Die genannten Schwierigkeiten führen auch zu unbefriedigenden Situationen aus der Sicht des Datenschutzes.

Die Absicht, das System INPOL neu zu konzipieren, ist daher auch im Interesse des Datenschutzes zu begrüßen, wird es damit doch auch möglich, neue technische Entwicklungen für einen verbesserten Datenschutz zu nutzen.

Das Grobkonzept liegt seit einer Reihe von Monaten vor und wird zwischen den wegen des Verbundcharakters insgesamt betroffenen Datenschutzbeauftragten und dem Bundeskriminalamt diskutiert. Der LfD ist an den Arbeiten aktiv beteiligt; er begrüßt die stattfindende Form der Beteiligung ausdrücklich, weil sie realisierbare Vorschläge in einem Stadium ermöglicht, in dem die konkrete Ausgestaltung noch weitgehend offen ist.

Die Grundstruktur von INPOL – neu – sieht anstelle der bisherigen Einzelanwendungen einen anwendungsunabhängigen Datenpool vor, in dem die Unterschiedlichkeiten bei den Speicherungen und den Zugriffsberechtigungen durch eine Bitleiste sichergestellt werden sollen. Es soll eine ausgebaute dialogorientierte Recherche geben. Die Erstellung deliktsorientierter Falldateien wird in gewünschter Form jederzeit ermöglicht.

Soweit jetzt schon Beurteilungen möglich sind, ist aus der Sicht des Datenschutzes zunächst grundsätzlich darauf zu achten, daß in der weiteren Ausgestaltung durch die sich dann ergebenden vielfältigen Recherchemöglichkeiten die Zweckbindung der Daten nicht unterlaufen wird. Da auch Informationen aus der Vorgangsverwaltung im System INPOL – neu – erfaßt werden sollen, ist zu klären, wie landesrechtliche Regelungen, die z. T. besondere Restriktionen und Zweckbindungsregelungen für Daten enthalten, eingehalten werden können. Die datenschutzrechtliche Verantwortung muß normenklar geregelt und sichergestellt werden. Dies gilt auch für die differenzierten Zugriffsberechtigungen und die noch nicht näher dargestellten Zugriffe Externer.

Recherchen im System dürfen nur im unerläßlich notwendigen Umfang und nur im Rahmen der jeweiligen Aufgabenerfüllung des Anfragenden unter strikter Beachtung der Zweckbindung ermöglicht werden. Durch eine hinreichende Protokollierung der automatisierten Verarbeitung muß eine jederzeitig wirksame Kontrolle durch die Datenschutzbeauftragten des Bundes und der Länder gewährleistet sein. Weitere Forderungen betreffen insbesondere die Wahrung des Grundsatzes der Verhältnismäßigkeit, z. B. bei der Definierung der Kriterien für die überregionale Bedeutung und Schwere von Tatvorwürfen bei der Aufnahme in INPOL – neu –, aber auch das weitere Unterlassen einer vorgangsunabhängigen Speicherung zu präventiven Zwecken von Personen, die lediglich als Opfer, Zeugen oder Hinweisgeber mit der Polizei in Berührung gekommen sind.

In diesem Sinne hat sich der LfD an das Ministerium des Innern und für Sport mit der Bitte um Unterstützung bei der weiteren Entwicklung gewandt.

Jetzt schon zu bedauern ist die Absicht, die gesetzlichen Vorgaben für INPOL – neu – nicht bereits jetzt in den Entwurf für die Neufassung des Gesetzes über das Bundeskriminalamt zu übernehmen, sondern erst dann, wenn das Systemkonzept in allen Einzelheiten feststeht. Die Gesetzesformulierungen mit den datenschutzrechtlichen Anforderungen, die sich letztlich aus dem Volkszählungsurteil des Bundesverfassungsgerichts ergeben, müßten schon jetzt möglich sein. Eine nachgehende gesetzliche Regelung würde in gewissem Sinne eine Abwertung des Gesetzgebers als Institution bedeuten, der dann aufgrund bereits vorgegebener faktischer und technischer Systemzwänge in eine seiner verfassungsmäßigen Stellung nicht angemessene Notarfunktion gedrängt wäre.

5.3 Verdeckte Erhebungen im Jugendzentrum Bingen

Im Januar 1993 wurden verdeckte Ermittlungen eines Beamten des polizeilichen Staatsschutzes in einem selbsverwalteten Jugendzentrum bekannt. Das Fachkommissariat des zuständigen Polizeipräsidiums vermutete in dem Jugendzentrum Angehörige der autonomen Szene, die möglicherweise als gewaltsame Störer bei jeweils bevorstehenden Veranstaltungen rechtsextremistischer Kreise auftreten könnten. Ziel der Ermittlungen waren insbesondere Erkenntnisse über die Anzahl der an evtl. Störungen Beteiligten aus dem Jugendzentrum und über deren nähere Absichten. Zu diesem Zweck besuchte ein Polizeibeamter im Laufe der Monate August bis Dezember 1992 insgesamt 14mal aus verschiedenen Anlässen eine Sonntagsveranstaltung des Jugendzentrums „Antifa-Cafe", die jedermann zugänglich war und bei der über Rechtsextremismus im allgemeinen und in der Region Rheinhessen im besonderen diskutiert wurde. Während der Veranstaltungen lagen auf einem Tisch verschiedene Schriften zu dem Thema aus. Der Beamte gab sich als solcher nicht zu erkennen, verwendete aber keine Legende. Er gab seinen richtigen Vornamen an, vermied jedoch die Nennung seines Nachnamens oder weiterer Identifikationsmerkmale und beteiligte sich an den Diskussionen derart, daß Zweifel an einer normalen Gruppenzugehörigkeit nicht aufkamen.

Die weiteren Teinehmer kannte der eingesetzte Beamte weitgehend mit den Vornamen. Neben dem sonntäglichen „Antifa-Cafe" wurden auch „Mitarbeiterbesprechungen" an jeweils einem bestimmten Wochentag besucht.

Die datenschutzrechtliche Überprüfung im Polizeipräsidium ergab zunächst das fast vollständige Fehlen schriftlicher Unterlagen über diesen Einsatz, aus denen Ziele und Grenzen des Auftrags nachvollziehbar hervorgegangen wären. Vorhanden waren lediglich einige genehmigte Dienstreiseanträge, aus denen unter der Rubrik „Erläuterung des Dienstgeschäfts" mit wechselnden Formulierungen hervorging, daß es jeweils um „Verdeckte Aufklärung bei einer Veranstaltung der ‚Autonomen Antifa' " in dem Jugendzentrum ging. Die gewonnenen Erkenntnisse wurden ohne die Nennung von Personennamen allgemein an die entsprechend betroffenen Polizeistellen per Fernschreiben weitergegeben.

Aus der Sicht des Datenschutzes ist es von entscheidender Bedeutung, daß hier das Grundrecht der Versammlungsfreiheit tangiert wird. Gesondert zu werten ist, daß Versammlungen in geschlossenen Räumen dem in Artikel 8 Abs. 2 GG normierten Gesetzesvorbehalt im Grundsatz nicht unterliegen.

Die Polizei hätte den Versammlungscharakter der von ihr selbst als „Veranstaltungen" bezeichneten Zusammenkünfte erkennen und in ihre Abwägung einbeziehen müssen. Die Zusammenkünfte in dem Jugendzentrum dienten einem verbindenden politischen Zweck, waren zeitlich bestimmt und begrenzt sowie öffentlich zugänglich; sie dienten der kollektiven Willensbildung, waren Ausdruck gemeinschaftlicher, auf Kommunikation angelegter Entfaltung. Generell ist davon auszugehen, daß Artikel 8 unabhängig von einfachgesetzlicher Normierung auch sonstige Beeinträchtigungen der Versammlungsfreiheit grundsätzlich für unzulässig erklärt, insbesondere die staatliche Aufsicht für einzelne Versammlungen, Bespitzelung u. ä. (siehe hierzu Herzog in Maunz-Dürig, Komm. z. GG, RdNr. 87 zu Artikel 8).

Vor diesem Hintergrund kann es dahinstehen, ob im einzelnen Besuchsfall das Versammlungsgesetz oder das Polizeiverwaltungsgesetz anzuwenden war. § 12 a des Versammlungsgesetzes nennt zwar nur Eingriffe durch Bild und Ton, schließt aber eingriffsschwächere Maßnahmen wie Beobachtung und Belauschung ohne Verwendung technischer Mittel nicht aus, wenn sie unter den gleichen tatbestandlichen Voraussetzungen erfolgen (Dietel/Gintzel/Kniesel, Demonstrations- und Versammlungsfreiheit, Komm. zum Versammlungsgesetz, Bem. 8 zu § 12 a). Danach müssen tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß von den Teilnehmern erhebliche Gefahren für die öffentliche Sicherheit ausgehen, wobei offenbleiben konnte, ob

es ausreicht, wenn die Gefahren für einen Zeitpunkt außerhalb der konkreten Versammlung angenommen wurden. Sowohl in diesen Fällen wie auch bei Anwendung des § 25 a Abs. 2 Satz 1 PVG (Informationserhebung in verdeckter Form) ist jedoch der Grundsatz der Verhältnismäßigkeit unter Berücksichtigung der heimlichen Beobachtung von Versammlungen besonders streng zu beachten.

Art und Schwere des Eingriffs führen hier zu dem Ergebnis, daß der Einsatz insgesamt unverhältnismäßig war. Eingegriffen wurde sowohl in das Grundrecht auf Versammlungsfreiheit wie auch in das Recht auf informationelle Selbstbestimmung. Hierbei sind insbesondere die Feststellungen des Bundesverfassungsgerichts im Volkszählungsurteil über die angstfreie Teilnahme an politischen Veranstaltungen einzubeziehen. Auf dieser Grundlage wirkt die Ausforschung von 14 Zusammenkünften in dem gedrängten Zeitraum von nur vier Monaten unabhängig von den Absichten der Polizei im einzelnen im Blick auf die Teilnehmer wie eine Dauerbeobachtung.

Demgegenüber kann das Ziel, mehr Einzelerkenntnisse über geplante Straftaten und Störungen im Zusammenhang mit anderen bevorstehenden Veranstaltungen zu erhalten, nicht überwiegen, denn sowohl Zeit und Ort dieser Ereignisse wie auch die Gefahr gewalttätiger Störungen waren auch ohne die Erkenntnisse aus dem Jugendzentrum bekannt. Es konnte also nur um Einzelerkenntnisse gehen, die für die Gefahrenabwehr sicher von Bedeutung, jedoch nicht Voraussetzung waren.

Diese datenschutzrechtliche Beurteilung beschränkt sich auf die hier geschilderte besondere Fallgestaltung, die insbesondere durch die Wirkung der Maßnahme als praktisch permanente Beobachtung gekennzeichnet ist.

Die Beurteilung wurde dem Ministerium des Innern und für Sport kurze Zeit nach Bekanntwerden der Angelegenheit schriftlich mitgeteilt.

Der Minister des Innern und für Sport hat sich in seiner ausführlichen Stellungnahme vor dem Landtag dieser Auffassung im Kern angeschlossen.

Als Konsequenz aus der Sicht des Datenschutzes forderte der LfD, in geeigneter Weise – ggf. durch Dienstanweisung – sicherzustellen, daß Maßnahmen mit einer solchen Eingriffstiefe jederzeit sowohl für die zuständigen Aufsichtsbehörden wie auch für die datenschutzrechtliche Kontrolle nachvollziehbar bleiben. Hierzu wäre es erforderlich, die entsprechenden dienstlichen Aufträge schriftlich kurz niederzulegen sowie möglichst konkret und präzise zu fassen. Auch müßte nach Abschluß der Maßnahme eine entsprechende schriftliche Dokumentation erfolgen.

Weiterhin sollten bis zur anstehenden grundlegenden Novellierung der Bestimmungen des POG über die Informationsverarbeitung Verwaltungsbestimmungen über nähere Voraussetzungen für die in Frage kommenden besonderen Arten von verdeckten Erhebungen erarbeitet werden.

Das Ministerium des Innern und für Sport hat wenige Wochen nach dem Bekanntwerden der Angelegenheit auf die Vorschläge des LfD reagiert und in einer umfassenden Anleitung die mit entsprechenden Einsätzen befaßten Polizeistellen über die dabei auftretenden datenschutzrechtlichen Problemstellungen informiert; sie wurden u. a. detailliert angewiesen, Aufgaben und Durchführung sowie die hierzu führenden rechtlichen Überlegungen und für die Abwägung maßgebenden Umstände nachvollziehbar zu dokumentieren.

5.4 Einsatz verdeckter Ermittler

Bei örtlichen Feststellungen im Landeskriminalamt wurde der Datenschutz beim Einsatz sog. „verdeckter Ermittler" nach § 25 b PVG im Jahre 1992 überprüft. Die hierfür erforderlichen Unterlagen waren – sofern nicht bereits im LKA vorhanden – auf Wunsch des LfD dort von den zuständigen Stellen zusammengeführt worden. In allen Fällen ging es um die vorbeugende Bekämpfung der in § 25 b Abs. 1 Ziff. 2 PVG aufgeführten Katalogstraftaten. Die Maßnahmen konnten von der Schwere der zu erwartenden Tatvorwürfe wie von der Notwendigkeit der besonderen Informationserhebung her durchweg als verhältnismäßig angesehen werden. Die materiellen Gründe für die Anordnung der Maßnahmen im einzelnen waren anhand der vorhandenen Unterlagen in ausreichendem Maße rekonstruierbar.

Die Überprüfung konzentrierte sich sodann auf diejenigen Fälle, in denen wegen Gefahr im Verzuge in Anwendung von § 25 b Abs. 1 Ziff. 2, Satz 2 i. V. mit § 21 Abs. 1 Satz 1 PVG die ansonsten vorgeschriebene richterliche Anordnung nicht eingeholt und die Maßnahme von der Exekutive selbst angeordnet worden war. In diesen Fällen lagen entsprechende Anordnungen des Präsidenten des LKA vor. Typische Schwierigkeiten bestehen bei solchen Einsätzen, die Landesgrenzen überschreiten. Die Voraussetzungen für das Tätigwerden eines verdeckten Ermittlers richten sich nach dem Recht des Landes, in das er sich begibt. Die dortige Polizei trägt die Verantwortung für das Vorliegen der Voraussetzungen und muß die richterliche Anordnung einholen oder bei Gefahr im Verzuge die Maßnahme selbst anordnen. Durch die Kommunikationswege zwischen dem verdeckten Ermittler und seiner „Heimatbehörde" sowie auch zwischen dieser und der anordnenden Stelle kann je nach Lage des Einzelfalles die verbleibende disponible Zeit die Einholung der richterlichen Entscheidung nicht mehr zulassen.

Gefahr im Verzuge besteht, wenn die richterliche Anordnung nicht eingeholt werden kann, ohne daß der Zweck der Maßnahme gefährdet wird (vgl. Kleinknecht/Meyer, Komm. z. StPO, 40. Aufl., Bem. 6 zu § 98, m. w. N.). Die Überprüfung, einschließlich der Befragung der zuständigen Beamten, ergab auch insoweit keinen Grund zur Beanstandung.

Da der Einsatz verdeckter Ermittler ohnehin regelmäßig zu besonders schweren Eingriffen in das Recht auf informationelle Selbstbestimmung führt, sind dann, wenn er ohne richterlichen Beschluß angeordnet wird, besondere Anforderungen, insbesondere an die Nachvollziehbarkeit der Gründe, zu stellen. Das Ministerium des Innern und für Sport wurde daher gebeten, in geeigneter Weise dafür zu sorgen, daß nicht nur die materiellen Voraussetzungen für den Einsatz, sondern auch die speziellen Gründe für die Annahme von Gefahr im Verzuge schriftlich festgehalten werden. Die Anordnung soll in diesem Fall dem Behördenchef vorbehalten bleiben.

Das Ministerium des Innern und für Sport hat daraufhin die rechtliche und tatsächliche Problematik bei der polizeilichen Vorfeldarbeit zum Gegenstand eines umfassenden Rundschreibens an die in Frage kommenden Polizeistellen gemacht.

5.5 Organisierte Kriminalität; „Großer Lauschangriff"

Bei der Verabschiedung des Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität im Sommer 1992 wurde die Frage des Einsatzes technischer Mittel zur Informationserhebung in Wohnungen zurückgestellt. Der Bundestag hat auf Empfehlung des Rechtsausschusses (Bundestagsdrucksache 12/2720, S. 5) eine Entschließung gefaßt, wonach die damit „verbundenen schwierigen rechtlichen, insbesondere auch verfassungsrechtlichen Fragen im Rahmen der Beratungen des vorliegenden Gesetzentwurfs nicht mit der erforderlichen Sorgfalt" geklärt werden konnten. Die Beratungen sollten nach der Sommerpause 1992 fortgeführt werden. Seitdem liegt die Initiative bei der Innenministerkonferenz. In Erwartung entsprechender gesetzgeberischer Schritte hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (bei Gegenstimme Bayerns) Anfang Oktober 1992 erneut an die Innenminister und an den Bundestag gewandt und sich gegen den „Lauschangriff" auf Privatwohnungen für Zwecke der Strafverfolgung ausgesprochen. Die Datenschutzbeauftragten betonten dabei ausdrücklich, daß sie die Gefahren, die das organisierte Verbrechen für die Opfer und auch für die Demokratie und den Rechtsstaat heraufbeschwört, sehr ernst nehmen. Eine Abwägung zwischen den Verfolgungsinteressen und dem Schutz der Persönlichkeitsrechte der Bürger dürfe jedoch nicht eine „Wahrheitserforschung um jeden Preis" zum Ergebnis haben.

Um sich dringenden Notwendigkeiten der Strafverfolgung nicht zu verschließen, halten es die Datenschutzbeauftragten aber für zulässig, unter Abänderung des geltenden Wohnungsbegriffs die technische Informationsgewinnung aus solchen Räumen zu regeln, die allgemein zugänglich sind oder beruflichen oder geschäftlichen Tätigkeiten dienen, wie etwa die Hinterzimmer von Gaststätten, Spielcasinos, Saunaclubs oder Bordellen. Dies wird für hinnehmbar gehalten, wenn die Regelung auf einen abschließenden Straftatenkatalog eng begrenzt wird. Außerdem sollten die gewonnenen Erkenntnisse präzisen Verwendungsbeschränkungen (z. B. Aufklärung von Katalogtaten) unterliegen. Die Eingriffe dürften nur vom Richter angeordnet werden.

Der dargestellten grundsätzlichen Ablehnung liegt im wesentlichen die auf das Mikrozensus-Urteil des Bundesverfassungsgerichtes (BVerfGE 27, 1,6) gestützte Auffassung zugrunde, wonach die heimliche Informationsbeschaffung aus Wohnungen mit technischen Mitteln den Kernbereich der Artikel 2 und 13 des Grundgesetzes berührt. Wer die Wohnung für fremde Ohren öffne, öffne den innersten Raum privater Existenz und damit auch das Innere des Menschen, der dort wohne (so der Hessische Datenschutzbeauftragte, Prof. Dr. Hassemer, in der Deutschen Richterzeitung 1992, S. 358).

In der Zwischenzeit hat sich auch die Erkenntnis durchgesetzt, daß eine gesetzliche Zulassung der heimlichen Informationsgewinnung aus Wohnungen mit technischen Mitteln nur durch eine Änderung des Grundgesetzes möglich ist. Artikel 13 GG bestimmt in Absatz 1: „Die Wohnung ist unverletzlich". Abgesehen von der Regelung für Durchsuchungen in Absatz 2 bestimmt Absatz 3 für andere Eingriffe und Beschränkungen zweierlei: Zur Abwehr einer gemeinen Gefahr oder einer Lebensgefahr für einzelne Personen wird eine unmittelbare Eingriffsermächtigung erteilt. Zur Verhütung dringender Gefahren für die öffentliche Sicherheit und Ordnung sind Eingriffe und Beschränkungen aufgrund eines Gesetzes zulässig, insbesondere für bestimmt bezeichnete, hier aber nicht einschlägige Bereiche. Auf dieser Grundlage haben verschiedene Länder Bestimmungen über den Einsatz technischer Mittel zur Datenerhebung aus Wohnungen als präventive Maßnahme in ihren Polizeigesetzen getroffen, darunter das Land Rheinland-Pfalz (§§ 25b, 20 f. POG). Diese Ermächtigung kann aber wegen ihrer Beschränkung auf präventive Maßnahmen nicht für entsprechende Erhebungen aus Wohnungen im Rahmen strafrechtlicher Ermittlungsverfahren herangezogen werden. Dies ist – wie bereits gesagt – in rechtsstaatlich einwandfreier Weise nur zusammen mit einer Änderung des Grundgesetzes möglich.

Soweit sich die Rechtslage in den wichtigsten EG-Staaten übersehen läßt, ist die akustische Überwachung in Privaträumen überwiegend nicht durch spezielles Gesetz oder überhaupt gesetzlich geregelt. Dies geschieht zumeist in Erlassen oder durch Einführung strafrechtlicher Rechtfertigungsgründe. Im Grundsatz scheint die Informationsbeschaffung mit technischen Mitteln aus Wohnungen ohne Kenntnis der Betroffenen für die Sicherheitsorgane überwiegend erlaubt zu sein, wenn das auch

tatsächlich als letztes Mittel maßvoll praktiziert wird. Überall ist die Maßnahme – auf welcher Rechtsgrundlage auch immer – auf die Verfolgung besonders schwerer Delikte beschränkt. Zumeist wird die Anordnung durch den Richter vorausgesetzt. In einigen Ländern bestehen Überlegungen, die entsprechenden Eingriffsbefugnisse der Sicherheitsbehörden nunmehr gesetzlich zu regeln. Die Rechtssituation in unseren Partnerländern wird in der weiteren Diskussion angesichts der anstehenden vielfältigen Kooperation insbesondere zur Bekämpfung der organisierten Kriminalität nicht völlig außer Betracht bleiben können.

In diesem Zusammenhang ist zu erwähnen, daß in der Praxis der Strafverfolgung in Deutschland häufig eine sog. „Gemengelage" entsteht, in der eine konkrete Maßnahme der polizeilichen Informationsbeschaffung sowohl präventiven wie repressiven Zwecken dient. Meistens wird es aber so sein, daß – insbesondere bei Bekämpfung der organisierten Kriminalität – regelmäßig bereits ein Anfangsverdacht im Sinne der Strafprozeßordnung vorliegt, so daß korrekterweise eine Maßnahme nur auf deren Bestimmungen gestützt werden kann, was bedeutet, daß die vorhandenen gesetzlichen Ermächtigungen in den Polizeigesetzen praktisch ausscheiden.

Eine andere Rechtslage besteht für den Verfassungsschutz in Bund und Ländern, der kein Instrument der Strafverfolgung ist. Die Informationsbeschaffung mit technischen Mitteln aus Wohnungen ist – sofern und soweit zugelassen – hier ein „nachrichtendienstliches Mittel". Schon wegen der unterschiedlichen gesetzlichen Voraussetzungen hält es der LfD aus der Sicht des Datenschutzes für unvertretbar, den Verfassungsschutz – wie z. Z. teilweise erwogen – mit der sog. „Vorfeldbeobachtung" der organisierten Kriminalität zu betrauen (vgl. unten Nr. 6.3).

Nicht zuletzt warnt der LfD davor, im sog. Großen Lauschangriff das entscheidende Mittel im Kampf gegen die organisierte Kriminalität zu sehen. Diesem Phänomen kann nicht nur durch Polizei und Justiz begegnet werden. Notwendig ist vielmehr eine konzertierte Aktion, die von der Unterbindung der Geldwäsche bis zu bestimmten sozialen Maßnahmen reicht.

5.6 Arbeitsgruppe Asylbetrug der Polizei Rheinland-Pfalz

Bundesweite Beachtung hat das vom Ministerium des Innern und für Sport entwickelte und erfolgreich in die Praxis umgesetzte Modell einer polizeilichen „Arbeitsgruppe zur Verhinderung des Mißbrauchs des Asylrechts (AG Asylbetrug)" gefunden, die zunächst bei der ZAST in Ingelheim die Arbeit aufnahm. Da potentielle „Asylbetrüger" aufgrund schnell und weiträumig einsetzender Mundpropaganda ihre Chancen reduziert sahen, unerkannt aufgenommen zu werden, war schon bald ein deutlicher Rückgang der Asylbewerberzahlen in Rheinland-Pfalz im Jahre 1992 zu verzeichnen. Die Aufgaben der AG Asylbetrug wurden von Anfang an von denen der im Bereich der ZAST sonst allgemein tätigen Vollzugspolizei strikt getrennt. Im einzelnen obliegt es der Arbeitsgruppe, Verstöße gegen das Asylverfahrensgesetz und das Ausländergesetz zu bearbeiten, die im Zusammenhang mit Personenüberprüfungen bekannt werden. Solche Personenüberprüfungen werden systematisch im engeren und weiteren Umfeld der ZAST durchgeführt, um auf diese Weise Anhaltspunkte zur Identitätsfeststellung, zum Reiseweg und zu „Schleusern" zu gewinnen. Weiterhin sind durch die AG alle Delikte zu bearbeiten, die im Zusammenhang mit Doppel- und Mehrfachidentitäten bekannt werden.

Die datenschutzrechtlichen Feststellungen konzentrierten sich auf die Kriterien für die Gewinnung des Anfangsverdachts im Einzelfall sowie die damit im Zusammenhang stehenden und folgenden Erhebungen. Nach Darstellung der Polizei stützt sich der Anfangsverdacht im überwiegenden Teil der eingeleiteten Ermittlungsverfahren auf Meldungen des BKA über Mehrfachidentitäten, die durch konkrete Anfragen der Ausländerbehörde veranlaßt sind. Weitere Ermittlungsansätze ergeben sich bei Durchsuchungen, wenn andere Ausweispapiere gefunden werden, die von der bei Antragstellung vorgegebenen Identität abweichen oder wenn sich Hinweise auf den Aufenthalt in anderen Asylunterkünften wie Schlüssel oder Hausausweise finden. Durchsuchungsanlaß sind in der Regel Indizien, wie hochwertige Kleidung und Gegenstände, die auf Einkommen neben der einfachen Sozialhilfe schließen lassen. Hinzu kommen Hinweise über die Beobachtung von Verhaltensweisen, die für den Gebrauch von Mehrfachidentitäten und den Mehrfachbezug von Sozialleistungen typisch sind.

Im Rahmen der auf den Anfangsverdacht folgenden Ermittlungen werden die durch evtl. Sozialhilfebetrug geschädigten Gebietskörperschaften festgestellt und um schriftliche Auskunft über den Schadensumfang ersucht. Nötigenfalls werden die Anschriften von entsprechenden Betroffenen aus den Unterlagen der ZAST erbeten, um so an die geschädigten Gebietskörperschaften zu kommen.

Aus datenschutzrechtlicher Sicht war zunächst die Berechtigung der ZAST zur Übermittlung oder Offenbarung der Anschrift zu klären. Finden etwa die bereichsspezifischen Bestimmungen über das Sozialgeheimnis in den § 35 des SGB I und in den §§ 67 ff. des SGB X Anwendung? Die ZAST ist jedoch kein Leistungsträger im Sinne des § 35 Abs. 1 SGB I; soweit sie als Nebenaufgabe unterhaltswirksame Leistungen, wie kurzfristige Unterkunft, Verpflegung und Taschengeld, erbringt, wendet sie nach der LVO über die zentrale Anlaufstelle für Asylbewerber vom 2. Juli 1984 das BSHG nicht unmittelbar, sondern ausdrücklich nur „sinngemäß" an. Hauptaufgabe bleibt die Verteilung der Asylbewerber auf die Kommunen. Auf Übermittlungen durch die ZAST ist daher das LDatG anzuwenden. Wegen der Rechtmäßigkeit der Aufgabenerfüllung durch die AG Asylbetrug, ergibt sich die Zulässigkeit der Anschriftübermittlung zweifelsfrei aus dessen § 6 Abs. 1. Eine Anwendung des SGB würde

überdies zu keinem anderen Ergebnis führen, denn § 68 Abs. 1 SGB X läßt die Offenbarung der Anschrift des Betroffenen im Wege der Amtshilfe ausdrücklich ohne richterliche Entscheidung zu.

Das gilt übrigens auch für die Offenbarung der an beschuldigte Asylbewerber gezahlten Sozialhilfe durch die Träger. Auch hierfür ist keine richterliche Anordnung erforderlich. Anstelle des § 73 ist § 69 Abs. 1 Ziff. 1, 1. Alternative SGB X, anzuwenden. Danach ist die Offenbarung zulässig, wenn und soweit sie erforderlich ist für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch, d. h. einer eigenen Aufgabe des Trägers der Sozialhilfe. Hierzu zählen die Verhinderung des Mißbrauchs im Einzelfall, seine Aufklärung und der Ersatz. Die offenbarende Behörde wird nach Mitteilung des Verdachts durch die Polizei in eigener Aufgabenerfüllung und aufgrund eigenen Entschlusses tätig.

In der Zwischenzeit sind entsprechende Arbeitsgruppen auch in Trier und Neustadt/Weinstr. eingerichtet worden.

5.7 „Fremdenfeindlich" als personengebundener Hinweis (PHW)

Nach einem Beschluß der Innenministerkonferenz wird bundesweit für Speicherungen in INPOL einschließlich KAN (Kriminalaktennachweis) und APIS (Arbeitsdatei PIOS-innere Sicherheit) der Katalogbegriff „fremdenfeindlich" eingeführt und auch als PHW (personenbezogener Hinweis) verwendet, letzterer auch in den INPOL-Dateien „Personenfahndung" und „Erkennungsdienstliche Unterlagen". Betroffen sind Täter oder Verdächtige wegen Taten, die aus intoleranter Haltung heraus gegen Personen begangen wurden, denen die Täter aufgrund Nationalität, Volkszugehörigkeit, Rasse, Hautfarbe, Weltanschauung, Herkunft oder aufgrund ihres äußeren Erscheinungsbildes ein Bleiberecht in ihrer Wohnumgebung oder in Deutschland bestreiten. Einbezogen sind auch Handlungen gegen sonstige Personen, Einrichtungen und Sachen aus fremdenfeindlichen Motiven. Die bundesweiten Richtlinien für die kriminalpolizeilichen Meldedienste in Staatsschutzsachen wurden entsprechend ergänzt.

Der LfD wurde durch das Ministerium des Innern und für Sport frühzeitig beteilgt. Angesichts aller Umstände hat es der LfD nicht als Ziel des Datenschutzes angesehen, die Polizei durch zu hohe datenschutzrechtliche Anforderungen an der Beschaffung von Informationen zu hindern, die zur wirksamen Bekämpfung des Rechtsextremismus erforderlich sind.

Das Ministerium des Innern und für Sport hatte schon zu einem wesentlich früheren Zeitpunkt für Rheinland-Pfalz eine eigene POLDOK-Datei „fremdenfeindliche Kriminalität" zur Erfassung von „Straftaten, die bewußter Ausdruck von Fremdenfeindlichkeit sind" eingerichtet und auch hierbei den LfD beteiligt. Dabei konnten verschiedene Präzisierungen im Sinne des Datenschutzes erreicht werden, ohne das mit der Maßnahme verfolgte Ziel zu beeinträchtigen; sie betrafen im wesentlichen die erheblich kürzere und umfassendere Definition des Dateianlasses sowie die Begrenzung von Datenverarbeitungen auf diesen, auch eine jährliche Überprüfung der weiteren Erforderlichkeit der Datenverarbeitung im Einzelfall.

5.8 Neuere Entwicklungen bei der polizeilichen Videoüberwachung von Versammlungen

Aus konkretem Anlaß war die Frage der rechtlichen Behandlung von sog. „Übersichtsaufnahmen" zu klären, die zu reinen Dokumentationszwecken erfolgen, also nicht der Fertigung von Bildern einzelner Personen dienen. Unterliegen sie besonderen – leichteren – Zulässigkeitsvoraussetzungen? Hierzu ist zunächst festzuhalten, daß nach dem derzeitigen Stand der Technik die Unterscheidung zwischen Übersichtsaufnahmen und gezielten Aufnahmen nicht mehr tauglich ist, da auch aus Übersichtsaufnahmen Bilder von Einzelpersonen ohne besondere Schwierigkeiten herausvergrößert werden können. Nach einer vom OVG Bremen in seinem Urteil vom 24. April 1990 (NJW 1990, 1188 ff.) vertretenen Auffassung stellt die optische Dokumentation einer Demonstration eine Erhebung personenbezogener Daten dar, und zwar unabhängig davon, ob Übersichts- oder Einzelaufnahmen angefertigt werden. Dieser Auffassung ist in Übereinstimmung mit dem Ministerium des Innern und für Sport beizutreten. In den §§ 19 a und 12 a des Versammlungsgesetzes findet sich für die Datenerhebung zum Zwecke der bloßen Dokumentation (ohne Zweckbestimmung zur Gefahrenabwehr) kein Anhaltspunkt für eine gesonderte Beurteilung. Demnach dürfen die Aufnahmen bei oder im Zusammenhang mit öffentlichen Versammlungen nur angefertigt werden, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß von diesen erhebliche Gefahren für die öffentliche Sicherheit und Ordnung ausgehen. Gleiches gilt bei Versammlungen unter freiem Himmel und Aufzügen.

In diesem Zusammenhang war auch der Einsatz von Videokameras ohne Videoband, die gleichsam als Sichthilfen eingesetzt werden, zu beurteilen. Hier geht es primär nicht um den Gesichtspunkt der Datenerhebung und -speicherung, sondern um die innere Versammlungsfreiheit. Das Bundesverfassungsgericht hatte im Volkzählungsurteil u. a. gefordert, daß Versammlungsteilnehmer grundsätzlich nicht befürchten sollen, Objekt von Überwachung und Aufzeichnung zu werden. Gerade die „abschreckende" Wirkung des Kameraeinsatzes und nicht erst die Datenerhebung und -speicherung stellt in diesem Sinne den Eingriff in das Grundrecht dar. Ob dieser Konflikt dadurch gelöst werden kann, daß im Rahmen der zwischen Polizei und Veranstalter gebotenen Kooperation Hinweise auf die fehlende Aufzeichnung gegeben werden, erscheint fraglich.

Schließlich geht es um die datenschutzrechtliche Bewertung von Videokameras, die ständig zu Zwecken der Verkehrsüberwachung installiert sind, wenn auf den Straßen Demonstrationen stattfinden. Hier wird man davon ausgehen können, daß bei

derartiger „Vorbelastung" der öffentlichen Verkehrswege noch kein Eingriff darin zu sehen ist, wenn die Verkehrsüberwachungskameras ohne Aufzeichnungen während der Demonstration angeschaltet bleiben. Werden die Kameras allerdings zur Aufzeichnung geschaltet, müßten hierfür die genannten gesetzlichen Voraussetzungen vorliegen.

5.9 Abgleich mit Arbeitnehmerdaten

Ein Vorgang beschäftigte in den Monaten Februar und März 1992 wochenlang die Öffentlichkeit und den Landtag. Der Werkschutz der BASF hatte über einen längeren Zeitraum dem Polizeipräsidium Ludwigshafen monatlich bis zu dreihundert Kopien von Karteikarten überlassen, die die Namen, Adressen, das Geburtsdatum und den Arbeitgeber der Mitarbeiter von Firmen enthielten, die auf dem Werksgelände der BASF Arbeiten verrichteten (sog. „Fremdfirmen"). Es handelte sich dabei um Kopien von Werksausweisen für die Dauer der Tätigkeit auf dem Firmengelände. Die Kopien wurden gebündelt in Umschlägen beim Werkschutz der Firma bereitgehalten und von Beamten des Polizeipräsidiums regelmäßig abgeholt. Im Polizeipräsidium wurden die Daten durch Abgleich mit dem polizeilichen Informationssystem überprüft, um Personen festzustellen, die zur Fahndung oder zur Aufenthaltsermittlung ausgeschrieben waren. Ergaben sich Treffer zur Festnahme, so wurde der Werkschutz eingeschaltet, wenn diese nur auf dem Werksgelände möglich war. Soweit die Abfrage negativ verlief, wurden die Kopien spätestens nach einem Zeitablauf von vier Wochen vernichtet. Die vom Ministerium des Innern und für Sport geführten Ermittlungen sowie die unabhängig hiervon selbständig getroffenen örtlichen Feststellungen des LfD beim Polizeipräsidium wie auch bei der Staatsanwaltschaft Frankenthal haben keine Hinweise darauf ergeben, daß über die genannten Festnahmefälle hinaus von dem Ergebnis der Abgleiche Rückmeldungen an die BASF erfolgten. Die geschilderte Praxis wurde vom Polizeipräsidenten sofort nach Bekanntwerden unterbunden.

Im Zusammenhang mit der Ermittlung dieser Vorgänge ergaben sich Hinweise auf andere unzulässige Datenverarbeitungen auch durch Polizeibeamte. Soweit erforderlich, wurde Strafantrag nach § 27 LDatG gestellt. Die Vorgänge sind jedoch für die Beurteilung der oben dargestellten Zusammenarbeit zwischen Polizei und BASF nicht relevant.

Die in dem fraglichen Zeitraum bestehenden Kontakte der BASF mit dem Verfassungsschutz sind, soweit feststellbar, nicht durch eine institutionalisierte, regelmäßige Abgleichspraxis ganzer Personalbereiche gekennzeichnet gewesen. Datenübermittlungen finden anlaßbezogen in unterschiedlicher Form statt und sind in jedem einzelnen Fall gesondert datenschutzrechtlich zu beurteilen.

Die öffentliche Diskussion der Angelegenheit hat zu einer Reihe von Eingaben besorgter Bürger geführt, denen der LfD einzeln sowohl für den Bereich der Polizei wie auch beim Verfassungsschutz nachgegangen ist.

Der stattgefundene regelmäßige Abgleich der von der BASF erhaltenen Kopien war datenschutzrechtlich unzulässig. Diese Praxis konnte weder auf das Polizeiverwaltungsgesetz noch etwa auf die Strafprozeßordnung oder andere Rechtsvorschriften gestützt werden. Die einschlägige Bestimmung des § 25 a PVG setzt bestimmte Zwecke voraus, nämlich die Abwehr einer im Einzelfall bestehenden Gefahr oder die vorbeugende Bekämpfung von Straftaten. Von konkreten Gefahren (Einzelfall) ist in dem zu beurteilenden Zusammenhang nichts bekannt. Aber auch zur vorbeugenden Bekämpfung von Straftaten konnten die Daten nicht genutzt werden, da es sich nicht um die Sammlung und Auswertung bereits aus kriminalpolizeilichen Vorgängen stammender Informationen zur künftigen leichteren Aufklärung von Straftaten handelte.

Ein weiterer Aspekt verdient Beachtung: Bei den regelmäßig von der BASF zur Verfügung gestellten Daten der Arbeitnehmer von auf ihrem Gelände arbeitenden Fremdfirmen handelt es sich um „Informationsbestände bestimmter Personengruppen", für deren Abgleich mit anderen Informationsbeständen (Rasterfahndung § 25 d PVG – besondere Formen des Informationsabgleichs –) spezielle Voraussetzungen, nämlich die Erforderlichkeit zur Abwehr einer erheblichen gegenwärtigen Gefahr, gefordert sind. Die genannte Bestimmung regelt zwar unmittelbar nur das Recht der Polizei, zu dem bezeichneten Zweck von anderen öffentlichen und privaten Stellen die Übermittlung von Informationsbeständen zu verlangen. Es ist aber unschwer die Absicht des Gesetzgebers zu erkennen, den Eingriff in das Grundrecht einer Vielzahl unbeteiligter Personen auf ein möglichst enges Maß zu beschränken. Es kann daher bei Beachtung der vom Bundesverfassungsgericht zum Recht auf informationelle Selbstbestimmung aufgestellten Grundsätze keinen Unterschied machen, ob die Informationsbestände auf Verlangen der Polizei oder freiwillig von der BASF herausgegeben worden sind, weil sich zumindest durch das anschließende Handeln der Polizei der Grundrechtseingriff für die betroffenen Unbeteiligten in gleicher Weise darstellt. Ebensowenig konnten die Voraussetzungen für Ermittlungen auf der Grundlage der Strafprozeßordnung angenommen werden. Auch insoweit wären die oben dargestellten Überlegungen anzustellen gewesen.

Als wichtigste Konsequenz aus den bei den durchgeführten Feststellungen und anschließend andernorts gesammelten Kontrollerfahrungen wurde vom LfD die Zusatzprotokollierung bei Abfragen aus POLIS gefordert und nach näherer Absprache vom Ministerium des Innern und für Sport landesweit eingeführt (vgl. Tz. 5.10). Darüber hinaus ist der Komplex ein weiterer Beweis für die Notwendigkeit, die Tätigkeit privater Sicherheitsdienste, zu denen auch der Werksschutz von Industrieunternehmen gehört, bundesgesetzlich zu regeln.

Die Vielzahl ehemaliger Polizeibeamter bei diesen Einrichtungen und die damit erhöhten Gelegenheiten einvernehmlichen Zusammenwirkens bilden im Sinne des Datenschutzes eine faktische Gefahrenquelle, der zuerst mit normenklaren Regelungen zu begegnen ist.

Für den Bereich des Verfassungsschutzes ergibt sich die Notwendigkeit präziserer Regelungen in dem alsbald zur Novellierung anstehenden Landesverfassungsschutzgesetz. Speziell für die hier interessierenden Übermittlungen an Private muß deren Einzelfallcharakter noch deutlicher werden. Die schon jetzt vorgeschriebene Zustimmung des Ministers sollte nur im Verhinderungsfalle und nur durch seinen Vertreter ersetzt werden können. Außerdem sollte für jeden Übermittlungsfall ein gesondert aufzubewahrender Nachweis mit allen für die Überprüfung der Rechtmäßigkeit erforderlichen Angaben vorgeschrieben werden.

5.10 Lückenlose Kontrolle von Polis-Abfragen durch Zusatzprotokollierung

Wie bekannt, unterhalten die Polizeien des Bundes und der Länder ein gemeinsames, arbeitsteiliges elektronisches Informationssystem INPOL, in dem ihre IT-Einrichtungen im Verbund zusammenwirken. Für Rheinland-Pfalz besteht das polizeiliche Informationssystem POLIS, das gleichzeitig Landesbestandteil von INPOL ist.

Als polizeiinternes Arbeitsmittel enthält POLIS personenbezogene Daten von erheblicher Sensitivität. Der noch nicht erhärtete Verdacht findet sich ebenso wie Fahndungs- und Haftdaten, Hinweise auf vorhandene Kriminalakten, Personenbeschreibungen und Hinweise auf erfolgte erkennungsdienstliche Behandlungen. Es versteht sich von selbst, daß die Verarbeitung derartiger z. T. „weicher" Daten einen Eingriff in die Persönlichkeitssphäre des einzelnen darstellt und daher nur auf rechtlich einwandfreier Grundlage erfolgen darf. Im datenschutzrechtlichen Sinne gehören hierzu auch wirksame Sicherungen. Eine davon ist die Möglichkeit lückenloser Kontrolle.

Zu diesem Zweck wurde bereits in der Vergangenheit jede einzelne Abfrage für eine Zeitdauer bis zu zwei Jahren auf einem Logband protokolliert. Wie sich allerdings bei Kontrollen im Berichtszeitraum herausstellte, reicht die Kenntnis aller Abfragen über Einzelpersonen von einem Terminal während eines bestimmten Zeitraumes nicht aus. Sinn der Kontrolle kann es ja nur sein festzustellen, ob eine Abfrage aufgrund eines konkreten polizeilichen Vorgangs erfolgte und ob sie zu dessen ordnungsgemäßer Bearbeitung im Sinne des Gesetzes erforderlich war. Soweit dies aktenkundig ist, muß der entsprechende Vorgang beigezogen und anhand seines Inhalts die Erforderlichkeit geprüft werden.

Diese Prüfkette ist unterbrochen, wenn der im Zeitpunkt der Abfrage für das Terminal verantwortliche Beamte für einen anderen tätig geworden ist. Häufig kommen derartige Anforderungen aus Funkstreifenwagen, aus denen Direktabfragen in POLIS in der Regel nicht möglich sind. Abfragen werden aber auch in nicht unerheblichem Umfang für andere Stellen aus gesetzlich zugelassenen Anlässen getätigt. Kann sich der abfragende Beamte im Zeitpunkt der Prüfung wegen der Menge der täglichen Einzelvorgänge und wegen des Zeitablaufs nicht an seinen Auftraggeber oder den Anlaß erinnern, dann ist nicht mehr oder nur schwer feststellbar, ob die Anfrage zulässig war oder nicht.

Zur Schließung dieser Lücke wurde in Zusammenarbeit zwischen dem Ministerium des Innern und für Sport und dem LfD das System einer Zusatzprotokollierung entwickelt und mit Hilfe des LKA und des Landesrechenzentrums realisiert. Diese Maßnahme dient übrigens – wie vielfach übersehen wird – nicht nur der Kontrolle, sondern mindestens ebenso dem Schutz des Bedieners, denn rechtmäßiges Handeln und Verantwortlichkeiten werden nun nachweisbar.

Die Zusatzprotokollierung ist wie folgt realisiert:

- Bei jeder 20. Abfrage erfolgt automatisch am Bildschirm die Aufforderung zur Zusatzprotokollierung. Bis dahin ist jede weitere Abfrage unterbunden.
- Eine Zusatzprotokollierung ist laut Dienstanweisung darüber hinaus immer dann vorzunehmen, wenn im Auftrag eines anderen abgefragt wird.
- Jeder Bediener kann jederzeit von sich aus eine Zusatzprotokollierung vornehmen.
- Dies kann für bestimmte Terminals auch vom LKA auf Zeit oder auf Dauer angeordnet werden.

Bei der Zusatzprotokollierung ist der Anlaß nach einem Schlüssel anzugeben (Fahndungsüberprüfung, Personenüberprüfung, Verfahrenskontrolle u. a.). Erfolgt die Abfrage im Auftrag eines anderen, ist dieser voll identifizierbar anzugeben (z. B. Name mit Organisationseinheit oder Tagebuch-Nr. oder Aktenzeichen oder Rufname des Fahrzeugs).

Erweist sich eine Zusatzprotokollierung bei einzelnen Maßnahmen wegen des bekannten einheitlichen Abfragegrundes (z. B. bei Großkontrollstellen) als nicht erforderlich, kann das LKA Ausnahmen zulassen, denn die datenschutzrechtliche Nachvollziehbarkeit ist dann wegen der Besonderheit der Maßnahme ohnehin gegeben.

Die zusätzlichen Protokolldaten werden ein Jahr lang aufbewahrt.

Die Nutzung der Protokolldaten für andere als Kontrollzwecke ist nicht gestattet. Eine Ausnahme gilt für die Bekämpfung von Kapitaldelikten mit Genehmigung des Ministeriums im Einzelfall. Auch nach dem neuen LDatG soll dies nur insoweit möglich sein, als es zur Abwehr erheblicher Gefährdungen der öffentlichen Sicherheit, insbesondere für Leben, Gesundheit oder Freiheit, erforderlich ist.

Mit dieser Regelung hat Rheinland-Pfalz als erstes Bundesland in diesem Umfang die Nachvollziehbarkeit der Nutzung des polizeilichen Informationssystems im Sinne des Datenschutzes sichergestellt.

5.11 POLADIS

Auf die datenschutzrechtlichen Fragen bei der Vorgangsverwaltung POLADIS hatte der LfD bereits im 13. Tb. hingewiesen (Tz. 5.9). POLADIS ersetzt als dezentrales System die Registrierung und Dokumentation der polizeilichen Vorgänge u. a. in einer Vielzahl von unterschiedlichen Tagebüchern, Sammlungen und manuellen Dateien. Drei Monate nach Abschluß wird ein Vorgang für etwa fünf Jahre archiviert. Damit entsteht eine umfassende Datenbank, die jedenfalls theoretisch die Gefahr in sich birgt, daß ihre Daten auch zu anderen Zwecken als die der Vorgangsverwaltung verwendet werden, insbesondere zur Umgehung gesetzlicher Voraussetzungen, beispielsweise zu verkürzten Auskünften ohne Kenntnis des Akteninhalts oder als Ersatz einer protokollierbaren POLIS-Abfrage.

Die Regelung des Zugriffs auf die Archivdaten war bei Abfassung des 13. Tb. noch offen. Hier konnte erreicht werden, daß Abfragen der Archivdaten nur über das Geschäftszimmer der jeweiligen Polizeistelle, also nur über eine einzige Stelle erfolgen können. Der Veranlasser wird dort protokolliert. Auch die Vergabe der Berechtigung des Zugriffs wird protokolliert. Die Protokoll- oder Logdateien werden zwei Jahre aufgehoben, dann aber gelöscht.

Ein Polizeipräsidium handhabte die Regelung anfangs derart, daß der Geschäftszimmerbeamte die Abfrageersuchen schriftlich stellen ließ und sammelte, bis „genügend" viele davon vorlagen. Eine derartige Praxis ist geeignet, die Akzeptanz einer notwendigen datenschutzrechtlichen Maßnahme zu vermindern und trägt viel zu Vorurteilen gegenüber dem Datenschutz bei. Diese Verfahrensweise wurde rasch abgestellt.

5.12 Landesgesetz zur Änderung des Polizeiverwaltungsgesetzes Rheinland-Pfalz (PVG)

Im Zuge der Neuorganisation der Polizei und der damit verbundenen Entlastungen der Vollzugspolizei haben die bisherigen Ortspolizeibehörden eine stärker auf ihr Tätigkeitsgebiet zugeschnittene gesetzliche Grundlage erhalten; nachdem sie keine Polizeibehörden mehr sind, führen sie die Bezeichnung „allgemeine Ordnungsbehörden".

Die in den §§ 25 a ff. PVG geregelten Befugnisse der Polizei zur Informationsverarbeitung sind den allgemeinen Ordnungsbehörden entsprechend ihrer Aufgabenstellung nur begrenzt übertragen. So können sie die in § 25 a Absatz 1 PVG geregelten allgemeinen Befugnisse zur Informationsverarbeitung nur zur Abwehr von im Einzelfall bestehenden Gefahren, zum Schutz privater Rechte sowie zur Erfüllung von durch andere Gesetze übertragenen Aufgaben wahrnehmen, nicht hingegen zur vorbeugenden Bekämpfung von Straftaten und zur Vollzugshilfe. Die Übertragung der Eingriffsbefugnisse erfolgt insoweit durch den neu geschaffenen Absatz 1 a. Der LfD hatte in einer Anhörung vor dem Innenausschuß des Landtags angeregt, ergänzend zu bestimmen, daß die allgemeinen Ordnungsbehörden Abgleiche nur mit ihren eigenen Dateien, nicht hingegen auch mit den Dateien der Vollzugspolizei, wie z. B. INPOL, POLADIS oder mit POLDOK-Dateien, vornehmen dürfen. Dieser Klarstellung dient der im Innenausschuß angefügte Satz „Die allgemeinen Ordnungsbehörden können personenbezogene Daten mit dem Inhalt ihrer Dateien abgleichen, soweit gesetzlich nicht etwas anderes bestimmt ist." Eine weitere Wirkung ist mit der Regelung nicht beabsichtigt.

Nachdem in der Begründung der Regierungsvorlage erneut eine Korrektur der bereichsspezifischen datenschutzrechtlichen Regelungen des PVG in einer eigenen Gesetzesnovellierung nach der Neufassung des Landesdatenschutzgesetzes angekündigt wurde, hat der LfD von weiteren Änderungsvorschlägen abgesehen.

5.13 Novellierung der Informationsbestimmungen des Polizei- und Ordnungsbehördengesetzes

Das rheinland-pfälzische Polizeiverwaltungsgesetz (jetzt „Polizei- und Ordnungsbehördengesetz" – POG –) wurde im Jahre 1986 zu einem verhältnismäßig frühen Zeitpunkt aufgrund des Volkszählungsurteils des Bundesverfassungsgerichts um bereichsspezifische Regelungen über die Informationsverarbeitung ergänzt. Zwischenzeitlich haben sich sowohl die Praxis als auch die Anschauungen über den Datenschutz bei der Polizei weiterentwickelt, wie sich auch aus den später verabschiedeten Polizeigesetzen anderer Länder ergibt. Eine Reihe typischer Fallkonstellationen der Alltagsarbeit, wie z. B. die Gefahrenvorsorge, erfordern spezielle Regelungen im Gesetz.

Die Informationsbestimmungen im POG folgen in ihren materiellen Strukturen wie auch im weiteren Aufbau einer Systematik, die von anderen Ländern weitgehend nicht übernommen wurde. Letzteres erschwert nicht nur die Rechtsvergleichung und damit den bundesweiten Austausch von Erfahrungen und datenschutzrechtlichen Überlegungen, sondern dürfte sich behindernd in der länderübergreifenden Praxis auswirken. Schon von daher empfiehlt sich eine Neufassung der Bestimmungen über die polizeiliche Informationsverarbeitung.

Die notwendige Angleichung im systematischen Aufbau muß nicht notwendigerweise mit einer Änderung der allgemeinen Ermächtigungsregel des § 25 a POG in verschiedene Einzelermächtigungen für die verschiedenen Grundverarbeitungsphasen verbunden sein. Zum einen hat die Praxis in der Vergangenheit erwiesen, daß die genannte zusammenfassende Regelung dem in Rheinland-Pfalz erreichten vergleichsweise zufriedenstellenden Datenschutzstandard bei der Polizei nicht entgegenstand. Zum anderen hat sich allgemein gezeigt, daß auch durch die vollständige Enumeration Regelungen von einem textlichen Umfang entstehen, der sowohl der Akzeptanz durch die Praxis „vor Ort" im Wege steht als auch die vom Bundesverfassungsgericht ausdrücklich geforderte Transparenz für die Bürger erheblich vermindert. Die Systematik im übrigen sollte aber derjenigen in anderen Ländern stärker entsprechen.

Zusätzliche oder verbesserte Regelungen sind nach Auffassung des LfD u. a. in folgenden Punkten angebracht:

a) Die besonderen Formen des Datenabgleichs (sog. „Rasterfahndung") sind in ihren Voraussetzungen und im Anwendungsverfahren im Sinne einer rechtsstaatlichen Regelung weiter zu präzisieren (evtl. Aufzählung der in Frage kommenden Fallgruppen statt „erhebliche Gefahr") und die Maßnahme selber von einer vorherigen richterlichen Entscheidung wie bei Durchsuchungen und bei bestimmten „besonderen Informationserhebungen" (§ 25 b) abhängig zu machen, falls nicht Gefahr im Verzuge besteht.

b) Die Ausschreibung einer Person zur „Polizeilichen Beobachtung", damit andere Sicherheitsbehörden das Antreffen dieser Person oder ihres Fahrzeugs z. B. anläßlich einer Kontrolle melden können, ist ein schwerwiegender Eingriff in das Persönlichkeitsrecht des Betroffenen. Hierfür ist eine spezielle Befugnisnorm erforderlich, welche die Voraussetzungen und Modalitäten transparent und erschöpfend regelt. Hierzu gehören ebenso Regelungen hinsichtlich dabei angetroffener Kontakt- und Begleitpersonen einschließlich verkürzter Löschungsfristen, soweit deren Daten suchfähig in Dateien gespeichert werden.

c) Angesichts der z. Z. bestehenden Unklarheiten über die rechtliche Behandlung von Daten, die die Landespolizeien als Datenbesitzer in Verbunddateien eingestellt haben, sollte – wie andernorts bereits geschehen – gesetzlich bestimmt werden, unter welchen Voraussetzungen und Bedingungen mit anderen Ländern und dem Bund ein Datenverbund vereinbart werden kann.

d) Wegen der besonderen Bedeutung, die in Dateien gespeicherten Bewertungen schon wegen ihrer oft stark verkürzten Form zukommen kann, muß sowohl für die Behörden als auch für den Betroffenen nachvollziehbar sein, wer die Bewertung vorgenommen hat und bei welcher Stelle die entsprechenden Unterlagen geführt werden.

e) Auch die polizeiliche Vorgangsverwaltung und befristete Dokumentation, die derzeit durch POLADIS verwirklicht wird (vgl. Tz. 5.11), bedarf einer speziellen Ermächtigung, die aus der Befugnisnorm des § 25 a POG für die Vielzahl der vorkommenden Arten von Speicherungen nicht ohne weiteres hergeleitet werden kann. Dabei ist eine Nutzungsbeschränkung auf den Zweck der Datei vorzusehen.

f) Dies gilt auch für die Erhebung und Speicherung personenbezogener Daten zur Vorbereitung für die Hilfeleistung und das Handeln in Gefahrenfällen. Dabei geht es im wesentlichen um die Erreichbarkeit von Personen, deren Kenntnisse und Fähigkeiten zur Abwehr noch nicht eingetretener aber möglicher Gefahren benötigt werden, sowie von Verantwortlichen für Anlagen oder Einrichtungen, von denen erhebliche Gefahren ausgehen können oder die selbst gefährdet sind. Derartige Daten werden gegenwärtig z. B. in den Systemen ELIAS gespeichert.

g) In einer großen Zahl von Fällen müssen Ordnungsbehörden im Rahmen von Verwaltungsverfahren die Zuverlässigkeit von Personen überprüfen. Ob es um Erlaubnisse nach dem Gaststättengesetz oder gewerberechtliche Erlaubnisse und Versagungen nach der Gewerbeordnung geht, um Jagdscheine, waffenrechtliche Erlaubnisse, einschließlich derjenigen nach dem Sprengstoffgesetz oder um Fahrerlaubnisse, Fahrlehrererlaubnisse bis hin zur Ausgabe der sog. roten Kennzeichen: fast immer sind für die beurteilende Behörde Erkenntnisse aus dem Bereich der Polizei eine unverzichtbare Entscheidungshilfe.

Dem geltenden POG kann eine befriedigende Regelung dieser Fallgruppe nicht entnommen werden. Der Komplex muß aus der Sicht der polizeilichen Tätigkeit einheitlich gesehen werden, so daß vereinzelte spezialgesetzliche Übermittlungsregelungen in dem Zusammenhang wenig hilfreich sind und überdies wegen der unterschiedlichen Rechtsanwendung polizeiliche Arbeitskapazität unnötig binden. Schon die DSK hatte sich mehrfach mit dem Fragenbereich u. a. für Gaststättenkonzessionen zu befassen, einem Feld, das heute, nicht zuletzt im Zusammenhang mit der sog. organisierten Kriminalität, bedeutsam ist. Der LfD hatte schon mehrfach gegenüber dem Ministerium des Innern und für Sport auf die Notwendigkeit einer Regelung hingewiesen.

Diese kann wegen der unklaren Gesetzeslage nicht durch Verwaltungsvorschrift erfolgen. Die mit den Übermittlungen verbundenen Eingriffe, die großteils einschneidende Folgen für Einzelexistenzen haben, bedürfen eindeutig gesetzlicher Regelung unter Einschluß verfahrenssichernder Maßnahmen zur Konkretisierung des Rechts auf informationelle Selbstbestimmung. Hier ist u. a. zu fordern: die Schriftlichkeit und damit die Nachvollziehbarkeit des Verfahrens, eine strikte Zweckbindung, ein Verbot der Abgabe von Bewertungen im Hinblick auf den einem Ersuchen zugrundeliegenden Anlaß, Beschränkung auf dienstlich gewonnene Erkenntnisse, Verbot von Auskünften über Verfahren, die erkennbar zu einem Freispruch geführt haben oder mangels Tatverdacht eingestellt worden sind u. a.

h) Die DSK und der LfD hatten sich mehrfach mit der Speicherung und Übermittlung von Daten bei Suizidversuchen zu befassen (vgl. 13. Tb., Tz. 5.7). Dabei war davon auszugehen, daß als Rechtsgrundlage nicht § 25 a Abs. 1 PVG herangezogen werden kann, da dort (Nr. 2) nur die Speicherung „zur vorbeugenden Bekämpfung von Straftaten" zugelassen wird. Hier geht es jedoch zumindest in erster Linie um gefährdete Personen bzw. um den Schutz der Betroffenen selbst. Auch hier wäre eine eindeutige Rechtsgrundlage zu schaffen.

i) Bei der Auskunft an den Betroffenen ist in jüngster Zeit eine bedenkliche Praxis festzustellen. Unternehmen des privaten Sicherheitsgewerbes nutzen die im POG gegebene Auskunftsmöglichkeit für den Betroffenen zur Überprüfung von Bewerbern. Diese werden veranlaßt, auf bereits vorgedruckten Formularen die Polizei um Mitteilung evtl. über sie gespeicherter Daten zu ersuchen. Die Antworten dienen offensichtlich der Beurteilung, ob ein Bewerber im Sinne des Unternehmens als geeignet erscheint. Es ist zumindest fraglich, ob diese Praxis mit dem Zweck der Regelung übereinstimmt, den Bürger aus Gründen des Grundrechtsschutzes über ihn betreffende polizeiliche Speicherungen zu informieren. Faktisch wird damit aus einer Grundrechtssicherung ein Überwachungsinstrument. Es wird zu prüfen sein, ob und ggf. in welcher Weise dem durch eine Ergänzung im Gesetz entgegenzuwirken ist.

5.14 EUROPOL

Auf deutsche Initiative beschlossen die Staats- und Regierungschefs der EG-Mitgliedstaaten am 28./29. Juni 1991 in Luxemburg, zur Intensivierung des Kampfes gegen den international organisierten Drogenhandel und die sonstige international organisierte Kriminalität eine europäische kriminalpolizeiliche Zentralstelle (EUROPOL) zu schaffen.

Vor Ratifizierung einer völkerrechtlichen Konvention sollte EUROPOL nach einem Ministerübereinkommen in einer ersten Ausbaustufe als europäische Rauschgift-Zentralstelle bis zum Jahresbeginn 1993 eingerichtet werden. Das Ministerübereinkommen wurde Anfang Juni dieses Jahres unterzeichnet. Der endgültige Standort ist noch nicht bestimmt. Derzeit arbeitet EUROPOL DRUGS UNIT (EDU) in Straßburg. Die Tätigkeit beschränkt sich auf den Gesamtbereich Drogen und besteht im bilateralen Austausch von Informationen. Bei dieser „PC-Lösung" fragen die einzelnen nationalen Beamten auf Anfrage mit jeweils eigenem PC ihre nationalen Systeme ab und geben die Informationen unter Berücksichtigung der Voraussetzungen ihres nationalen Rechts an den Anfragenden weiter. Darüber hinaus werden Lagebilder ohne Personenbezug erstellt und den nationalen Polizeien zur Verfügung gestellt.

Der LfD hat es in Übereinstimmung mit dem Ministerium des Innern und für Sport für unabdingbar erklärt, daß der deutsche EUROPOL-Verbindungsbeamte im Trefferfall bei den „Länderdaten" die Anfrage an die datenbesitzende Stelle des jeweiligen Bundeslandes zur Entscheidung über die Übermittlung nach Länderrecht weitergibt. Ein Recht des BKA – und damit des Verbindungsbeamten –, diese Entscheidung im Einzelfall auch für Länderdaten zu treffen, kann aus der Zentralstellenbefugnis des BKA nach geltendem Recht nicht hergeleitet werden. Um die datenschutzrechtliche Kontrolle nicht leerlaufen zu lassen, hat der LfD weiterhin gefordert, alle Übermittlungen an ausländische Verbindungsbeamte bei EUROPOL-EDU zu dokumentieren.

So sehr die Initiative zur EG-weiten Bekämpfung des organisierten Drogenhandels und weiterer grenzüberschreitender Schwerkriminalität auch zu begrüßen ist, so sind für EUROPOL insgesamt doch mit Nachdruck verfahrensrechtliche und materielle Sicherungen zur Einhaltung der Grundrechte zu fordern. Rechtsgrundlage für einen personenbezogenen Datenaustausch kann nur entweder eine besondere Zulässigkeitsprüfung im Einzelfall nach geltendem Recht oder eine anzustrebende zwischenstaatliche Vereinbarung (Konvention) sein.

Diese müßte insbesondere eine klare materielle Zuständigkeitsregelung und eine Definierung der rechtlichen Verantwortlichkeit der Verbindungsbeamten enthalten. Ebenso ist der Rechtsschutz für die Betroffenen zu regeln und eine unabhängige Datenschutzkontrolle sicherzustellen. Ob darüber hinaus ein Verfahren erforderlich ist, fremde Fahndungsmaßnahmen auf ihre Vereinbarkeit mit nationalem Recht zu prüfen, bedarf noch der Diskussion. Jedenfalls werden sich diese und andere Forderungen nur im Verein mit den anderen Datenschutzbeauftragten in Bund und Ländern erfolgreich vertreten lassen.

5.15 Ist bei Geschwindigkeitsüberschreitungen jede Ermittlungsmethode erlaubt?

Ein PKW-Fahrer wird auf der Autobahn eines Nachbarbundeslandes bei einer Geschwindigkeitsüberschreitung von 24 km/h „geblitzt", kann sich aber bei der schriftlichen Anhörung nicht erinnern, ob er selbst oder eine Begleitperson im fraglichen

Moment gefahren ist. Daraufhin übersendet die Autobahnpolizei der für den Betroffenen zuständigen Schutzpolizeiinspektion das Frontfoto, das den Fahrer zeigt; ein Beamter will den Betroffenen aufsuchen, trifft wegen dessen Kurzurlaub aber niemanden an. Seine Tochter (Schülerin) findet abends die unter der Wohnungstür durchgeschobene Visitenkarte mit der schriftlichen Bitte um Rücksprache „wegen einer Verkehrsordnungswidrigkeit"; sie informiert tags darauf die Polizei von dem Kurzurlaub ihres Vaters. Obwohl es bis zur Verjährung der Ordnungswidrigkeit noch zwei Monate waren, hatte zwischenzeitlich der Eifer den Beamten zum Handeln getrieben. Das Frontfoto wurde den Nachbarn zur Identifizierung des Täters gezeigt. Diese erfuhren dadurch von dem Tatvorwurf.

War die Polizei damit zu weit gegangen?

Nach § 53 Abs.1 des Gesetzes über Ordnungswidrigkeiten – OWiG – haben die Beamten des Polizeidienstes Ordnungswidrigkeiten nach pflichtgemäßem Ermessen zu erforschen und dabei alle unaufschiebbaren Maßnahmen zu treffen, um die Verdunkelung der Sache zu verhüten; in diesem Rahmen entscheidet die Polizei, wie und mit welchen Mitteln sie den Sachverhalt aufklärt. Dabei ist das öffentliche Interesse an der Verfolgung einer Ordnungswidrigkeit gegen mögliche Nachteile abzuwägen, die sich aus der Art der Beschaffung von Beweismitteln ergeben. Die damit verbundenen Nachteile für den Betroffenen dürfen nicht außer Verhältnis zu dem konkreten Verfolgungszweck stehen. Der Grundsatz der Verhältnismäßigkeit gilt heute als Verfassungsgebot für alles staatliche Handeln; er setzt voraus, daß eine Maßnahme geeignet, erforderlich und angemessen ist. Das Einschalten der Nachbarn stellt ohne Zweifel einen Eingriff in die Rechte des Betroffenen dar, denn es werden Kenntnisse über ihn vermittelt. Nachteile für das Nachbarschaftsverhältnis sind zumindest nicht auszuschließen. Vor diesem Hintergrund war die Maßnahme zumindest nicht erforderlich, denn bis zur Verjährung waren noch zwei Monate Zeit. Jedenfalls aus dem gleichen Grunde war das Vorgehen auch nicht angemessen. Man hätte schonender vorgehen können. Daß der Betroffene über sechs Wochen Urlaub machen würde, war keinesfalls anzunehmen. Die Benachrichtigung unter Verwendung einer Visitenkarte muß hingegen als zulässig angesehen werden, denn bei einer postalischen Vorladung hätten Familienangehörige von dem Vorwurf ebenfalls Kenntnis erhalten können.

5.16 Verwendung von Lichtbildern im Personalausweisregister für die Fahndung nach Verkehrssündern

Wie bereits oben dargestellt, ist es aus datenschutzrechtlicher Sicht ein schwerer Eingriff, wenn Polizeibeamte die Frontfotos von Verkehrsüberwachungskontrollen bei den Nachbarn herumzeigen, um den „Täter" zu identifizieren. Jede weniger belastende Erhebungsmethode muß vorgehen. Gilt das auch für den Vergleich mit den Lichtbildern, die sich im Personalausweis- und im Paßregister befinden?

Nach § 2 b Abs. 2 des Personalausweisgesetzes und der entsprechenden Bestimmung im Paßgesetz dürfen der Polizei auf deren Ersuchen Daten aus dem Ausweisregister übermittelt werden, wenn sie aufgrund von Gesetzen oder Rechtsverordnungen berechtigt ist, solche Daten zu erhalten, wenn sie ohne Kenntnis der Daten nicht in der Lage wäre, eine ihr obliegende Aufgabe zu erfüllen und und wenn die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden könnten oder nach der Art der Aufgabe, zu deren Erfüllung die Daten erforderlich sind, von einer solchen Datenerhebung abgesehen werden muß.

Die grundsätzliche Berechtigung der Polizei als ersuchende Behörde ergibt sich aus § 53 OWiG i. V. m. §§ 161 ff. StPO. Nach einem Rundschreiben des Ministeriums des Innern und für Sport von 1987 über die Zusammenarbeit der Polizei mit den Personalausweis- und Paßbehörden kommt bei Verkehrsordnungswidrigkeiten im Regelfall eine Nutzung dieser Register aus Gründen der Verhältnismäßigkeit nicht in Betracht. Was nicht mehr als „Regelfall" zu gelten hat, muß der Einzelfallbehandlung vorbehalten bleiben.

Die Frage, ob die Einsicht in die Registerfotos oder die Befragung von Zeugen (Nachbarn) der größere Eingriff ist, wird bundesweit nicht einheitlich beantwortet. Der LfD geht mit dem Ministerium des Innern und für Sport jedoch für Rheinland-Pfalz davon aus, daß es aus der Sicht des Betroffenen stärker beeinträchtigt, wenn die Radarbilder bei den Nachbarn herumgezeigt werden. Dies müßte eigentlich das absolut letzte Mittel sein.

5.17 Keine Registrierung von Dirnen

Schon im 12. Tb. (Tz. 5.22 und Tz. 5.52) war über die automatisierte Verarbeitung von Hinweisen auf Prostitution berichtet worden. Es ging um die Einrichtung der Arbeitsdatei „MENZU" (Menschenhandel und Zuhälterei), um die restriktive Verwendung des personengebundenen Hinweises (PHW) „Prostitution" in POLIS sowie um die Bedenken gegen eine erkennungsdienstliche Behandlung von Prostituierten „auf freiwilliger Basis". Bereits zu diesem Zeitpunkt lag allen Maßnahmen und Regelungen der Gedanke zugrunde, daß die Ausübung der Prostitution für sich alleine betrachtet kein ausreichender Grund für eine Speicherung von Daten sein konnte. Gerade die Einrichtung von „MENZU" und die Verwendung des PHW sollen die Speicherung von Hinweisen auf ausgeübte Prostitution dann sicherstellen, wenn dies im Zusammenhang mit der Aufklärung oder Bekämpfung von Straftaten im konkreten Einzelfall erforderlich ist, und damit strafrechtlich beziehungslose Hinweise vermeiden.

Erneute Feststellungen hierzu haben ergeben, daß nunmehr die letzte – noch manuell – bei einem Polizeipräsidium geführte Datei über Prostituierte vernichtet worden ist. Obwohl auch diese Datei vor allem im Bereich der Rauschgiftkriminalität über verzeichnete Spitz- und Kosenamen zur Aufklärung einiger Straftaten beigetragen hat, ist die Speicherung personenbezogener Daten von Prostituierten nur aus diesem Grunde nicht mehr vertretbar. Immerhin ist die Prostitution vom Gesetzgeber weder verboten noch poenalisiert worden. Strafbarkeitsbestimmungen knüpfen vielmehr nur an außerhalb der Prostitution liegende besonders qualifizierende Merkmale an. In der Rechtsprechung wird die Ausübung der Prostituition im Rahmen des Schutzbereichs des Artikels 2 Abs. 1 GG gesehen (vgl. BVerwGE 60, 284, 286), während in der Kommentarliteratur zusätzlich die Auffassung vertreten wird, daß es sich um eine durch Artikel 12 GG geschützte Berufsausübung handele (siehe hierzu Rupert Scholz in Maunz-Dürig, RdNr. 25 zu Artikel 12).

5.18 „Arbeitslos (Prostituierte)"

Auf dem polizeilichen Formular für die Anhörung von Beschuldigten fand sich dieser Hinweis in dem Feld, das für die Angabe des Berufs vorgesehen ist. Nach näheren Feststellungen beruhte der Klammerhinweis auf einem 14 Monate alten Vermerk, der nach einer polizeilichen Kontrolle gefertigt worden war.

Der LfD hat darauf hingewiesen, daß ein derart sensibles Datum nicht ohne Hinweis auf den beachtlichen Zeitablauf in dem Personalbogen hätte vermerkt werden dürfen. Zudem wurde empfohlen, derart sensible und gleichzeitig ungesicherte Angaben gesondert in einem zusätzlichen Vermerk festzuhalten, insbesondere, wenn die oder der Betroffene bei der Vernehmung selbst nicht mitgewirkt hat, also z. B. nicht erschienen ist. Dabei ist auch zu berücksichtigen, daß der zu verwendende Vordruck POLRP 1101/82 mit dem Vordruck POLRP 1103/82 – Merkblatt – durchschreibefähig ist. Wird ein entsprechender Vermerk in den Personalbogen aufgenommen, ist nicht auszuschließen, daß die ungesicherten und sensiblen Angaben über das Merkblatt in der KpS weitergeführt und bei entsprechendem Anlaß erneut ungeprüft übernommen werden.

5.19 Sachfahndung nach gestohlenen Kraftfahrzeugen

Der bandenmäßige, in großem Stil betriebene Diebstahl von Kraftfahrzeugen und deren Verschiebung in bestimmte Staaten hat in den letzten Jahren Ausmaße angenommen, die über die Prämien und sonstigen Konditionen der Kaskoversicherer eine Vielzahl von Kfz-Haltern zu spüren bekommt. Um die Fahndung nach einigen besonders betroffenen Automarken zu intensivieren, entwickelte das BKA eine unkonventionelle Methode, indem die technischen Daten (nicht die Halterdaten) als gestohlen gemeldeter Kraftfahrzeuge den Fahrzeugherstellern und dem HUK-Verband übermittelt werden, die sie in ihre EDV-Systeme übernehmen. Für den Fall der Feststellung eines solchen Fahrzeugs oder von entsprechenden Fahrzeugteilen wurde zugesagt, die Polizei zu informieren.

Der LfD wurde frühzeitig vom Ministerium des Innern und für Sport über das Vorhaben informiert und um Stellungnahme gebeten. Er antwortete kurzfristig, daß aus der Sicht des Datenschutzes keine Einwände bestehen. Maßgebend hierfür war zunächst die Tatsache, daß es sich im wesentlichen um Sachdaten handelt, die nur insoweit einen Personenbezug aufweisen, als die Fahrgestell-Nummer Auskunft über den rechtmäßigen Halter bzw. den Ersterwerber gibt. Diese Daten sind aber ohnehin den Herstellern bekannt. Der HUK-Verband erfährt sie nach dem Diebstahl kurzfristig. Schließlich können schutzwürdige Interessen der Betroffenen durch die Datenübermittlung so gut wie nicht beeinträchtigt sein.

Gleichwohl wurde das Vorhaben bei den Datenschutzbeauftragten sowie zwischen diesen und dem BKA während des Jahres 1992 diskutiert. Einer der Hauptpunkte war die Frage der Rechtsgrundlage für die Übermittlung ganzer polizeilicher Datenbestände an private Unternehmen. Die Forderung, daß die Einbeziehung Privater in Maßnahmen der polizeilichen Fahndung die Ausnahme bleiben muß, wird auch vom LfD unterstützt. Aus den genannten Gründen führte die Meinungsbildung bei den Datenschutzbeauftragten dann aber mehrheitlich dazu, „daß überwiegende datenschutzrechtliche Interessen jedenfalls nicht grundsätzlich gegen das geplante Verfahren sprechen". Dies wurde so vom Vorsitzenden des Arbeitskreises Sicherheit der Datenschutzbeauftragten dem Präsidenten des BKA mitgeteilt.

Keine Übereinstimmung gab es hinsichtlich der Kritik der Datenschutzbeauftragten an der falschen Vorstellung des BKA über die Verteilung der Verantwortung im INPOL-Verbund für die von den Ländern eingegebenen Daten. Bei der Kfz-Sachfahndungsdatei handelt es sich in der ganz überwiegenden Mehrzahl um Daten, die von den Polizeibehörden der Länder eingegeben worden sind. Das Gesetz über das Bundeskriminalamt verleiht diesem keine Befugnis, die hier relevanten Teilbestände der Kfz-Sachfahndungsdatei ohne Abstimmung mit den zuständigen Landesbehörden über den Gegenstand, den Zweck und die Form der Übermittlung auf eigene Initiative an Dritte zu übermitteln. Dementsprechend ging zunächst offenbar auch das BKA davon aus, daß die Zulässigkeit der Übermittlung durch eine generelle Zustimmung der Länderpolizeien als Datenbesitzer zu klären sei. Im weiteren Verlauf hielt sich das BKA dann aber als Zentralstelle gem. § 1 Abs. 1 Satz 2 BKAG i. V. m. § 16 BDSG für übermittlungsbefugt. Dies wird von der überwiegenden Mehrheit der Datenschutzbeauftragten, wie auch vom Ministerium des Innern und für Sport, grundsätzlich anders gesehen. Die anstehende Neufassung des BKAG erst soll hier Klarheit bringen.

Nachdem in diesem Punkt bereits eine tragfähige Lösung für das im Interesse der Bürger zu begrüßende Projekt gefunden war, verwundert es, daß das BKA ohne sachliche Notwendigkeit die Gelegenheit zu nutzen versucht, seine interessenbezogene Auslegung der Zentralstellenfunktion durchzusetzen.

Abschließend sei bemerkt, daß ein entscheidender Beitrag zur Verminderung der Kfz-Diebstähle von der Automobilindustrie in Form von wirksamen und kostengünstigen Diebstahlssicherungen erwartet werden muß. Wenn hier nicht mehr geschieht, wird der Ruf nach dem Gesetzgeber unvermeidlich. Auf den sehr aufschlußreichen Aufsatz des Abteilungspräsidenten des BKA, Dr. Wolfgang Steinke, Wiesbaden, in der Zeitschrift für Rechtspolitik (ZRP) vom März 1992 sei in diesem Zusammenhang hingewiesen.

5.20 Keine Privat-PC bei der Polizei

Im Laufe der Berichtsperiode war in einem Fall der über einige Monate erstreckte Gebrauch eines privaten Heimcomputers mit Drucker durch einen Dienststellenleiter der Polizei festzustellen. Er wurde verwendet, um dienstlichen Schriftverkehr zu erstellen. Der Schriftverkehr wurde auf zwei Disketten gespeichert. Der PC war ausschließlich dem Dienststellenleiter zugänglich. Dieser hatte den Computer aus Anlaß der Vorbereitung eines größeren Einsatzes genutzt, um Stärkemeldungen zu erstellen; als Grundlage hierfür enthielt eine Diskette ein Dokument mit einer „Personalliste". In der Folgezeit war dann auch anderer Schriftverkehr auf dem mitgebrachten PC bearbeitet worden.

Die Nutzung privater PC bei der Polizei ist in Rheinland-Pfalz im Grundsatz nicht zu gelassen. Andernfalls ergäbe sich aus der Sicht des Datenschutzes die Notwendigkeit, eine Dienstanweisung zu erlassen, um durch geeignete Regelungen die Gefahr eines „abgestuften" Datenschutzes je nach Eigentumsverhältnissen soweit wie möglich zu vermeiden. Hierzu wird auf die Ausführungen im 12. Tb., Tz. 7.3.3.3, über die Nutzung von Personalcomputern durch Staatsanwälte hingewiesen.

Der Rechner wurde unverzüglich aus den Diensträumen entfernt, die beiden Disketten wurden gelöscht.

5.21 Behandlung von Fällen nach § 218 StGB

Schon zu einem frühen Zeitpunkt hatte die Polizei Rheinland-Pfalz sich in Absprache mit der DSK entschieden, alle Datenspeicherungen von Frauen, gegen die im Zusammenhang mit § 218 StGB ermittelt wurde, in den polizeilichen Erkenntnisdateien zu löschen und auch auf künftige Speicherungen zu verzichten. Dies wird vom LfD überprüft. In den in der Kriminalstatistik für 1992 ausgewiesenen fünf Fällen und in dem einen Fall, der in der Statistik für das erste Halbjahr 1993 enthalten ist, sind keine personenbezogenen Daten in POLIS gespeichert und auch keine Kriminalakten angelegt.

Inwieweit darüber hinaus auch Speicherungen in den polizeilichen Vorgangssystemen (POLADIS) auf das unerläßliche Minimum reduziert werden können, wird derzeit auf Anregung des LfD geprüft. Hier kommt es im wesentlichen auf die sog. Tagebuchfunktion an. Denkbar wäre es z. B., bei zu archivierenden Vorgängen den Hinweis auf die Art des in Frage stehenden Straftatbestandes zu unterdrücken oder einen entsprechenden Effekt durch Programmänderung herbeizuführen. Die archivierten Daten in der Vorgangsverwaltung sind ohnehin nur einem begrenzten Kreis von Sachbearbeitern einer Dienststelle unter zusätzlichen Sicherungen zugänglich (vgl. Tz. 5.11).

5.22 Generalerrichtungsanordnungen

In der Vergangenheit hat sich gezeigt, daß Dateierrichtungsanordnungen nach § 25 g PVG, die nach § 10 Abs. 2 LDatG beim LfD in verkürzter Form anzumelden sind, in einer Vielzahl von Fällen im wesentlichen den gleichen Inhalt, oft auch den gleichen Text haben. Die Anmeldung mit dem vollen Text in jedem Einzelfall führte zu nicht unerheblichem Verwaltungsaufwand und zu zeitlichen Verzögerungen in allen Bereichen. Schon vor einiger Zeit war daher für die Errichtung von Dateien in Strafermittlungsverfahren mit Telefonüberwachung (TÜ) mit dem Ministerium des Innern und für Sport eine Generalerrichtungsanordnung „PHONE" ausgearbeitet worden, die im Lande einheitlich Verwendung findet. In jedem Fall der Errichtung einer Datei erfolgt weiterhin die Anmeldung beim LfD unter Angabe des Verfahrens, der zuständigen Polizeibehörde und des Gegenstands des Verfahrens sowie der voraussichtlichen Dauer der Datei wie bisher. Im übrigen wird auf den Inhalt der Generalerrichtungsanordnung Bezug genommen. Soll beim Betrieb der Datei vom Inhalt der Generalerrichtungsanordnung abgewichen werden, ist dies unter näherer Darstellung dem LfD bei der Anmeldung mitzuteilen.

Das Verfahren hat sich bewährt. Die Anmeldungen sind damit im Grunde nicht auf die in § 10 Abs. 2 LDatG genannten verkürzten Merkmale beschränkt, sondern enthalten darüber hinaus den gesamten Inhalt der Errichtungsanordnung nach § 25 g PVG, was sich insbesondere bei evtl. Abweichungen auswirkt. Das Anmeldeverfahren ist beschleunigt, der Überblick verbessert. Darüber hinaus wird bewirkt, daß aus der Sicht des Datenschutzes mitunter problematische Sonderregelungen einzelner Polizeistellen stark reduziert sind, was auch für Soforterrichtungsanordnungen gilt.

Aufgrund der Erfahrungen ist jetzt dieses Verfahren auf die Anmeldung von Dateien in polizeilichen Ermittlungsverfahren ausgedehnt worden. Dabei konnte erreicht werden, daß zukünftig auch die Löschung bzw. Auflösung einer Datei dem LfD gesondert und „von Amts wegen" mitgeteilt wird.

Mit jeder Anmeldung wird auch weiterhin die Art des eingesetzten EDV-Systems gesondert angegeben.

5.23 Reality-TV und Menschenwürde

Eine Tendenz privater Fernsehanstalten, spektakuläre Unfälle, andere polizeiliche Aktivitäten und Rettungseinsätze möglichst realitätsnah und auch unter Beteiligung wirklich an dem jeweiligen Ereignis Beteiligter darzustellen (vgl. unten 19.2), darf nicht dazu führen, daß z. B. durch Großaufnahmen Verletzter, Geschockter oder Verzweifelter deren Persönlichkeitsrechte oder die Menschenwürde verletzt werden. Hier geht die Würde des Menschen dem presserechtlichen Informationsrecht eindeutig vor, wie es auch in § 4 des Landespressegesetzes klar zum Ausdruck kommt. Dort ist u. a. bestimmt, daß Auskünfte verweigert werden können, wenn durch sie ein schutzwürdiges privates Interesse verletzt würde. Dies muß auch für die Hergabe von im Auftrag gefertigtem Bildmaterial gelten. Von einer – etwa mutmaßlichen – Einwilligung der Betroffenen wird angesichts ihres besonderen Zustandes im Zweifel nicht ausgegangen werden können.

Diese Auffassung hat der LfD unabhängig von der medienrechtlichen Beurteilung schon frühzeitig in Gesprächen mit dem Ministerium des Innern und für Sport vertreten. Auch die Innenministerkonferenz und der Innenminister des Landes haben sich kritisch geäußert. Hier soll erneut klargestellt werden, daß öffentlich Bedienstete rechtswidrig handeln, wenn sie sich an der Herstellung und Weitergabe von Bildmaterial beteiligen, das die Würde von Menschen in der genannten Weise verletzt.

5.24 Die Polizei als Vermittler für Transplantate von Verkehrstoten?

Bestimmte, für Transplantationen dringend benötigte Organe sind in der Praxis schwer zu beschaffen. Oft liegen zwischen der Entnahme und dem Zeitpunkt der letzten Verwendbarkeit nur kurze Zeiträume. Es ist deshalb verständlich, wenn von den in Frage kommenden Kliniken die Frage gestellt wird, ob die Polizei bei tödlichen Verkehrsunfällen rechtzeitig geeignete Hinweise geben kann.

Auch der LfD sieht die dringende Notwendigkeit, Patienten rechtzeitig mit den erforderlichen Ersatzorganen zu versorgen. Zunächst ist festzuhalten, daß die bereichsspezifischen datenschutzrechtlichen Übermittlungsbestimmungen im Polizeirecht (§ 25 a Abs. 1 POG) nicht herangezogen werden können, da sie sich nur auf personenbezogene Daten beziehen, es hier aber um die Daten Verstorbener geht.

Gleichwohl stellt sich eine Reihe von Fragen. Zunächst geht es darum, ob und wie eine evtl. Strafbarkeit des offenbarenden Beamten nach § 203 Abs. 2 StGB wegen Verletzung von Privatgeheimnissen ausgeschlossen werden kann. Dies ist sicher dann unproblematisch, wenn die Einwilligung des Spenders (z. B. im Organspendepaß) zu Lebzeiten erteilt wurde oder die von der Polizei benachrichtigten Angehörigen der Offenbarung zustimmen. Dieser Weg dürfte allerdings in der Mehrzahl der Fälle zu zeitaufwendig und auch zu kompliziert sein. Die Annahme eines rechtfertigenden Notstandes nach § 34 StGB setzt wiederum eine Notstandslage und eine hierauf gestützte Güterabwägung durch den Polizeibeamten vor Ort voraus. Diese Güterabwägung muß naturgemäß auch die konkrete Situation auf der Empfängerseite einschließen, die dem Beamten im fraglichen Zeitpunkt nicht vollständig bekannt sein dürfte. Ob Gerichte angesichts der besonderen Umstände das Vorliegen der Voraussetzungen einer Güterabwägung dennoch anerkennen, kann nicht abgeschätzt werden.

Eine „mutmaßliche Einwilligung" könnte nur dann als Rechtfertigungsgrund für eine Offenbarung angesehen werden, wenn ohne weiteres davon ausgegangen werden könnte, daß die Betroffenen zu Lebzeiten mit einer Transplantation einverstanden gewesen wären oder daß Angehörige einer Transplantation zustimmen. Dies ist aber nicht der Fall. Nicht zuletzt aus diesem Grunde ist der Gesetzgeber aufgerufen, durch ein Transplantationsgesetz für mehr Rechtssicherheit zu sorgen und die Voraussetzungen für eine angemessene Bereitstellung von Transplantaten zu schaffen.

5.25 Benutzung gewerkschaftseigener PC in Diensträumen der Polizei

Im Zusammenhang mit der Nutzung privater oder gewerkschaftseigener PC hatte sich der LfD u. a. mit der Frage der Verwendung im Rahmen der Personalratsarbeit zu befassen.

Sollen für diese Zwecke nichtdienstliche PC verwendet werden, beantwortet sich die Frage der datenschutzrechtlichen Zulässigkeit im Grundsatz nicht anders als beim Einsatz privater PC zu dienstlichen Zwecken im Bereich der Polizei überhaupt (vgl. Tz. 5.20): Sie sind grundsätzlich nicht zugelassen. Im Falle der Zulassung wäre durch Dienstanweisung die Einhaltung technisch-organisatorischer Datensicherungsanforderungen und deren Kontrollierbarkeit unter den gleichen Bedingungen wie bei dienstlichen Geräten zu gewährleisten. Die Frage, wer für den Erlaß der Dienstanweisung zuständig ist, wäre organisations-

rechtlich zu klären. Im Bereich der Kontrollierbarkeit würden die Probleme weiter gesteigert, wenn personenbezogene Daten aus der dem dienstlichen Bereich zuzuordnenden Personalratsarbeit mit solchen aus der zum nichtöffentlichen Bereich gehörenden Gewerkschaftstätigkeit gemeinsam auf einem PC verarbeitet werden. Hiergegen bestehen aus der Sicht des Datenschutzes grundsätzliche Bedenken.

5.26 Studentische Praktikanten und Echtdaten

Jurastudenten absolvieren nach dem Deutschen Richtergesetz und dem Landesgesetz über die Juristische Ausbildung in der vorlesungsfreien Zeit während eines Monats ein Praktikum auch bei einer Verwaltungsbehörde, wozu auch die Polizei zählt. Nach einer förmlichen Verpflichtung zur Verschwiegenheit zu Beginn des Praktikums erhalten sie im Interesse einer praxisnahen Vermittlung der Grundzüge des Geschäftsbetriebes auch Echtdaten von Bürgern bei Vernehmungen oder bei anderen Anlässen zur Kenntnis.
Dies war aus dem Bereich der Polizei unter Hinweis auf den Datenschutz problematisiert worden.

Ein Verstoß gegen Vorschriften des Datenschutzes kann jedoch übereinstimmend mit dem Ministerium des Innern und für Sport und dem Ministerium der Justiz in der auch bei der Justiz geübten Praxis nicht gesehen werden. Die gesetzlich vorgesehene praxisbezogene Ausbildung wäre sonst nicht möglich. Der Ausbilder wird jedoch im Einzelfall zu prüfen haben, ob schutzwürdige Belange eines Betroffenen überwiegen und bejahendenfalls von der Verwendung der Daten absehen. Angesichts der Vielgestaltigkeit der Lebenssachverhalte lassen sich hierfür jedoch keine erschöpfenden allgemeinen Kriterien aufstellen.

5.27 Datenverarbeitung durch private Sicherheits- und Überwachungsdienste sowie Nutzung der datenschutzrechtlichen Auskunftsverpflichtung der Polizei

Auf die besonderen Gefahren, die mit der Verarbeitung personenbezogener Daten Dritter durch private Sicherheits- und Überwachungsdienste für den inzwischen erreichten Datenschutzstandard im Sicherheitsbereich verbunden sein können, hat der LfD bereits im 13. Tb. (Tz. 21.5) hingewiesen. In der Zwischenzeit wurde die Tätigkeit dieser Dienste zumindest im Umfang erheblich ausgeweitet. Von Vertretern des BKA wird in dem Zusammenhang zu Recht auf die entstehende Diskrepanz zu den datenschutzrechtlichen Normierungen im Polizeibereich hingewiesen. Hier könnten mittelfristig Akzeptanzprobleme bei der Polizei entstehen. Die Forderung nach einer allfälligen gesetzlichen Regelung muß daher mit verstärkter Dringlichkeit wiederholt werden.

Neuerdings häufen sich die Fälle, in denen Bewerber für den Dienst in einer Bewachungsfirma beim Landeskriminalamt Anträge auf „Selbstauskunft" stellen. Die Anträge sehen gleichartig aus, auch wenn sie überwiegend handschriftlich ausgefüllt sind. Dies und andere Merkmale, wie z. B. anfänglich an anderer Stelle gesammelt durch eine Firma eingesandte Anträge, lassen vermuten, daß offenbar die Vorlage eines sog. polizeilichen Führungszeugnisses durch einen Bewerber nicht genügt, weil das Bundeszentralregister differenzierte Nutzungsregelungen für gespeicherte Informationen enthält, weshalb auf polizeiliche Auskünfte zurückgegriffen werden soll.

Soweit eine Bewachungsfirma erkennbar selbst die Auskunftsanträge vorlegt, bestünden keine Bedenken, wenn die Polizeibehörde auf die Regelung in § 5 der Bewachungsverordnung hinweist, nach der der Gewerbetreibende Vor- und Zunamen, Geburtstag und Geburtsort, Wohnort und Wohnung der Wachpersonen, die er beschäftigen will, der Erlaubnisbehörde vorher zu melden hat. Weitergegeben wird – entsprechend eines vom Ministerium für Wirtschaft und Verkehr akzeptierten Vorschlags des LfD – lediglich eine inhaltlich auf das Ergebnis beschränkte Beurteilung der Zuverlässigkeit des Bewerbers. Damit bleibt es für den Bewerber möglich, solche Speicherungen nicht offenbaren zu müssen, die die Erlaubnisbehörde selbst nicht für relevant hält.

Begehrt der Betroffene jedoch selbst die Auskunft, so ist diese nach § 25 f POG zu erteilen, da von den in dieser Bestimmung (Absatz 2) aufgezählten Ausnahmetatbeständen keiner zutrifft.

Es wäre in Erwägung zu ziehen, Auskunftsbegehrenden eine nur mündliche Auskunft zu erteilen, wenn die Auskunft offensichtlich nur im Zusammenhang mit einer Bewerbung beantragt wird.

Dennoch bleibt die Überlegung, daß die als Schutz- und Abwehrrecht konzipierte Auskunftsmöglichkeit sich hier im Ergebnis zu Ungunsten des Betroffenen auswirken kann und die sich abzeichnende Praxis die weiteren Schutzregelungen im Bundeszentralregistergesetz praktisch ebenso leerlaufen läßt wie die Praxis bei der Anwendung des § 5 der Bewachungsverordnung. Bei alledem muß darauf hingewiesen werden, daß die Erkenntnisdateien der Polizei interne Arbeitsmittel sind, die ihrem Zweck entsprechend Daten auch über nicht belastende Vorgänge enthalten, die in aller Regel nur von der Polizei selbst zutreffend gewürdigt werden können.

Eine Lösung kann im Zweifel jedoch nur durch den Gesetzgeber im Bereich des Arbeitsrechts erfolgen.

5.28 Blutalkoholproben

Bei der Entnahme von Blutalkoholproben werden empfindliche medizinische Daten erhoben. Vom sorgfältigen Umgang mit ihnen hängt das Wohl und Wehe vieler betroffener Bürger ab. Schon im vorangehenden Tätigkeitsbericht wurde deswegen der Datenschutz bei der Staatlichen Untersuchungsstelle für Blutalkohol besonders angesprochen (Tz. 5.6). Offengebliebene Punkte konnten seitdem im wesentlichen im Sinne des Datenschutzes geklärt werden. Die vom LfD problematisierte Formblattfrage nach „von dem jetzigen Vorfall unabhängigen Krankheiten oder Leiden" soll nicht zu entsprechenden Speicherungen im Datensatz führen. Die Antworten verbleiben jedoch im Vorgang. Es geht dabei um alternative Erklärungen für ein auffälliges Verhalten des Probanden, wie Diabetes, Epilepsie, Geisteskrankheiten oder frühere Hirnverletzungen. Die Probanden werden zwar auf die Protokollierungen hierüber aufmerksam gemacht. Der LfD wies jedoch darauf hin, daß Fragen in dieser Richtung wegen ihrer hohen Sensitivität nur eng auf den Zweck begrenzt gestellt werden dürfen.

Inzwischen ist beabsichtigt, die Blutalkoholuntersuchungen für den Bereich des Polizeipräsidiums Rheinhessen im Wege der Auftragsdatenverarbeitung gemäß § 4 LDatG an ein Unternehmen zu vergeben, das in gleicher Weise bereits für das Polizeipräsidium Wiesbaden tätig ist. Hierfür wurde ein Generalvertrag zwischen dem Land, vertreten durch das Ministerium des Innern und für Sport, und dem Unternehmen entworfen, bei dessen Vorbereitung der LfD eingeschaltet wurde. Ursprünglich wurde aus der Sicht des Datenschutzes eine Lösung gefordert, nach der anstelle des bisher mit den Blutproben von der Polizei vorgelegten Formularprotokolls mit Name und Anschrift des Probanden eine Ziffernkombination mitgegeben wird, die zwar den Polizei- und Justizbehörden, nicht aber dem Auftragnehmer die Reidentifikation ermöglicht. Leider sah sich das Ministerium trotz anfänglicher Zusage dann doch nicht in der Lage, diese im Sinne des Datenschutzes sauberste Lösung zu realisieren.

Im weiteren Verlauf konnten jedoch verschiedene wesentliche Forderungen im Vertragstext verankert werden. So ist das Unternehmen verpflichtet, die Vorschriften des LDatG in der jeweiligen Fassung zu beachten und auch Kontrollen des LfD zu akzeptieren. Auch das Land hat sich ein jederzeitiges Prüfungsrecht einräumen lassen. Der Gegenstand der Datenverarbeitung und die Weisungen der auftraggebenden Stelle für die Datenverarbeitung sind mit hinreichender Deutlichkeit beschrieben. Bei Verletzung der Datenschutzbestimmungen ist eine fristlose Vertragskündigung vorgesehen.

5.29 Mehr Transparenz bei Einstellungsuntersuchungen für den Polizeidienst

In einer ergänzenden Verwaltungsvorschrift zur Polizeidienstvorschrift 300 ist jetzt bundeseinheitlich bestimmt, daß bei der Beurteilung der Polizeidiensttauglichkeit wie auch der Polizeidienstfähigkeit zusätzliche ärztliche Unterlagen anderer Stellen nur durch den Arzt und nur mit Zustimmung des Bewerbers oder der Bewerberin angefordert werden dürfen. Die Praxis in Rheinland-Pfalz ging im Ergebnis bisher diesen Weg, da alle ärztlichen Fragen, die nicht von dem untersuchenden Polizeiarzt beurteilt werden konnten, von dem Bewerber durch Vorlage spezieller Befunde selbst zu klären waren. Nun ist aber auf Betreiben sowohl des Bundesbeauftragten wie auch des Landesbeauftragten für den Datenschutz der Grundsatz ausdrücklich und bundesweit festgeschrieben. Auch Bewerber für den Polizeidienst haben ein Anrecht darauf zu wissen, auf welchen Erkenntnisquellen die für ihren Berufsweg entscheidende polizeiärztliche Beurteilung beruht.

6 Verfassungsschutz

6.1 Sicherheitsüberprüfungsgesetz des Bundes
– zu viel Geheimschutz –

Ein entscheidender Beitrag zur Verbesserung des Datenschutzes im Bereich der Sicherheitsüberprüfung und der Verschlußsachen wäre eine drastische Verringerung der Überprüfung von Personen und der Einstufung von Vorgängen von VS-NUR FÜR DEN DIENSTGEBRAUCH bis STRENG GEHEIM. Sowohl bei Ermächtigungen wie auch bei Einstufungen sollte wesentlich kritischer geprüft werden, ob sie im einzelnen Fall überhaupt erforderlich sind und bejahendenfalls, ob nicht ein geringerer Grad ausreicht. Der Ist-Bestand wäre in diesem Sinne nach Auffassung des LfD stark reduzierbar.

Jeder Ermächtigung geht nach den Stufen unterschiedlich intensiv die Erhebung z. T. hochsensibler Daten voraus; sie verursacht aber auch einen starken Verwaltungsaufwand sowohl beim Verfassungsschutz als mitwirkender Behörde wie auch bei den Geheimschutzbeauftragten in den öffentlichen Stellen bis auf die Gemeindeebene. Auch die Einstufung von Verschlußsachen verursacht zusätzlichen Verwaltungsaufwand, der sich bei ihrer Bearbeitung ständig fortsetzt. Eine Reduzierung, wo immer vertretbar, sollte sich deshalb schon aus dem Gebot wirtschaftlicher Verwaltungsführung ergeben.

Die nach der Wiedervereinigung veränderte Sicherheitslage wäre ein plausibler Grund für ein „Großreinemachen".

Der LfD nahm die Beratungen zum Entwurf für ein Sicherheitsüberprüfungsgesetz (SÜG) des Bundes zum Anlaß für Empfehlungen in diese Richtung. So sollten die jeweils tragenden Gründe für die Einstufung eines Vorganges oder die Überprüfung einer Person einschließlich des Grades dokumentiert und die einstufende Stelle verpflichtet werden, die Notwendigkeit und die Richtigkeit in regelmäßigen Abständen zu überprüfen. Das Ministerium des Innern und für Sport, das den Überlegungen im Grunde positiv gegenübersteht, konnte sich bei den Beratungen im Bundesrat insoweit jedoch nicht durchsetzen.

Im übrigen schloß sich der LfD den Vorschlägen des Bundesbeauftragten auch gegenüber dem Ministerium des Innern und für Sport an, nachdem er bereits im Zuge der Beratungen des ersten Referentenentwurfs im Herbst 1991 ausführlich Stellung genommen hatte.

Dabei hatte der LfD u. a. Bedenken gegen den ausnahmslosen Ausschluß eines Einsichtsrechts des Betroffenen sowohl in die beim Geheimschutzbeauftragten seiner Behörde geführte Sicherheitsakte wie auch der Sicherheitsüberprüfungsakte beim Verfassungsschutz als mitwirkender Behörde geltend gemacht. Dies hat im Verein mit der Haltung anderer DSB zwar zu einem eingeschränkten Auskunftsanspruch über gespeicherte personenbezogene Daten geführt. Eine Akteneinsicht durch den Betroffenen ist jedoch nur für den Fall und insoweit zugelassen, als eine Auskunft für die Wahrnehmung seiner rechtlichen Interessen nicht ausreicht; sie ist überdies auf die beim Geheimschutzbeauftragten der Dienstbehörde geführte Sicherheitsakte beschränkt, die in aller Regel nur dienstliche Daten und Personalien enthält, die dem Betroffenen ohnehin bekannt sein dürften. Ein Einblick in die bei der mitwirkenden Verfassungsschutzbehörde geführte Sicherheitsüberprüfungsakte bleibt nach wie vor ausgeschlossen. Die Akte enthält aber die Überprüfungsfeststellungen gfl. unter Einschluß der bei den Referenzpersonen gewonnenen Befragungsergebnisse, also ebenso hochsensible wie „weiche" Daten. Immerhin sollen diese Unterlagen erst fünf Jahre nach Ausscheiden des Betroffenen aus der sicherheitsempfindlichen Tätigkeit vernichtet werden.

Es sollte auch jetzt noch geprüft werden, ob der mit alledem verbundene Eingriff nur dann verhältnismäßig ist, wenn ein Einsichtsrecht auch für die Sicherheitsüberprüfungsakten vorgesehen wird, dessen Gewährung im Einzelfall vom Ergebnis einer Abwägung des informationellen Selbstbestimmungsrechts des Betroffenen einerseits sowie bestimmten, näher zu definierenden Sicherheitsbelangen des Staates und den Rechten der Referenzpersonen andererseits abhängt.

6.2 Führung der Sicherheitsüberprüfungsakten beim Verfassungsschutz

Sicherheitsüberprüfungsakten werden beim Verfassungsschutz über diejenigen Personen geführt, die Zugang zu im öffentlichen Interesse geheimhaltungsbedürftigen Tatsachen, Gegenständen oder Erkenntnissen erhalten oder sich verschaffen können und hierfür überprüft werden, bevor der zuständige Geheimschutzbeauftragte der Dienstbehörde die entsprechende Ermächtigung ausspricht.

Die Akten wurden stichprobenweise an mehreren Tagen überprüft. Die Auswahl erfolgte nach dem Zufallsprinzip. Alle erforderlichen Auskünfte und Erläuterungen wurden seitens des Verfassungsschutzes bereitwillig gegeben.

Das Ergebnis kann im wesentlichen wie folgt zusammengefaßt werden:

Der zahlenmäßige Rahmen der zu überprüfenden Personen ist weit gespannt; er reicht von der bis „streng geheim" überprüften Telefonistin eines Polizeipräsidiums über eine Pressereferentin bis zum Hausmeister, der gelegentlich auch als Fahrer eingesetzt wird. Im Blick auf die auch aus der Sicht des Datenschutzes unabhängig von geltenden Richtlinien allgemein wünschenswerte Reduzierung der Überprüfungsfälle sollten engere Kriterien für deren Notwendigkeit überlegt werden.

Erst in jüngerer Zeit werden im Blick auf die vorgeschriebenen Fristen für die Aktenvernichtung Wiedervorlagevermerke angebracht. So fehlte der Wiedervorlagevermerk z. B. in der Akte eines Beamten, der bei der Ermächtigung 63 Jahre alt war und zwischenzeitlich aus dem Dienst ausgeschieden sein dürfte.

In einer Reihe von Akten befanden sich Listen von zu überprüfenden, bereits überprüften sowie ausgeschiedenen Personen, die von den Geheimschutzbeauftragten der einzelnen Behörden vorgelegt werden. Dabei sind nicht selten die Listen abgelichtet und komplett zur Akte jedes Betroffenen genommen. Zu den in den Listen enthaltenen Namen ist zumeist auch das Geburtsdatum aufgeführt. In einem Fall hat eine Bezirksregierung auf diese Weise 54 Namen von Betroffenen aufgeführt, die zur Wiederholungsprüfung anstanden.

Ein von einer ermächtigten Person eingereichter Reisebericht über eine Gruppenfahrt in den Ostblock enthält eine Liste von 21 Fahrtteilnehmern ohne jeden Bezug zu Sicherheitsbelangen. Für jeden Fahrtteilnehmer waren außer dem Namen und der Wohnanschrift das Geburtsdatum, der Beruf und die Paßnummer eingetragen.

In einem Fall hatten offenbar anfänglich Zweifel gegen eine Ermächtigung bestanden, die sich in umfangreichen Vermerken und Befragungsprotokollen auch des Betroffenen niederschlugen. Hier wäre aus der Sicht des Datenschutzes die Zusammenfassung des Überprüfungsergebnisses in einem Bericht unter Weglassung irrelevanter Hinweise und Bemerkungen der bessere Weg gewesen. Zumindest hätten entkräftete Verdachtspunkte durch einen ergänzenden Hinweis in der Akte klargestellt werden sollen.

In einem Fall war überprüft worden, obwohl der Betroffene im Fragebogen sich mit der Speicherung eigener Daten „nicht einverstanden" erklärt hatte.

Die Ergebnisse der Befragung von Referenzpersonen sind in verschiedenen Fällen zu breit dargestellt. Nicht immer ist die Wiedergabe der Gesprächsinhalte auf das in den Richtlinien geforderte notwendige Minimum beschränkt. Damit werden Behauptungen gespeichert, deren Gegenstand für die Zwecke des Geheimschutzes nicht erforderlich ist. Dies gilt insbesondere für folgende Bereiche:

Medizinische Daten: Klagen über Gallenbeschwerden, Hinweise auf den Krankenstand, Totgeburt, Schilddrüsenerkrankung.

Berufliche Leistungsdaten: Hinweise auf berufliche Fähigkeiten und Leistungsvermögen, zumeist gegeben von ehemaligen Kollegen und Vorgesetzten.

Höchstpersönliche Angelegenheiten: Zum Beispiel die Betroffene hat früher ein Verhältnis mit einem Studenten gehabt – mit weiteren Einzelheiten –. Oder: Beurteilungen ohne jeden Geheimschutzbezug über den Zustand und die Entwicklung einer Ehe.

Politische Daten: Die Frage nach der Stellung des Betroffenen gegenüber der freiheitlich-demokratischen Grundordnung wird nicht selten mit der Mitteilung seiner Parteizugehörigkeit oder sogar mit Hinweisen auf sein wahrscheinliches Wahlverhalten beantwortet.

Der LfD hat empfohlen:

a) Es ist zu prüfen, ob in Zukunft anstelle der gesonderten und detaillierten Wiedergabe der Gespräche mit Referenzpersonen vermehrt zusammenfassende Schlußberichte zu fertigen und zu den Akten zu nehmen sind.

b) Gleichwohl verwendete Befragungsprotokolle sollten auf das sachlich notwendige Minimum beschränkt bleiben und grundsätzlich keine Angaben über Gesundheit, Intimangelegenheiten, dienstliche Leistungen, Daten Dritter und Parteizuordnungen enthalten, es sei denn, es liegt gerade in diesen Feststellungen ein unmittelbarer Geheimschutzbezug.

c) Enthält eine Akte den Niederschlag umfangreicher Ermittlungen und Entscheidungsprozesse, sollte nach einer gewissen Zeit (etwa nach zehn Jahren) geprüft werden, ob derartige Vorgänge entfernt werden können, wenn sich in der Zwischenzeit die Zweifel als unbegründet erwiesen haben. Bei umfangreichen Akten könnte das bereits jetzt sukzessive geschehen.

d) Listen mit Daten anderer Personen dürfen in den Akten nicht enthalten sein.

e) Soweit bei früheren Vorgängen trotz fehlender Zustimmung von Betroffenen Überprüfungen stattfanden, sollte in geeigneter Weise ein rechtmäßiger Zustand hergestellt werden.

f) Es sollte ebenfalls in geeigneter Weise darauf hingewirkt werden, daß die Anzahl der Überprüfungsfälle und der Aktenbestand weiter abnehmen. Der Gesamtbestand der Akten ist zwar innerhalb von zweieinhalb Jahren um ein gutes Drittel verringert worden, erscheint aber mit 6 574 noch als beträchtlich hoch.

6.3 Soll der Verfassungsschutz in die Bekämpfung der organisierten Kriminalität einbezogen werden?

Ein Aspekt der bundesweiten Diskussion über die Verbesserung der öffentlichen Sicherheit ist der Vorschlag, den Verfassungsschutz bei der Bekämpfung der organisierten Kriminalität zu beteiligen; er soll ihre Strukturen und ihre Entwicklungen im Vorfeld beobachten. In einem Bundesland haben diese Überlegungen bereits in einem Gesetzentwurf konkret Gestalt angenommen.

Wenn hier vor der Realisierung solcher Bestrebungen gewarnt wird, so geschieht das nicht etwa in Verkennung der effektiven Gefahren, die von der organisierten Kriminalität für den einzelnen Bürger und ebenso für das Gemeinwesen ausgehen. Es sind vielmehr rechtsgrundsätzliche und auch praktische Bedenken, die die Einbeziehung des Verfassungsschutzes in die Verbrechensbekämpfung derzeit als unzulässig und überhaupt als ungeeignetes Mittel erscheinen lassen.

Die Befürworter bleiben zunächst die Erläuterung schuldig, an welcher Stelle und in welcher Form der Einsatz des Verfassungsschutzes in der Praxis beginnen soll und wo er zu enden hat. Die bislang wenig leistungsfähigen und mehr beschreibenden Definitionen der organisierten Kriminalität eignen sich in diesem Zusammenhang nicht als gesetzliches Tatbestandsmerkmal zu einer abgrenzenden Aufgabenzuweisung, denn in der Praxis ist eine Trennung von organisierter Kriminalität und Alltagskriminalität so gut wie unmöglich. Der Verfassungsschutz würde geradezu zwangsläufig tief in die allgemeine Straftatenbekämpfung hineingezogen. Hieran knüpfen ernsthafte Zweifel, ob sein Personal aufgrund der bisherigen Aufgabenstellung und Praxis ohne zusätzliche gründliche Ausbildung mit Erfolgsaussicht eingesetzt werden könnte. Der Vorschlag wäre also – wenn überhaupt – nur mit erheblicher Zeitverzögerung zu verwirklichen.

Sicherlich würden auch die unterschiedlichen Eingriffsbefugnisse von Polizei und Verfassungsschutz eine an den Vorgaben des Grundgesetzes orientierte gesetzliche Regelung erfordern. So kann z. B. derzeit der Verfassungsschutz unter näher bestimmten Voraussetzungen nachrichtendienstliche Mittel zur Informationsgewinnung einsetzen, wozu auch der Einsatz elektronischer Abhöreinrichtungen in Wohnungen gehört. Deren allgemeine Verwendung zu Zwecken der Strafverfolgung wird aber von Artikel 13 des Grundgesetzes in seiner gegenwärtigen Fassung nicht gedeckt (siehe hierzu die Diskussion um den sog. „Großen Lauschangriff"). Die aus einer entsprechenden Informationsbeschaffung gewonnenen Erkenntnisse könnten also grundsätzlich nicht ohne Umgehung des Grundgesetzes an die Strafverfolgungsbehörden übermittelt werden.

In diesem Zusammenhang ist auf die Notwendigkeit einer ebenso transparenten wie effektiven Ausgestaltung der Rechtswegegarantie für einen erweiterten Eingriffsbereich des Verfassungsschutzes hinzuweisen.

Als unmittelbare Folge für den Datenschutz würden sich die unterschiedlichen Kontrollbefugnisse der Datenschutzbeauftragten bei der Polizei einerseits und dem Verfassungsschutz andererseits auswirken. Verschiedene Maßnahmen des Verfassungsschutzes werden nicht durch die Datenschutzbeauftragten, sondern von den G-10-Kommissionen bzw. von den Parlamentarischen Kontrollkommissionen überprüft. Für den Verfassungsschutz besteht auch keine Pflicht zur Anmeldung seiner Dateien. Weiterhin können in bestimmten Fällen dem Datenschutzbeauftragten Einsichtnahmen in Akten und Unterlagen verweigert werden (Ministervorbehalt). Durch diese Reduktion der Kontrollmöglichkeiten entstünde überdies ein nicht unerhebliches Transparenzdefizit. Dies würde noch durch die gegenüber dem Strafverfahren und dem Polizeirecht unterschiedlichen Zuständigkeitsabgrenzungen zwischen den Verfassungsschutzbehörden des Bundes und der Länder vergrößert. So setzt das Tätigwerden des Bundesamtes für Verfassungsschutz in einem Lande nur das Benehmen mit dessen Verfassungsschutzbehörden voraus, wenn das Bundesamt selbst bestimmte Voraussetzungen als gegeben annimmt.

Sollte jedoch tatsächlich beabsichtigt sein, die angesprochenen Fragen gesetzlich zu regeln, um den Einsatz des Verfassungsschutzes bei der Bekämpfung der organisierten Kriminalität zu ermöglichen, so wäre dies ganz gewiß nicht ohne eine erhebliche Vergrößerung der jetzt schon von der polizeilichen Praxis zu Recht beklagten Regelungsdichte denkbar.

7 Justiz

7.1 Allgemeines

7.1.1 Kompetenzkonflikte

Erneut gab es Meinungsverschiedenheiten über den zulässigen Umfang der Tätigkeiten des LfD im Bereich des Ministeriums der Justiz.

Es war erforderlich, in Gesprächen mit dem Minister der Justiz auf die zurückliegenden Absprachen hinzuweisen, die bereits eine deutliche Beschränkung der Tätigkeit des LfD darstellen. Dennoch gab es im nachgeordneten Bereich Bestrebungen, hinter diese Regelungen zurückzugehen.

Um den Dissens über die Kontrollbefugnisse der Datenschutzkommission im Bereich der herkömmlichen (manuellen) Datenspeicherung auch angesichts der erwarteten raschen gesetzlichen Neuregelung im Wege des Kompromisses praktisch zu überwinden, war Einigkeit erzielt worden, die Sachaufklärung in laufenden Ermittlungsverfahren der Staatsanwaltschaften nur über das Ministerium der Justiz zu betreiben, wenn der Bereich der Datenspeicherung in Akten betroffen ist. Mit diesem Inhalt hat der LfD diese seinerzeit mit der DSK getroffene Vereinbarung auch für seine Person bestätigt.

Dem Anliegen, daß der Verkehr zwischen dem Datenschutzbeauftragten und den Justizbehörden generell – insbesondere soweit die Sachaufklärung betroffen ist – nicht unmittelbar, sondern nur mit dem Ministerium der Justiz abgewickelt werden solle, konnte der LfD nicht entsprechen. Eine derartige Abrede existiert im gesamten Landesbereich mit keiner anderen obersten Landesbehörde. Im Verhältnis zum LfD ist dieses Verfahren gesetzlich nicht vorgesehen und auch nicht üblich. Schließlich ist auch nicht ersichtlich, daß im Justizbereich außerhalb der rechtsprechenden Tätigkeit Besonderheiten existierten, die gerade hier erforderlich machen würden, die Befugnisse des LfD in dieser Weise zu beschränken. Insbesondere bei der Bearbeitung von Eingaben betroffener Bürger kommt dem Gesichtspunkt der zeitnahen Erledigung erhebliche Bedeutung zu. In welchem Umfang hier Verzögerungen durch die Einschaltung der obersten Aufsichtsbehörde eintreten können, haben konkrete Eingaben gezeigt. So hat etwa die Weiterleitung eines unveränderten Antwortschreibens einer Staatsanwaltschaft auf dem Dienstweg über das Ministerium der Justiz eine Zeitverzögerung von ca. drei Monaten verursacht.

Auch der anläßlich der Novellierung des LDatG erhobenen Forderung des Ministeriums der Justiz, die Kompetenzen des LfD in laufenden Strafverfahren gesetzlich deutlich zu beschränken, mußte der LfD im Interesse eines wirksamen Datenschutzes widersprechen, zumal die Erörterung der konkreten Tätigkeit sowohl der DSK wie des LfD keinen Fall hat erkennen lassen, in dem die Einschaltung des LfD zu Behinderungen der Tätigkeit der Justizbehörden geführt hätte. Nach persönlichen Gesprächen mit dem Minister der Justiz konnte schließlich weitgehend Einigkeit erzielt werden.

7.1.2 Gesetzliche Defizite

Die Praxis des Datenschutzes im Bereich der Justiz wird dadurch erheblich beeinträchtigt, daß notwendige gesetzliche Regelungen – die durch den Bundesgesetzgeber zu erlassen wären – noch fehlen. Zu nennen sind hierbei insbesondere das Justizmitteilungsgesetz sowie die datenschutzrechtlichen Ergänzungen des Strafvollzugsgesetzes, der Strafprozeßordnung sowie der Zivilprozeßordnung. In die Strafprozeßordnung sind zwar im Zusammenhang mit dem Gesetz zur organisierten Kriminalität Neuregelungen eingefügt worden, diese sollen jedoch primär der Effektivität der polizeilichen Aufklärungsarbeit und nicht dem Datenschutz der Betroffenen dienen. Aus den bisher vorliegenden Entwürfen zur Ergänzung der Strafprozeßordnung sind also diejenigen Regelungen nicht in das Gesetz aufgenommen worden, die primär dem Schutz der Betroffenen dienen. Es ist daran zu erinnern, daß nach wie vor eine Regelung über den genetischen Fingerabdruck (die Genomanalyse) zu Strafverfolgungszwecken in der StPO fehlt; ebenso fehlen allgemeine Rechtsgrundlagen für die Datenverarbeitung durch die Staatsanwaltschaften.

Im Bereich der Zivilprozeßordnung macht sich das Fehlen datenschutzfreundlicher Regelungen zum Schuldnerverzeichnis besonders negativ bemerkbar.

Außerdem ist hier an die fehlenden Protokollierungsregelungen für Einsichtnahmen in die gerichtlichen Register zu erinnern. Näheres hierzu wird unten ausgeführt.

Die Justizverwaltungen der Bundesländer können sich freilich in diesem Zusammenhang nicht darauf berufen, daß diese Untätigkeit des Gesetzgebers nicht auch in ihren Verantwortungsbereich falle. Insbesondere die Bedenken der Landesjustizverwaltungen dürften nämlich verhindert haben, daß etwa das Strafvollzugsgesetz mit seinen datenschutzrechtlichen Ergänzungen und das Justizmitteilungsgesetz verabschiedet worden sind.

Der LfD appelliert eindringlich an den Minister der Justiz, weiterhin das in seiner Macht Stehende zu tun, den hier zu konstatierenden Stillstand zu überwinden.

7.1.3 Aufbewahrungsfristen – Wie lange soll die Justiz wissen, was sie getan hat?

Die Frage, wie lange Unterlagen, Akten gerichtlicher Entscheidungen, Karteien und Protokollbücher aufzubewahren sind, hat für das informationelle Selbstbestimmungsrecht der Betroffenen eine herausragende Bedeutung.

In der Vergangenheit wurden entsprechende Bestimmungen (die im Bereich der Justiz bundeseinheitlich als Verwaltungsvorschriften erlassen sind), primär – wenn nicht ausschließlich – unter dem Gesichtspunkt der Lagerkapazität und der praktischen Bedürfnisse beurteilt. Datenschutzüberlegungen, also Überlegungen, welche die Rechte der Betroffenen zum Ausgangspunkt haben, und für die das Vernichten von Vorgängen ein Ausdruck der „Gnade des Vergessens" ist, die für jeden Bürger wichtig sein kann, haben bei der Formulierung der entsprechenden Fristen in der genannten Verwaltungsvorschrift in der Vergangenheit sicher keine besondere Rolle gespielt.

Dieser Themenkreis wird künftig an Bedeutung zunehmen: Bislang war es nicht sehr bedeutsam, daß sich Urteile und Strafbefehle, die sich auf Bagatelldelikte bezogen haben (etwa auf eine unbedeutende Geldstrafe wegen eines Warenhausdiebstahls), 30 Jahre im Keller einer Staatsanwaltschaft befunden haben. Im Regelfall nach zehn, spätestens nach 15 Jahren war es praktisch unmöglich, ein solches Urteil ohne die Kenntnis des Aktenzeichens noch zu finden. Die Findmittel, die an den Namen des Betroffenen anknüpften, waren nämlich nach diesem Zeitraum im allgemeinen – primär aus Platzgründen – vernichtet. Ein möglicherweise bestehendes Interesse des Betroffenen, auch nach Zeiträumen von 20 bis 30 Jahren noch das Urteil zum Nachweis möglicherweise auch eines Freispruches noch erhalten zu können, wurde dadurch gewahrt, daß der Betroffene unter Nennung des Aktenzeichens bei der zuständigen Staatsanwaltschaft in sein Urteil Einblick nehmen konnte bzw. auch eine Kopie erhalten konnte.

Wenn aber die Urteile selbst in automatisierter Form erfaßt sind oder wenn chronologische Findmittel, die vom Aktenzeichen ausgehen (wie das Js-Register), automatisiert erfaßt werden, dann begründet die Technik der EDV die Möglichkeit, nach jedem beliebigen gespeicherten Begriff zu suchen und damit auch beispielsweise unter dem Namen Informationen über lange zurückliegende Bagatelldelikte abzurufen.

Wenn also die Aufbewahrungsfristen der genannten Verwaltungsvorschrift unbesehen auch für die Bemessung von Speicherfristen bei Nutzung der EDV übernommen werden, kommt es im Vergleich zur bisherigen Lage zu erheblichen zusätzlichen Eingriffen in die Rechte der Betroffenen. Insbesondere auch die Wertungen des Bundeszentralregistergesetzes mit seinen strikten Tilgungsregelungen würden dadurch weitgehend wirkungslos werden. Vor dem Hintergrund der beabsichtigten Einrichtung staatsanwaltschaftlicher Informationsverbundsysteme würde also – wenn nicht rechtzeitig einschränkende Regelungen getroffen werden – das abgewogene System des Bundeszentralregisters ausgehebelt werden. Diese Überlegungen betreffen aber nicht nur den Bereich des Strafrechts. Dienstordnungsverfahren, Verwaltungsstreitverfahren und auch

zivilrechtliche Auseinandersetzungen können bei zu langfristigen Zugriffsmöglichkeiten ähnlich belastende Auswirkungen wie die zweckwidrige Verwendung von Informationen aus lange zurückliegenden Strafverfahren haben.

Aus der Sicht des LfD sind hier folgende Forderungen zu erheben:

- Für die Aufbewahrung und Löschung von Daten sowohl in den Akten als auch in den Dateien der Justiz müssen besondere gesetzliche Regelungen geschaffen werden.
- Es ist unzulässig, bei einer Aufbewahrung von Daten auf Bild- oder Datenträgern, die an die Stelle der Urschriften getreten sind, die jeweils längste Aufbewahrungsfrist einzelner Teile (z. B. Urteile) zum Maßstab der Dauer der Aufbewahrung des gesamten Datenträgers zu machen.
- Bei der automatisierten Speicherung von Urteilen bzw. von Strafbefehlen ist die derzeit geltende generelle 30jährige Aufbewahrungsfrist nicht angemessen. Hier ist nach der Schwere der verhängten Sanktion zu differenzieren und ein Gleichlauf mit den Tilgungsfristen des Bundeszentralregistergesetzes anzustreben.
- Bei der Berechnung des Beginns von Aufbewahrungsfristen muß an den Termin der Rechtskraft der ergangenen Entscheidung angeknüpft werden.
- Bei Akten, die mehrere Täter betreffen, ist eine Teilsperrung bezüglich solcher Aktenteile vorzusehen, die einzelne Täter betreffen, wenn deren Unterlagen eigentlich gelöscht werden müßten, aus praktischen Grüßen aber keine Vernichtung erfolgen kann.
- Insgesamt sind die Aufbewahrungsfristen im Detail daraufhin zu überprüfen, ob in einzelnen Bereichen nicht Verkürzungen in Betracht kommen. Dabei ist eine Differenzierung nach der Art der Speicherung (in automatisierten Verfahren oder in Akten) angemessen. Die Löschungsfristen für die automatisierten Systeme sind besonders restriktiv, orientiert am informationellen Selbstbestimmungsrecht und an den Konkretisierungen dieses Grundrechts im Bundeszentralregistergesetz, festzulegen. Eine einfache Übernahme der Systematik der Aufbewahrungsbestimmungen in das Gesetz verbietet sich.
- Die Frage der Vernichtung der Karteikarten des zentralen Namensverzeichnisses (Nr. 602 AufbewBest) sollte so gelöst werden, daß die Vernichtung der Karteikarte gleichzeitig mit der Vernichtung der Akte erfolgt. Zu klären bliebe aber wohl, welche Findmittel bzgl. der aufbewahrten Urteile und Strafbefehle zur Verfügung stehen sollen (Problem der – u. U. auch automatisiert geführten – Js-Register).

Wesentliche Forderungen in diesem Zusammenhang hat die Konferenz der Datenschutzbeauftragten bereits 1986 in einem Beschluß formuliert. Die Konferenz hat betont, daß die Aufbewahrung und Löschung der Daten sowohl in den Akten als auch in den Dateien der Justiz gesetzlich geregelt werden muß (Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 24./25. November 1986). Sie hat darauf hingewiesen, daß die maßgebenden Fristen gekürzt werden sollten und in jedem Fall unter Berücksichtigung des Verfahrensausganges und der Schwere der Tat stärker abgestuft werden müßten. Die Löschungsbestimmungen für automatisierte Systeme seien gesondert zu regeln.

Diesen Anforderungen wurde bis heute nicht entsprochen.

Im Gegenteil: Ohne Einbeziehung der Datenschutzbeauftragten haben die Landesjustizressorts einheitlich im Juli 1993 Änderungen der untergesetzlichen Aufbewahrungsbestimmungen beschlossen, die den datenschutzrechtlichen Bestrebungen teilweise zuwiderlaufen, sie im übrigen aber ignorieren.

Der LfD bemüht sich darum, eine abgestimmte Stellungnahme der Datenschutzbeauftragten herbeizuführen, um die Justizverwaltungen der Bundesländer von den genannten grundsätzlichen datenschutzrechtlichen Anforderungen zu überzeugen. Eine Korrektur, die sich auf die Verkürzung weniger Fristen beschränken und die genannten grundsätzlichen datenschutzrechtlichen Anliegen ausblenden würde, wäre unzureichend.

7.1.4 Interne Urteilssammlungen der Gerichte

Zumindest bei den Obergerichten des Landes (Oberlandesgerichte, Oberverwaltungsgericht, Landesarbeitsgericht, Landessozialgericht) werden neben den Verfahrensakten auch zu Zwecken der allgemeinen Rechtsinformation gesonderte Urteilssammlungen geführt. Die in diese Sammlungen aufgenommenen Urteile sind nicht anonymisiert. Sie stehen allen interessierten Gerichtsangehörigen zur Information zur Verfügung.

Aus datenschutzrechtlicher Sicht hat der LfD gefordert, daß derartige Urteile jedenfalls zu dem Zeitpunkt anonymisiert werden, zu dem ihre Aufbewahrung in personenbezogener Form nach den Aufbewahrungsbestimmungen der Justiz unzulässig geworden ist.

Die Erfüllung dieser Forderung trifft jedoch derzeit noch auf erhebliche Widerstände: So argumentieren die Gerichtsverwaltungen zum einen, daß eine solche Anonymisierung einen erheblichen Arbeitsaufwand verursachen würde; zum anderen sind sie der Auffassung, daß bei komplizierteren Sachverhalten die Verständlichkeit leiden würde, wenn die Namen entfernt bzw. gelöscht würden.

Aus der Sicht des LfD wird jedoch spätestens bei der automatisierten Führung solcher Urteilssammlungen das Argument des Arbeitsaufwandes keine entscheidende Rolle mehr spielen. Dann allerdings wäre auch der Zeitpunkt gekommen, zu dem aus datenschutzrechtlicher Sicht eine Anonymisierung bereits bei der Einspeicherung von Urteilen in die automatisiert geführte Urteilssammlung durchzuführen wäre. Der LfD wird dieses Anliegen auch weiterhin verfolgen.

7.2 Ziviljustiz

7.2.1 Der beleidigte Richter

Aufgrund einer Eingabe ist der LfD mit der auch in anderen Zusammenhängen bedeutsamen Frage konfrontiert worden, ob bei schriftlichen beleidigenden Äußerungen gegenüber einem Richter und gegenüber anderen Verfahrensbeteiligten (im vorliegenden Fall im Kostenfestsetzungsverfahren nach Abschluß des eigentlichen Verfahrens) der Richter das Recht besitzt, den Staatsanwalt sowie die anderen beleidigten Personen über den Vorgang durch Übersendung des beleidigenden Schriftsatzes zu informieren.

In dem dem LfD aufgrund einer Eingabe zur Kenntnis gelangten Fall war es durchaus zweifelhaft, ob tatsächlich eine Beleidigung des Richters und der Zeugen vorgelegen hat. Dies kann jedoch dahinstehen. Die zu entscheidende Rechtsfrage war unter der Voraussetzung zu entscheiden, daß der tätigwerdende Richter eine Beleidigung für gegeben ansah.

Das Ministerium der Justiz beurteilte diesen Sachverhalt wie folgt: Wenn ein Richter in einem im Verfahren vorgelegten Schriftsatz beleidigt werde, so habe er grundsätzlich das Recht, Strafanzeige zu erstatten und zu diesem Zweck den Schriftsatz nebst Verfahrensakten der Staatsanwaltschaft zuzuleiten. Seine Berechtigung hierzu folge letztlich aus der grundgesetzlich geschützten Menschenwürde, Artikel 1 Abs. 1 GG.

Diesen Ausführungen stimmt der LfD im Ergebnis zu. Allerdings hält er es für zweifelhaft, ob Rechtsgrundlage für eine entsprechende Übermittlung an die Staatsanwaltschaft tatsächlich die verfassungsrechtlich geschützte Menschenwürde ist oder ob sich eine Rechtsgrundlage nicht auch schon aus dem allgemeinen Persönlichkeitsrecht ergibt. Klärungsbedürftig ist aber insbesondere, ob die die Datenübermittlung an die Staatsanwaltschaft betreffende Entscheidung des Richters als dienstliche Handlung anzusehen ist (dann wäre vor allem auch der Verhältnismäßigkeitsgrundsatz zu beachten, s. u.) oder ob sie dem privaten Bereich des Richters zuzuordnen ist. Letzteres entspricht der Auffassung des LfD.

Die zweite Frage, die zur Entscheidung anstand, ist, ob der Richter auch die anderen betroffenen Verfahrensbeteiligten durch Übersendung einer Kopie des betreffenden Schriftsatzes unterrichten darf, soweit diese betroffen sind. Das Ministerium der Justiz hatte auch gegen die Übersendung einer Kopie des betreffenden Schriftsatzes an die hiervon ebenfalls betroffenen Zeugen (im vorliegenden Fall Polizeibeamten) aus datenschutzrechtlicher Sicht keine Bedenken. Unter dem Gesichtspunkt der aus dem Rechtsstaatsprinzip abzuleitenden nachprozessualen Fürsorgepflicht sei die Übersendung gerechtfertigt gewesen. Der Richter brauche und dürfe es nicht hinnehmen, daß die im Verfahren gehörten Zeugen aus Anlaß und im Zusammenhang mit ihrer Zeugenstellung von dem Betroffenen beleidigt werden. Die Unterrichtung der Zeugen durch Übersendung einer Schriftsatzkopie stelle sich als adäquate Maßnahme dar, um der nachwirkenden Fürsorgepflicht Rechnung zu tragen.

Diese Auffassung erscheint dem LfD zweifelhaft. Fraglich ist insbesondere, ob die nachprozessuale Fürsorgepflicht als Ausfluß des Rechtsstaatsprinzips den Richter tatsächlich zu einer solchen Datenübermittlung berechtigt. Aufgabe des Richters ist es sicherlich, Zeugen gegen Angriffe oder Ehrverletzungen durch einen Angeklagten unter Ausnutzung der gerichtsverfassungsrechtlichen Mittel in der Hauptverhandlung zu schützen (§§ 177, 178 GVG). Ob allerdings ein Schutzbedürfnis in gleicher Weise in einem nachprozessualen schriftlichen Verfahren (wie hier im Kostenfestsetzungsverfahren) besteht, ist durchaus nicht selbstverständlich. Die hier vorgenommene Zweckänderung bedürfte wohl grundsätzlich einer gesetzlichen Regelung. Unabhängig davon handelt es sich bei einer Datenübermittlung in einem solchen Zusammenhang jedenfalls um die Wahrnehmung einer dienstlichen Aufgabe. Dann ist das Verhältnismäßigkeitsprinzip zu beachten. Hilfreich für die Konkretisierung des Verhältnismäßigkeitsgrundsatzes in diesem Zusammenhang ist Nr. 232 RiStBV.

Diese Vorschrift lautet wie folgt:

„Nr. 232 RiStBV, Beleidigung von Justizangehörigen, Abs.2:
Wird in Beschwerden, Gnadengesuchen oder ähnlichen Eingaben an Entscheidungen und anderen Maßnahmen von Justizbehörden oder Angehörigen in beleidigender Form Kritik geübt, so ist zu prüfen, ob es sich um ernstzunehmende Ehren-

kränkungen handelt und es zur Wahrung des Ansehens der Rechtspflege geboten ist, einzuschreiten. Offenbar haltlose Vorwürfe unbelehrbarer Querulanten oder allgemeine Unmutsäußerungen von Personen, die sich in ihrem Recht verletzt glauben, werden regelmäßig keine Veranlassung geben, die öffentliche Klage zu erheben, es sei denn, daß wegen falscher Verdächtigung vorzugehen ist."

Zwar betrifft diese Regelung nur die Frage, wann die öffentliche Klage in diesem Zusammenhang durch die Staatsanwaltschaft zu erheben ist. Dennoch tendiert der LfD dazu, auch Datenübermittlungen an Dritte durch den Richter nur unter den Voraussetzungen für zulässig zu halten, unter denen für die Staatsanwaltschaft die Erhebung der öffentlichen Klage in Betracht käme. Die genannten Fragen werden derzeit noch im Kreis der Datenschutzbeauftragten erörtert.

7.2.2 Offenbarungen im Zusammenhang mit der Prozeßkostenhilfe

Mehrmals wurde von Beschwerdeführern vorgetragen, die Gerichte würden im Zusammenhang mit der Beantragung von Prozeßkostenhilfen zu umfangreiche Einkommensnachweise fordern. So wandte sich der neue Ehemann einer geschiedenen Frau dagegen, daß er gegenüber dem Gericht im Rahmen des Prozeßkostenhilfeverfahrens für die Scheidung seiner neuen Ehefrau seine Einkommensverhältnisse offenbaren sollte, obwohl er mit dem Scheidungsverfahren nichts zu tun und außerdem Gütertrennung vereinbart hätte. Ergänzend wandte er sich dagegen, daß nun seine Ehefrau einen vollständigen Überblick über seine Einkommensverhältnisse erhalten hätte.

Abgesehen davon, daß diese Fragen grundsätzlich in den Bereich der richterlichen Unabhängigkeit fallen und vom LfD nicht im Einzelfall zu überprüfen sind, hat der LfD den Beschwerdeführer darauf hingewiesen, daß die zivilprozessualen Regelungen, die die Berechnung des maßgeblichen Einkommens für die Prozeßkostenhilfe betreffen und aus denen folgt, daß das Einkommen von Unterhaltsverpflichteten bei der Berechnung der Bedürftigkeit von Prozeßkostenhilfeberechtigten zu berücksichtigen ist, dem allgemeinen Datenschutzrecht vorgehen.

Auch dagegen, daß die Ehefrau über die Einkünfte ihres Ehemannes bei Gelegenheit dieses Prozeßkostenhilfeverfahrens informiert worden ist, waren keine datenschutzrechtlichen Bedenken zu erheben. Abgesehen davon, daß die Ehefrau einen gesetzlichen Auskunftsanspruch über die Einkünfte des ihr unterhaltsverpflichteten Ehemannes besitzt, war es unabdingbar, in den entsprechenden Beschluß auch diese Informationen aufzunehmen.

7.2.3 Umfang der Auskunftspflicht eines Psychologen im Zwangsvollstreckungsverfahren

Die Frage, ob ein Psychologe im Rahmen der Abgabe der eidesstattlichen Versicherung dazu verpflichtet ist, auch die gegenüber seinen Patienten bestehenden offenen Forderungen anzugeben, wurde dem LfD durch ein Gericht vorgelegt. Sie stellt sich sowohl im Bereich der zivilgerichtlichen Zwangsvollstreckung (hier wäre der LfD wegen der richterlichen Unabhängigkeit, an der auch die Rechtspfleger teilhaben, nicht zuständig), als auch in Bereichen, die der vollen Kontrollkompetenz des LfD unterliegen: Dies ist insbesondere dann der Fall, wenn Vollstreckungsbeamte der Finanzverwaltung gem. § 284 Abgabenordnung (AO) die eidesstattliche Versicherung abnehmen und in diesem Zusammenhang ein Vermögensverzeichnis zu erstellen ist. Die hier bestehenden Fragen hat der LfD wie folgt beurteilt:

a) Die Erstellung des Vermögensverzeichnisses im Rahmen der Abgabe einer eidesstattlichen Versicherung (§ 284 Abs. 1 AO; § 807 Abs. 1 ZPO) ist als Datenerhebung durch öffentliche Stellen (sei es die Vollstreckungsstelle des Finanzamts oder das Vollstreckungsgericht) anzusehen. Diese Datenerhebung führt zu einer Speicherung von Informationen in Akten. Die Phasen der Erhebung sowie der Speicherung (außerdem aber auch die möglichen weiteren Übermittlungen an andere Verfahrensbeteiligte oder Dritte) sind jeweils bereichsspezifisch in der Abgabenordnung oder in der Zivilprozeßordnung geregelt, das Landesdatenschutzgesetz kommt daneben schon deshalb nicht zur Anwendung. Außerdem wären die Datenverarbeitungsregelungen des Landesdatenschutzgesetzes (insbesondere §§ 5, 6 und 7) auch wegen des fehlenden Dateibezuges der in Rede stehenden Datenspeicherung nicht anwendbar (§ 2 Abs. 2 LDatG).

b) Die Frage, ob und welche Geheimhaltungsrechte bzw. -pflichten des Vollstreckungsschuldners auch gegenüber der Offenbarungspflicht in den genannten Vorschriften der Abgabenordnung und der Zivilprozeßordnung bestehen, ist damit ebenfalls den Datenschutzgesetzen nicht zu entnehmen (das Bundesdatenschutzgesetz bleibt außer Betracht, weil die Datenerhebung und -verarbeitung im vorliegenden Zusammenhang durch öffentliche Stellen des Landes erfolgt).

c) Eine Geheimhaltungspflicht des Vollstreckungsschuldners, der Berufspsychologe ist, ergibt sich aus § 203 Abs. 1 Nr. 2 Strafgesetzbuch.

Soweit ersichtlich, sind sowohl Rechtsprechung wie Literatur in der Vergangenheit im Zusammenhang mit der Erstellung des Vermögensverzeichnisses nach § 807 ZPO durchgehend allerdings davon ausgegangen, daß der Name und die Höhe der Forderung von Mandanten bzw. Klienten von Ärzten, Steuerberatern und Rechtsanwälten nicht als „Geheimnis" im Sinne des § 203 Abs. 1 StGB anzusehen seien (für die Forderungen eines Rechtsanwalts gegen seine Mandanten siehe Kammergericht Berlin, Beschluß vom 29. November 1984, JR 85, S. 161; Landgericht Frankfurt, Beschluß vom 11. März 1985,

Anwaltsblatt 1985, S. 258; Landgericht Wiesbaden, Beschluß vom 6. Dezember 1976, bestätigt durch das OLG Frankfurt, Beschluß vom 25. Januar 1977, Juristisches Büro 1977, Spalte 728; für Forderungen eines Steuerberaters gegenüber seinen Auftraggebern: Landgericht Lübeck, Beschluß vom 2. August 1988, Rechtspfleger 1989, S. 32; für Honorarforderungen einer Kinderärztin Landgericht Aurich, Beschluß vom 28. September 1970, NJW 1971, S. 252). Mit gleichem Inhalt hat die Kommentarliteratur zu § 807 ZPO – allerdings nur in sehr kursorischer Weise – Stellung genommen (Münzberg in Stein/ Jonas, ZPO-Kommentar, Anm. 34 zu § 807; Ziegler, ZPO-Kommentar, Anm. 24 zu § 807; Hartmann in Baumbach/Lauterbach/ Albers/ Hartmann, Anm. 3 B a zu § 807).

Dies ist schon in den bereits genannten Fällen aus datenschutzrechtlicher Sicht nicht akzeptabel: Der Begriff des Geheimnisses in § 203 Abs. 1 Strafgesetzbuch ist weit zu fassen. Darunter fallen alle diejenigen Informationen, die dem Geheimnisträger im Hinblick auf seine besonders geschützte Funktion zur Kenntnis gelangt sind. Dies ist bereits die Tatsache der Inanspruchnahme der Dienste des betreffenden Geheimnisträgers selbst. Zutreffend behandelt die strafrechtliche Kommentarliteratur die hier zu entscheidende Problematik unter dem Gliederungspunkt „Befugnis" zur Offenbarung von Geheimnissen im Rahmen des § 203 StGB (z. B. Dreher/Tröndle, Anm. 31 zu § 203 StGB).

Jedenfalls in bezug auf einen Berufspsychologen ist höchstrichterlich anerkannt, daß schon die Tatsache seiner Inanspruchnahme als Geheimnis i. S. v. § 203 StGB anzusehen ist und nicht erst die Information über das Problem oder die Krankheit, die Anlaß für die Inanspruchnahme des Psychologen gewesen ist (so wörtlich das BAG im Urteil vom 13. Januar 1987, 1 AZR 267/85, Recht der Datenverarbeitung 87, 136, 139).

d) Der Vollstreckungsschuldner besitzt folglich nur dann eine Offenbarungspflicht im Sinne der §§ 284 AO, 807 ZPO auch bezüglich der Angaben zu seinen Mandanten und den ihnen gegenüber bestehenden noch offenen Forderungen, wenn er eine Offenbarungsbefugnis gem. § 203 StGB hat.

Eine solche Offenbarungsbefugnis im Sinne des § 203 StGB kann insbesondere aus gesetzlichen Offenbarungspflichten folgen. Grundsätzlich begründen die genannten Regelungen der AO sowie der ZPO selbst eine solche Pflicht. Bei einer konkreten Entscheidung über die Reichweite der Offenbarungspflicht ist jedoch das Schutzgut des § 203 StGB, das zumindest in seinem Kern Verfassungsrang besitzt, in angemessener Weise zu berücksichtigen. Dies bedeutet, daß der Datenerhebung und Datenspeicherung eine gesonderte Prüfung der Verhältnismäßigkeit vorauszugehen hat, in der die konkreten Umstände des Falles zu berücksichtigen sind (vergleichbar der Verhältnismäßigkeitsprüfung vor Gestattung der Wohnungsdurchsuchung im Rahmen der Zwangsvollstreckung). Die Höhe der zu vollstreckenden Forderung dürfte hier ebenso zu berücksichtigen sein wie die Zahl der betroffenen Patienten und die für den Gläubiger zu erwartenden realistischen Vorteile.

Insbesondere ist die sensitive Natur der hier betroffenen Informationen einzubeziehen. Bei den Angaben zu den Patienten eines Psychologen handelt es sich ausnahmslos um Daten, die aus ihrer Natur heraus bei Bekanntwerden negative Auswirkungen auf das soziale Umfeld des Betroffenen und seinen persönlichen Geltungsanspruch haben können. Gleiche Auswirkungen dürften aus entsprechenden Informationen über die Konsultation eines Rechtsanwalts, Steuerberaters oder Kinderarztes nur ausnahmsweise folgen. Dies rechtfertigt zwar nicht, das gesetzlich geregelte Vollstreckungsinteresse des Gläubigers generell und ausnahmslos hinter die Geheimhaltungspflicht des Psychologen zurücktreten zu lassen. Ein völliger Ausschluß der Durchsetzung von Forderungspfändungen gegenüber Psychologen wäre wohl als unverhältnismäßige Beeinträchtigung der Rechte des Gläubigers zu werten. Allerdings sind diese Gesichtspunkte im Rahmen der Verhältnismäßigkeitsprüfung angemessen zu berücksichtigen; sie könnten nach Auffassung des LfD durchaus rechtfertigen, von einer entsprechenden Datenerhebung abzusehen.

Bei einer im Ergebnis die Offenbarungspflicht bejahenden Wertung ist das Maß der Offenbarung zu beschränken: Außer der Angabe des Namens und der Anschrift des betroffenen Patienten sowie der Höhe der noch offenen Forderungen sind grundsätzlich keine Angaben zu machen. Es ist von allen Angaben zum Entstehungsgrund der Forderung (Häufigkeit der Inanspruchnahme des Psychologen, Daten der Inanspruchnahme etc.) abzusehen. Nur in diesem Rahmen wäre der gesetzlichen Offenbarungspflicht Folge zu leisten.

e) Ergänzend war darauf hinzuweisen, daß eine Weiterverbreitung von Informationen, die der Gläubiger durch die Kenntnisnahme des Inhalts der eidesstattlichen Versicherung erfahren hat, wohl Schadensersatzansprüche der betroffenen Patienten des Psychologen aus § 823 BGB begründen würde.

7.3 Strafrechtliche Verfahren

7.3.1 Änderungen und Ergänzungen der Strafprozeßordnung

Aus datenschutzrechtlicher Sicht weist die Strafprozeßordnung derzeit noch eine Reihe von erheblichen Defiziten aus: Es fehlen allgemeine Rechtsgrundlagen für die Datenverarbeitung durch die Strafverfolgungsbehörden, insbesondere wenn die

Daten automatisiert verarbeitet werden. Ebenso fehlen gesetzliche Regelungen für die erforderlichen Datenübermittlungen. Für weitere Einzelheiten wird auf das gemeinsam erarbeitete Papier der Datenschutzbeauftragten des Bundes und der Länder verwiesen, das als Anlage 2 zum 11. Tb. veröffentlicht worden ist.

Bislang sind in diesem Zusammenhang nur solche Neuregelungen in der Strafprozeßordnung erfolgt, die die Effektivität der Strafverfolgung steigern sollen (Regelungen zur Rasterfahndung, zum Einsatz verdeckter Ermittler etc.). Nach den dem LfD vorliegenden Informationen ist auch geplant, Regelungen für staatsanwaltschaftliche Informationsverbundsysteme einzuführen, ohne die ansonsten im Entwurf eines Strafverfahrensänderungsgesetzes (StVÄG) vorgesehenen datenschutzrechtlichen Ergänzungen zu übernehmen.

Diese Entwicklung ist aus der Sicht des LfD zu beklagen: Wenn einerseits die praktische Tendenz im Bereich der Strafverfolgung unabweisbar ist, Vorfeldermittlungen zu intensivieren und verstärkt auch grundrechtseinschränkende Ermittlungsmaßnahmen durchzuführen, dann ist es auf der anderen Seite ebenso wichtig, datenschutzrechtliche Vorkehrungen zu treffen, die zumindest verfahrenstechnisch und organisatorisch diese Grundrechtseinschränkungen begrenzen.

7.3.2 Gewinnaufspürungsgesetz: Wieviel Datenschutz soll es für Verdächtige geben?

Der derzeit vorliegende Entwurf eines Gewinnaufspürungsgesetzes, der vom Bundestag nunmehr verabschiedet wurde und im Bundesrat erörtert wird, regelt einige aus datenschutzrechtlicher Sicht bedeutsame Fragen nicht ausdrücklich. Hierauf ist der LfD durch den Datenschutzbeauftragten einer Sparkasse aufmerksam gemacht worden. In Abstimmung mit dem Ministerium des Innern und für Sport hat er sich um eine Klärung dieser Fragen bemüht. Es handelt sich um folgende Bereiche:

a) Umfang der Aufzeichnungspflicht bei Verdachtsfällen in § 6 des Entwurfs eines Gewinnaufspürungsgesetzes

   Die Pflicht, Identitätsfeststellungen sowie die Transaktionen zu speichern, betrifft auch die Verdachtsfälle gem. § 6 des Entwurfs. Aufzuzeichnen sind auch die Informationen über die Umstände, die den Verdacht begründet haben.

b) Auskunftsansprüche der betroffenen Bürger

   aa) Eine Auskunft über die Speicherungen zu den Verdachtsfällen ist grundsätzlich ausgeschlossen (§ 12 Abs. 3 des Gesetzentwurfs).

   bb) Eine Auskunft über die Speicherung in den Fällen, in denen die gesetzlichen Mindestbetragsgrenzen überschritten werden (derzeit DM 25 000 im Regelfall), ist grundsätzlich nach den Regelungen des Bundesdatenschutzgesetzes (§ 34) zulässig. Da die Speicherung in diesen Fällen lediglich aufgrund der gesetzlich fixierten Geldbetragsgrenzen erfolgt ist, sind die gespeicherten Daten sicherlich ihrem Wesen nach nicht geheimhaltungsbedürftig. In diesen Fällen dürfte auch die Auskunft nicht die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten, da die Auskunft selbst für den Betroffenen keine Neuigkeit enthalten dürfte. Sie könnte allerdings dazu dienen, die Richtigkeit der gespeicherten Informationen durch den Betroffenen nachprüfbar zu machen.

c) Weitere Behandlung von Verdachtsdaten

   Die Verdachtsdaten sind einerseits besonders geeignet, in Rechte von Betroffenen einzugreifen, andererseits werden sie besonders geheimgehalten. Aus datenschutzrechtlicher Sicht ist dafür Sorge zu tragen, daß die Stichhaltigkeit des Verdachts möglichst umgehend geprüft wird und die entsprechenden Informationen dann ergänzt (bzw. möglichst frühzeitig gelöscht) werden, wenn sich der Verdacht als gegenstandslos erwiesen hat. Nur dann kann aus datenschutzrechtlicher Sicht akzeptiert werden, daß Informationen über Bürger über längere Frist gespeichert werden, ohne daß die Betroffenen hierüber Kenntnis haben. Daraus folgt zum einen, daß die Polizeidienststellen, die die entsprechenden Informationen empfangen, ihrerseits von Amts wegen verdachtserhärtende oder verdachtsentkräftende Umstände möglichst zeitnah an die speichernde Sparkasse mitteilen. Daraus folgt aber auch, daß sich die Sparkasse nach angemessenen Zeitabständen über die Erforderlichkeit der weiteren Speicherung bzw. die Stichhaltigkeit des geäußerten Verdachts bei der datenempfangenden Polizeidienststelle informieren sollte.

Der LfD hat diese Überlegungen an den Sparkassen- und Giroverband herangetragen und gebeten, die betroffenen Sparkassen hierüber zu unterrichten.

7.3.3 Geschäftsstellenautomation der Staatsanwaltschaften, CUST

7.3.3.1 Allgemeines

Derzeit werden folgende Verfahren in der Nachfolge und zur Ablösung des aus Schleswig-Holstein übernommenen GAST-Verfahrens (Geschäftsstellenautomation der Staatsanwaltschaften, vgl. 13. Tb., Tz. 7.3.2) zentral zur automationsunterstützten Sachbearbeitung der Staatsanwaltschaften entwickelt und z. T. bereits praktisch eingesetzt:

- CUST UJs; hierbei handelt es sich um das Projekt, die Verfahren gegen (noch) unbekannte Täter abzuwickeln. CUST steht für „Computer-Unterstützung der Staatsanwaltschaften";
- CUST ZNK; dies ist das erste Teilprojekt der Computerunterstützung von Verfahren gegen bekannte Tatverdächtige (CUST Js) und beinhaltet u. a. die automatisierte Führung der zentralen Namenkartei;
- CUST Js.

7.3.3.2 CUST UJs

Im Bereich von CUST UJs sind allein die gespeicherten Opferdaten schutzbedürftig; andere personenbezogene Daten werden hier im Regelfall nicht gespeichert. Diese Opferdaten allerdings können äußerst sensibel sein und vor dem Hintergrund, daß beabsichtigt ist, im Endausbau jeder Geschäftsstelle mindestens ein Terminal zur Verfügung zu stellen und auch jeden Staatsanwalt damit auszurüsten, erschien es dem LfD unabdingbar, auch hier wirksame Vorkehrungen gegen Mißbrauch zu treffen. So wäre beispielsweise eine Liste aller Vergewaltigungsopfer oder aller Opfer von Erpressungen, die aus ungeklärten Quellen stammt und in unbefugte Hände gerät, ein Schreckgespenst für den Datenschutz. So hat der LfD zumindest eine wirksame Protokollierung gefordert, nachdem seine Vorschläge, nicht von allen angeschlossenen Terminals aus Zugriffe zu gestatten, als unpraktikabel zurückgewiesen wurden.

Aus datenschutzrechtlicher Sicht ist es erforderlich, bei jeder Abfrage, die entweder nur unter Nutzung des Namens des Betroffenen (ohne Eingabe eines Aktenzeichens) oder nur unter Eingabe eines Deliktstatbestandes erfolgt, die Abfrage von einer zusätzlichen Dateneingabe und deren Protokollierung abhängig zu machen. Diese Zusatzeingabe und die Protokollierung sollen den Namen des Veranlassenden der Abfrage sowie das Aktenzeichen des Verfahrens umfassen, für dessen Zwecke abgefragt wird (zusätzlich zur Erfassung und Protokollierung der abfragenden Person).

Da aus der Sicht der staatsanwaltschaftlichen und EDV-technischen Praxis eine solche ausnahmslose zusätzliche Dateneingabe und Protokollierung wohl zu arbeitsaufwendig wäre, wurde folgender Kompromiß unter persönlicher Beteiligung des Ministers der Justiz erzielt: Die genannten Zusatzmaßnahmen sind dann vorzusehen, wenn Delikte betroffen sind, die bezüglich des Opfers – und dies ist im UJs-Verfahren der entscheidende Gesichtspunkt – ein besonderes Schutzbedürfnis begründen. Zu dem Katalog der hier in Betracht kommenden Straftaten gehören zumindest Sexualdelikte und Erpressung, es ist aber auch an eine Reihe weiterer Delikte (insbesondere Körperverletzung, Nötigung, Beleidigungsdelikte – 14. Abschnitt des Strafgesetzbuches –) zu denken.

Bei Abfragen nur unter Nutzung des Namens sind entsprechende Zusatzeingaben und Protokollierungen dann durch das System automatisiert vorzusehen, wenn mit dem abgefragten Namen ein Deliktstatbestand in dem im System gespeicherten Datensatz verbunden ist, der dem angesprochenen Straftaten-Katalog entstammt.

Das Ministerium der Justiz hat bislang nur Angaben über die Opfer von Sexualdelikten und Tötungsdelikten als sensible Daten angesehen, für die die Protokollierung vorzusehen sei. Damit konnte sich der LfD bislang nicht zufrieden geben; zumindest Erpressung, Nötigung, üble Nachrede und Verleumdung begründen ebenfalls eine erhöhte Schutzbedürftigkeit des Opfers (wobei dem LfD nicht recht verständlich ist, wieso das Ministerium der Justiz davon ausgeht, daß die Opfer von Tötungsdelikten hier eines solchen erhöhten Schutzes bedürften).

Zudem sind aus der Sicht des LfD Regelungen bezüglich der Auswertung der Protokollierungen erforderlich. So sollte bestimmt werden, für welche Zeit diese Protokolldaten gespeichert bleiben sowie wer aus welchem Anlaß diese Protokollierungen zu Überprüfungszwecken nutzen darf bzw. nutzen soll. Es könnte beispielsweise daran gedacht werden, regelmäßige Stichprobenkontrollen aus dem Protokolldatenbestand vorzusehen. Die Diskussion hierüber dauert derzeit noch an.

7.3.3.3 CUST Zentrale Namenskartei/Verfahren gegen namentlich bekannte Verdächtige (CUST ZNK/CUST Js)

Zum Verfahren der Automatisierung des zentralen Namensverzeichnisses (CUST ZNK) haben örtliche Feststellungen den Anlaß zu einer Reihe von Fragen gegeben:

a) Grundsätzliches

Zunächst ist davon auszugehen, daß die Automation des zentralen Namensverzeichnisses nicht nur die automationsgestützte Führung der bisherigen Zentralen Namenskartei bezweckt. In diesem Rahmen findet vielmehr eine umfassendere Speicherung von Daten statt, die als integrierter Bestandteil des computerunterstützten Verfahrens – CUST – im Js-Bereich dienen soll. Dieses Verfahren soll zusätzlich zur traditionellen Aufgabe als Aktenfindmittel mindestens folgende Aufgaben erfüllen:

- Erstellung des Js-Verzeichnisses;
- Basis der weiteren Speicherungen und automationsunterstützten Bearbeitungen im Rahmen des Js-Verfahrens, wie z. B. Erstellung von Verfügungen;

– allgemeine Unterstützung der Sachbearbeitung, z. B. Informationen über den Verfahrensstand, Informationen über verfahrensrelevante Umstände des Beschuldigten etc.

Bevor nicht das Gesamtprojekt CUST-Js bekannt ist, kann also auch nicht abschließend beurteilt werden, in welchem Umfang Datenspeicherungen im Rahmen des Zentralen Namensverzeichnisses erforderlich sind und welche sonstigen Maßnahmen des Datenschutzes (u. a. auch Umfang der Protokollierung) angemessen bzw. unabdingbar sind. Es ist allerdings darauf hinzuweisen, daß zum gegenwärtigen Zeitpunkt der Erstellung des Pflichtenheftes für die Entwicklung des Js-Verfahrens eine Berücksichtigung datenschutzrechtlicher Anforderungen unter technischen Aspekten leichter möglich sein dürfte als die nachträgliche Änderung von Programmstrukturen. Eine frühzeitige Einbeziehung des LfD in diese Entwicklung dürfte sich also empfehlen.

b) Umfang des Datensatzes

aa) Bislang fehlende Angaben, die datenschutzrechtlich bedeutsam sind

Während einerseits feststeht, daß der gespeicherte Datensatz im Bereich CUST ZNK sehr viel umfassender ist, als dies für die Auffindung von Aktenvorgängen erforderlich wäre, fehlen andererseits bedeutsame Informationen, die für eine Nutzung dieser Daten zum Zweck der Sachbearbeitung unerläßlich wären. Zu diesen Daten gehören insbesondere Informationen über die Art der Beendigung abgeschlossener Verfahren. Diese Angaben fehlen bei allen Aktenzeichen, die aus der manuellen Kartei übernommen werden, sie sind auch nicht bei den neu erfaßten Verfahren vorgesehen. Außerdem fehlt bei allen Alt-Aktenzeichen die Angabe des Strafvorwurfs, so daß eine Liste der gespeicherten Strafverfahren im allgemeinen dafür untauglich sein dürfte, die Verfahren herauszusuchen, die relevante Informationen für das konkret zu bearbeitende neue Verfahren bieten. Aus der Sicht des LfD ist es bedenklich, wenn bezüglich eines Beschuldigten eine Vielzahl von Aktenzeichen ohne weitere Informationen hierzu aufgelistet werden. Bei diesen Aktenzeichen könnte es sich theoretisch um Bagatelldelikte handeln, die sämtlich wegen erwiesener Unschuld eingestellt sind. Dies ergibt sich aus dem System nicht. Bei dem sachbearbeitenden Staatsanwalt kann sich allerdings der Eindruck verfestigen, bei dem jeweiligen Beschuldigten handele es sich um einen Gewohnheitstäter (oder umgekehrt – etwa im Falle von dienstlich besonders häufig angezeigten Personen –, es handele sich sämtlich um unbedeutende eingestellte Verfahren, obwohl beispielsweise eine abgeurteilte schwere Verkehrsstraftat darunter ist). Fraglich ist, welchen Sinn die Aufzählung dieser Aktenzeichen hat, wenn nicht gleichzeitig verfügt wird, daß dem sachbearbeitenden Staatsanwalt sowohl der Strafvorwurf wie die Beendigung des jeweiligen Verfahrens mitgeteilt werden.

Eine Speicherung der Aktenzeichen ohne gleichzeitige Speicherung des Strafvorwurfs und der Beendigung des Verfahrens ist aus datenschutzrechtlicher Sicht unzulässig, weil diese Speicherung geeignet ist, einen unzutreffenden Eindruck zu erwecken und – wenn sie nicht zur Beiziehung der relevanten zugehörigen Akten führen kann – auch nicht erforderlich ist. Für ein datenschutzgerechtes Verfahren könnten etwa folgende zwei Lösungen in Betracht kommen:

– Im Namensverzeichnis werden das Js-Register und die herkömmliche Zentrale Namenskartei zusammengefaßt, so daß zu jedem Aktenzeichen das Datum, die Art der Erledigung und der Strafvorwurf erfaßt werden.

– Falls dies zu aufwendig erscheint, dürfte auf dem für die Handakten des Staatsanwalts bestimmten Ausdruck nur der Hinweis enthalten sein: Altverfahren vorhanden (u. U. mit der Angabe des Jahres der Anlage der jüngsten vorhandenen Akte). Wenn der Staatsanwalt aufgrund dieser oder weiterer Informationen (z. B. Auszug aus dem BZR) wissen will, welche Verfahren noch vorliegen, wäre eine Liste zu fertigen, in der neben den Az. auch aus dem Js-Register der jeweilige Strafvorwurf sowie Zeit und Art der Erledigung der Verfahren mit aufgenommen werden.

Das Fehlen der genannten Angaben (Zeitpunkt und Art der Beendigung, Strafvorwurf) führt auch zu Problemen bei der Löschung (s. unten c bb).

bb) Nicht erforderliche Daten

Unabhängig hiervon hält der LfD nach dem derzeitigen Kenntnisstand die Speicherung folgender Merkmale im Bereich des automatisierten Namensverzeichnisses für entbehrlich und in diesem Verfahrensstadium nicht für erforderlich:

– Familienstand,
– Ehrenamt,
– Beruf.

Diese Rubriken werden in der Praxis nach den getroffenen Feststellungen auch in der überwiegenden Zahl der Fälle offengelassen.

Im Bereich der Speicherung der „besonderen Hinweise" sollte durch eine zentrale Dienstanweisung klargestellt werden, welche Hinweise hier gespeichert werden können bzw. sollen.

c) Löschungsfristen

aa) Es wurde festgestellt, daß die Löschungsfristen grundsätzlich auf zehn Jahre nach dem Weglegen der Akten festgelegt werden. Allerdings wurde auch mitgeteilt, daß der Staatsanwalt hier abweichende Löschungsfristen vorsehen könne. Es sollte geklärt werden, nach welchen Kriterien diese Verlängerungen möglich sein sollen und ob solche Kriterien in Form einer generell-abstrakten Regelung existieren. Wenn nicht, müßten diese geschaffen werden.

bb) Datenschutzrechtlich problematisch erscheint dem LfD auch das Verfahren bei der Löschung von Aktenzeichen der jeweiligen Strafverfahren. Diese Aktenzeichen werden dann nicht gelöscht, wenn neue Straftaten innerhalb der Regelfrist (zehn Jahre im allgemeinen) hinzugekommen sind. Die Löschungsfrist bestimmt sich jeweils nach dem Datum, das für die letzte hinzu gekommene Straftat maßgeblich ist. Aus der Sicht des LfD kann es nicht hingenommen werden, daß Verfahren, die etwa wegen erwiesener Unschuld eingestellt worden sind, über lange Zeit hinweg gespeichert werden, ohne daß das Verfahrensergebnis deutlich wird. Die Löschung und die Bestimmung der konkret zu beachtenden Löschungsfrist der Aktenzeichen ist aus datenschutzrechtlicher Sicht grundsätzlich vom Ergebnis des jeweiligen Ermittlungsverfahren abhängig zu machen.

cc) Die Löschung der Daten erfolgt, wenn das Reorganisationsdatum erreicht ist. Dieses Datum wird in Neufällen dann eingegeben, wenn die entsprechende Akte zum Weglegen verfügt wird. Auf der Akte befindet sich dann ein Vernichtungsdatum. Dieses wird als Reorganisationsdatum in das System übernommen. Es sollte automationsunterstützt sichergestellt werden, daß nach fünf Jahren in jedem Fall überprüft wird, ob ein solches Reorganisationsdatum zwischenzeitlich eingegeben worden ist und wenn nein, warum dies nicht erfolgt ist. Auf diese Art könnte verhindert werden, daß die Eintragung des Reorganisationsdatums versehentlich unterbleibt.

d) Suchläufe

Die Suche nach Beschuldigten ist grundsätzlich unter Verwendung auch folgender Suchkriterien möglich:
Nationalität, Beruf, Familienstand, Titel, Ehrenamt, Straße und Wohnort.

Zumindest die Kriterien „Ehrenamt" und „Beruf" dürften als Suchkriterien entbehrlich sein, zumal schon die Speicherung dieser Merkmale grundsätzlich entfallen sollte.

e) Protokollierungen

Zur Protokollierung von Abrufen und Eingaben erscheinen dem LfD folgende Regelungen erforderlich:

aa) Alle Abrufe ohne Verwendung eines Aktenzeichens, die nicht von Mitarbeitern der zentralen Geschäftsstelle erfolgen, sollten unter Angabe des Anlasses protokolliert werden. Im Bereich der Js-Verfahren dürfte das Erfordernis, Datensätze abzurufen, in denen ein Aktenzeichen bei der Abfrage nicht bekannt ist, sich auf diejenigen Fälle beschränken, in denen nachgeprüft werden soll, ob der Anzeigeerstatter bzw. der Geschädigte im anderen Zusammenhang bereits als Beschuldigter in Erscheinung getreten ist. Dieses Problem könnte sich auch bezüglich der Zeugen ergeben. Es ist nicht ersichtlich, daß solche Abrufe eine Quantität erreichen, daß eine Protokollierung, wie sie vorgeschlagen wurde, zu unzumutbaren Belastungen führt.

bb) Außerdem sind nach § 9 Abs. 1 Nr. 7 LDatG alle Eingaben, die zur Veränderung eines Datensatzes führen, unter Speicherung von Zeitpunkt und Veranlasser zu protokollieren.

f) Sonstige Fragen des technischen und organisatorischen Datenschutzes

- Das Verfahren bei der Erteilung von Auskünften sollte auch bezüglich des automatisierten zentralen Namensverzeichnisses zweifelsfrei geregelt sein (z. B. telefonisch nur an Staats- und Amtsanwälte, Rechtspfleger und Geschäftsstellen und nur nach Feststellung der Identität, in allen anderen Fällen Verweis auf das zuständige Dezernat bzw. auf den Schriftweg).

- Die systemseitig bereits vorhandenen Möglichkeiten der Zugriffskontrolle werden derzeit nicht genutzt und sollten zur Anwendung kommen (Begrenzung der Gültigkeitsdauer der Paßwörter, Vorgabe einer Mindestlänge, Begrenzung ungültiger Anmeldeversuche usw.). Im Rahmen der vorgesehenen einheitlichen Konfiguration der Systeme bei allen Staatsanwaltschaften durch Mitarbeiter des Ministeriums der Justiz sollten entsprechende Vorgaben für die örtlichen Systemverwalter erfolgen.

- Wenn künftig ein zentraler Servereinsatz erfolgt, muß die erforderliche Abschottung der unterschiedlichen Datenbestände (z. B. AG, LG, OLG) durch Bildung entsprechender Benutzerprofile sichergestellt sein. Innerhalb der jeweiligen Institution sollte dies insoweit fortgesetzt werden, als über die vorhandene Menüberechtigungsliste Bildschirmmasken sowie Auswertungs- und Zugriffsmöglichkeiten nur entsprechend der jeweiligen Aufgabenstellung (Staatsanwalt, Geschäftsstellen) zur Verfügung gestellt werden. Dies betrifft die Möglichkeit der Eingabe von Suchkriterien, die Anzeige der Daten am Bildschirm sowie die Möglichkeiten zur Änderung, Neuaufnahme und Löschung von Datensätzen.

- Wie festgestellt wurde, wird bei der besuchten Staatsanwaltschaft die räumliche Absicherung der Zentraleinheit im Rahmen des künftig geplanten Einsatzes verbessert werden. Statt der Unterbringung in den stark frequentierten Räumen der Geschäftsstelle wird, zusammen mit den zentralen Komponenten der Gebäudeverkabelung, die Aufstellung in einem separaten, abschließbaren Raum erfolgen. Mit dem gleichen Hintergrund sollte die Möglichkeit der Anmeldung als Systemverwalter nicht grundsätzlich an allen angeschlossenen Terminals möglich sein, sondern auf bestimmte wenige beschränkt werden.

Es ist vorgesehen, diese Fragen weiter mit dem Ministerium zu erörtern. Ein entsprechendes Gesprächsangebot liegt dem Minister vor.

7.3.4 Telefonabhörmaßnahmen

Telefonabhörmaßnahmen, die zum Zweck der Strafverfolgung erfolgen, werden grundsätzlich durch einen Richter angeordnet (gem. § 100 a StPO). Dem LfD fehlt die Zuständigkeit, die Zulässigkeit solcher richterlicher Anordnungen zu überprüfen.

Dennoch gibt es eine Reihe von Fragen, die sich im Zusammenhang mit der Durchführung von Telefonabhörmaßnahmen ergeben und die unabhängig von der richterlichen Entscheidung der Anordnung einer solchen Maßnahme sind.

Angesichts der Tatsache, daß die Zahl der jährlich angeordneten Telefonabhörmaßnahmen stetig im steigen begriffen ist (insbesondere aufgrund des Einsatzes dieses Ermittlungsinstruments im Bereich der Verfolgung der Rauschgiftkriminalität, aber auch bei sonstigen Straftaten), ist es der Gegenstand besonderer Bemühungen des LfD gewesen, in diesem Zusammenhang den Grundrechtsschutz zu optimieren. Hierfür waren auch folgende Gesichtspunkte bedeutsam:

- Mit jeder Telefonabhörmaßnahme geht der Eingriff in Grundrechte einer Vielzahl nicht betroffener unschuldiger Personen einher. Im Regelfall werden Abhörmaßnahmen zunächst für drei Monate bei einer einmaligen Verlängerungsmöglichkeit um weitere drei Monate angeordnet. Dabei werden Gesprächspartner der verdächtigen Personen erfaßt und von den Ermittlungsorganen zur Kenntnis genommen, die in keinem Zusammenhang mit der Straftat stehen. Kriminologen schätzen, daß bei jeder Abhörmaßnahme mehrere hundert Nichtbetroffene in das Blickfeld der Ermittlungsbehörden geraten.
- Ein weiterer Gesichtspunkt ist, daß die Telefonabhörmaßnahmen einen äußerst intensiven Eingriff in die Privatsphäre der Betroffenen bedeuten: Von den Abhörmaßnahmen sind auch Gespräche mit den engsten Verwandten (Eltern, Kinder, Ehegatten) betroffen.

  Diese Gesichtspunkte gebieten es, den Verhältnismäßigkeitsgrundsatz hier besonders zu betonen.

7.3.4.1 Die Aufzeichnung von Verbindungsdaten in Mobilfunknetzen

Zwischen dem Bundesminister der Justiz und den Landesjustizressorts wurde die Frage erörtert, unter welchen Voraussetzungen Abhörmaßnahmen in bezug auf Anschlüsse im Funktelefon C-Netz durchgeführt werden können.

Dabei wurde hauptsächlich erörtert, ob die Voraussetzungen des § 100 a StPO (grundsätzlich richterlicher Beschluß sowie Ermittlungen wegen einer sog. Katalogstraftat) vorliegen müssen oder ob eine Auswertung bestimmter Informationen auch ohne einen solchen Beschluß erfolgen kann.

Die datenschutzrechtliche Beurteilung muß differenziert erfolgen:

- Soweit daran gedacht ist, Telefonate, die von Autotelefonen geführt werden oder die an einen Autotelefonanschluß gerichtet sind, auf Tonträgern zu erfassen und auszuwerten, sind rechtlich keine Besonderheiten ersichtlich, die ein Abweichen von den Voraussetzungen des § 100 a StPO in irgendeiner Weise rechtfertigen könnten. Möglicherweise bestehen hier technische Schwierigkeiten, auf die in Presseveröffentlichungen hingewiesen wurde. Die Frage, ob und in welcher Weise diese technischen Schwierigkeiten behoben werden können, ist grundsätzlich datenschutzrechtlich nicht relevant. Datenschutzrechtliche Fragen würden sich erst ergeben, wenn aus der technischen Ausgestaltung der Telefonabhörmaßnahmen im Funktelefonnetz auch ein inhaltlicher Unterschied in der Datenerhebung zu Abhörmaßnahmen zwischen stationären Telefonteilnehmern folgen würde. Dies ist nicht ersichtlich.
- Eine Besonderheit im Funktelefon C-Netz ergibt sich allerdings daraus, daß dort die Erstellung von „Bewegungsbildern" möglich ist. Sowie ein Funktelefon in der Form aktiviert wird, daß von ihm Gespräche ausgehen können oder daß Gespräche angenommen werden können (durch Einschieben einer besonderen Codekarte), werden ständig Meldungen über den Standort des Funktelefons bei der jeweils regional nächsten Funkvermittlungsstelle (20 im Bundesgebiet) sowie Funkfeststationen (160 im Bundesgebiet) erfaßt. Diese Meldungen werden derzeit noch nicht gespeichert. Sie verschwinden spurlos, wenn der Teilnehmer sich mit seinem Telefongerät in den Bereich einer anderen Telefonvermittlungsstelle begibt. Zwischenzeitlich ist das Funktelefonnetz D eingeführt worden, bei dem sich gleichartige Fragen ergeben.

Fraglich ist,

a) unter welchen Voraussetzungen im Einzelfall eine Datenübermittlung solcher gespeicherter Informationen an die Strafverfolgungsbehörden erfolgen darf,

b) ob die Post durch die Justizbehörden verpflichtet werden kann, eine dauerhafte Speicherung solcher Signale bezüglich aller oder einzelner Teilnehmer durchzuführen, auch wenn sie diese Speicherung aus Gründen der eigenen Aufgabenerfüllung nicht braucht.

Der LfD hat hierzu ein umfangreiches Gutachten erstellt und ist zu folgendem Ergebnis gekommen:

Zu a:

Die in Rede stehenden „flüchtigen" Verbindungsdaten im Funktelefonnetz unterliegen dem Post- und Fernmeldegeheimnis. Eine Rechtsgrundlage zur dauerhafteren Speicherung dieser Daten durch die Bundespost sowie zur Übermittlung an Strafverfolgungsbehörden ist weder der Vorschrift des § 100 a StPO noch der Regelung des § 12 FAG zu entnehmen, da sich beide Regelungen auf die Übermittlung von Daten bzw. Informationen beziehen, die aus dem „Fernmeldeverkehr", also aus konkreten Kommunikationsvorgängen stammen und die mit „Mitteilungen" an den oder von dem Betroffenen zusammenhängen. Die bloße Meldung, daß ein bestimmtes Funktelefon in einem bestimmten Bereich betriebsbereit gehalten wurde und für welche Zeitdauer dies jeweils erfolgt ist, ist nicht als solche Information anzusehen. Eine extensive Auslegung der genannten Rechtsvorschriften, die bezüglich der Begriffe „Mitteilung" und „Fernmeldeverkehr" auch die genannten technischen Vorfeldinformationen umfassen würde, ist mit Sinn und Zweck dieser Normen sowie mit der Verfassung nicht vereinbar, wonach grundrechtseinschränkende Gesetze prinzipiell restriktiv auszulegen sind.

Zu b:

Die Behörde, bei der die Staatsanwaltschaft anfragt, ist grundsätzlich zur Auskunft rechtlich verpflichtet (§ 161 Satz 1 StPO). Die befragte Behörde muß auch ggf. zumutbare eigene Aktivitäten entfalten, um die geforderten Nachrichten zu gewinnen (so Kleinknecht/Mayer, Anmerkung 1 zu § 161 StPO, mit Hinweis auf BGH 29, 109, 112 sowie BVerfGE 57, 250, 283 = NJW 81, 1719, 1723). Dies gilt allerdings nicht, wenn das Post- und Fernmeldegeheimnis betroffen ist. Hier treffen §§ 99, 100 a StPO sowie § 12 FAG abschließende Regelungen (so Kleinknecht/Mayer aaO). Neben diesen ausdrücklichen Durchbrechungsmöglichkeiten des Post- und Fernmeldegeheimnisses bieten weder § 161 StPO noch die allgemeinen Datenschutzgesetze ausreichende Rechtsgrundlagen, um das Post- und Fernmeldegeheimnis zu beschränken.

Das Verlangen an die Post, grundsätzlich flüchtige Informationen aufzuzeichnen, ist durch keine ausreichende Rechtsgrundlage gedeckt, da diese Informationen durch das Post- und Fernmeldegeheimnis geschützt werden und da die genannten Sondervorschriften auf diese Informationen – wie unter Buchst. a dargelegt – nicht anwendbar sind.

7.3.4.2 Die Aufzeichnung und Verwertung von Raumgesprächen

Der LfD hatte folgenden Sachverhalt zu beurteilen:

Aufgrund einer richterlichen Anordnung gem. § 100 a StPO wurde ein Telefonanschluß, den der Beschwerdeführer ständig nutzte, durch die Polizei abgehört. Im Zuge der längerfristigen Überwachung (sechs Monate) wurden mindestens in zwei Fällen sogenannte „Raumgespräche" mit aufgezeichnet, die der Beschwerdeführer mit Personen führte, die in dem Raum anwesend waren, in dem er sich selbst befand. Diese beiden Fälle unterscheiden sich voneinander:

a) In einem Fall hatte der Beschwerdeführer den Hörer abgenommen und die Nummer des Gesprächspartners gewählt. In der Zeit, in der das Freizeichen beim Angerufenen ertönte, also vor dem Zustandekommen eines Telefongesprächs, unterhielt er sich mit anderen Personen im Raum. Diese Unterhaltung wurde aufgezeichnet und auch schriftlich protokolliert.

b) In einem anderen Fall hat der Beschwerdeführer eine Nummer angewählt, der angewählte Teilnehmer hatte abgehoben, es wurde dort jedoch – im Rahmen einer Nebenstellenanlage – weiter verbunden. Während der Zeit der Weiterverbindung unterhielt sich der Beschwerdeführer mit anwesenden Personen. Auch dieses Gespräch wurde aufgezeichnet.

Die Frage, ob diese Raumgespräche aufgezeichnet werden durften, bestimmt sich nach § 100 a StPO. Dort ist geregelt, daß die Überwachung und Aufzeichnung des Fernmeldeverkehrs unter bestimmten Voraussetzungen angeordnet werden darf. In diesem Zusammenhang darf also nur das aufgezeichnet werden, was zum Fernmeldeverkehr gehört.

Selbstverständlich ist, daß die Kommunikation mit dem angerufenen Teilnehmer Fernmeldeverkehr darstellt. Unstreitig ist auch, daß bereits das Wählen der Nummer des angerufenen Teilnehmers Bestandteil des Fernmeldeverkehrs ist. Ebenso gehört dann der technische Vorgang der elektronischen Übermittlung von Signalen, der zum Ertönen des Freizeichens (oder u. U. des Besetztzeichens) führt, dazu.

Außer Streit steht auch, daß solche Raumgespräche, die nach Beendigung des Telefonats nur deshalb aufgezeichnet werden können, weil der Hörer nicht richtig aufgelegt wurde, nicht unter den Begriff des „Fernmeldeverkehrs" fallen. Dies hat der BGH im Jahre 1983 (Urteil vom 16. März 1983, Az. 2 StR 775/82, NJW 83, 1569) entschieden.

Ungeklärt und streitig sind folgende drei unterschiedliche Konstellationen:

a) Es wird ein Raumgespräch aufgenommen, das nach dem Abheben des Hörers während des Wählens und des darauf folgenden Rufvorganges, aber vor Abnehmen des Hörers durch den angerufenen Teilnehmer geführt wird.

b) Es wird ein Raumgespräch aufgezeichnet, das während des Weiterverbindens im Rahmen einer Nebenstellenanlage geführt wird, ohne daß eine Kommunikation mit einem angerufenen Teilnehmer stattfindet.

c) Es wird ein Raumgespräch aufgezeichnet, das parallel zu einem Telefongespräch geführt wird (im Hintergrund des Telefongesprächs). An diesem Gespräch kann der im Raum anwesende Teilnehmer des Telefonats beteiligt sein, denkbar ist auch die Fallgestaltung, daß er sich an diesem Raumgespräch nicht beteiligt. Diese Konstellation in beiden Varianten könnte man als eigentliches „Hintergrundgespräch" bezeichnen.

Die Beantwortung der Frage, ob Raumgespräche in allen drei genannten Fällen, nur in einem Teil davon oder überhaupt nicht zulässigerweise abgehört und ausgewertet werden dürfen, hängt davon ab, wie der Begriff des „Fernmeldeverkehrs" im Sinne des § 100 a StPO definiert wird. Nach der engsten an den Wortlaut anknüpfenden Auslegung dürften nur solche Informationen aufgezeichnet werden, die zielgerichtet und zweckbestimmt mit Hilfe der Technik transportiert werden. Nur diese sind als „Fernmeldeverkehr" im eigentlichen Sinn anzusehen.

Mit dieser grundsätzlich eng am Wortsinn orientierten Auslegung wäre es allerdings wohl auch vereinbar, Hintergrundgespräche, die während eines Telefongesprächs entstehen, genauso wie Hintergrundgeräusche bei einem Telefonat allgemein – unabhängig davon, ob es sich um sprachliche Kommunikation handelt – als Teil des Fernmeldeverkehrs in diesem Sinne aufzufassen: Das, was der angewählte Teilnehmer am Telefonat hören kann, ist Teil des Fernmeldeverkehrs und untrennbar mit diesem verbunden. Dies könnte dann auch durch die abhörende Stelle aufgezeichnet und verwertet werden.

Anders verhält es sich dagegen in den Fällen, in denen ein Teilnehmer am Telefonat entweder nicht vorhanden ist – wie in den Fällen, in denen der Teilnehmer (noch) nicht abgehoben hat –, oder in denen er jedenfalls konkret nicht aktiv als Kommunikationspartner teilnimmt, wie in den Fällen, in denen bei einer Nebenstellenanlage weiter verbunden wird. Dann sind die akustischen Signale, die beim Anrufer entstehen, grundsätzlich von diesem nicht zur Übermittlung mit Hilfe der Fernmeldetechnik bestimmt. Er geht auch nicht davon aus, daß die Fernmeldetechnik es schon in diesem Stadium ermöglicht, akustische Signale weiterzugeben. Objektiv findet in diesem Zeitraum keine zielgerichtete Übermittlung akustischer Signale an einen anderen Fernsprechteilnehmer, also „Fernmeldeverkehr", statt; nach der angesprochenen eng am Wortsinn orientierten Auslegung wäre die Aufzeichnung von Raumgesprächen unter diesen Bedingungen unzulässig.

Dies trifft jedenfalls auf den Fall zu, daß erst technisch beim Kommunikationspartner „angeklopft" wird, in der Phase also, in der nur das Rufsignal oder das Besetztzeichen ertönt. In der Phase der Weiterverbindung könnte man allerdings die Auffassung vertreten, daß hier ein konkreter Teilnehmer am Telefonat bereits aktiviert ist und daß der Anrufer damit rechnen muß, daß während des Weiterverbindens der angerufene Teilnehmer selbst durch die insoweit vom Anrufer nicht durchschaubare Technik die Möglichkeit hat, das zur Kenntnis zu nehmen, was beim Anrufer an akustischen Signalen entsteht.

Nach Auffassung der bisher beteiligten Ressorts findet jedoch in allen genannten Fällen Fernmeldeverkehr statt, Raumgespräche in diesem Zusammenhang werden generell als „Hintergrundgespräche" bezeichnet, die während des Fernmeldeverkehrs entstehen und die – als zwangsläufig mit ihm verbunden – auch abgehört und ausgewertet werden dürfen.

Aus datenschutzrechtlicher Sicht neigt der LfD allerdings der dargestellten eng am Wortsinn orientierten Auslegung des Begriffs „Fernmeldeverkehr" zu. Einer erweiternden Auslegung des Begriffs „Fernmeldeverkehr" in § 100 a StPO kann er aus den Gründen, die der BGH in seiner zitierten Entscheidung hiergegen angeführt hat, nicht folgen.

Zumindest der oben unter 2 Buchst. a geschilderte Fall dürfte danach jedenfalls nicht vom Begriff „Fernmeldeverkehr" und damit von der Eingriffsermächtigung des § 100 a StPO umfaßt sein.

Falls es für erforderlich gehalten wird, auch derartige Fälle im Rahmen von Telefonüberwachungsmaßnahmen zu erfassen, wäre eine entsprechende Gesetzesänderung unumgänglich.

Diese Beurteilung hat der LfD dem Ministerium der Justiz und dem ISM mitgeteilt.

7.3.4.3 Die Aufzeichnung von Verteidigergesprächen

Nach den dem LfD vorliegenden Informationen wird bei Telefonabhörmaßnahmen gem. § 100 a StPO wie folgt verfahren:

Wenn bezüglich eines bestimmten Anschlusses die Durchführung von Abhörmaßnahmen angeordnet wurde, werden sämtliche aus- und eingehenden Gespräche, an denen der entsprechende Anschluß beteiligt ist, durch die zuständige Polizeidienststelle mit Hilfe eines Tonbandgerätes aufgezeichnet. Dabei werden zwei Bänder parallel eingesetzt, ein Arbeits- und ein Beweisband. Die jeweiligen Verbindungsdaten zu den aufgezeichneten Gesprächen werden zusätzlich gespeichert.

Die Auswertungsphase, die auf die Aufzeichnung von Telefonaten folgt, besteht darin, zu jedem Band zunächst ein Verzeichnis der Gespräche anhand der gespeicherten Verbindungsdaten zu erstellen. Dabei werden Verteidigergespräche gesondert gekennzeichnet. Um in diesem Inhaltsverzeichnis erkennen zu können, an welcher Stelle des Tonbandes das Gespräch beginnt und an welcher Stelle es endet, ist es erforderlich, daß der auswertende Polizeibeamte auch in das Verteidigergespräch hineinhört, obwohl er es inhaltlich nicht weiter auswerten darf. Der auswertende Polizeibeamte bestimmt weiter, welche Gespräche im Sinne des Ermittlungsziels bedeutsam genug sind, um auch schriftlich festgehalten zu werden.
Eine Löschung der Verteidigertelefonate erfolgt erst zusammen mit den gesamten übrigen Aufzeichnungen auf dem Beweisband, um dessen Beweiseignung nicht zu gefährden.

Es dürfte allgemeiner Auffassung entsprechen, daß auch im Rahmen von zulässigen Telefonabhörmaßnahmen gem. § 100 a StPO Gespräche mit dem Verteidiger nicht aufgenommen, aufgezeichnet und verwertet werden dürfen, unabhängig davon, ob es sich um eingehende Gespräche handelt, zu denen die Initiative vom anrufenden Verteidiger ausgeht, oder um abgehende Gespräche vom abgehörten Anschluß zum Verteidiger (vgl. Kleinknecht/Meyer, StPO-Kommentar Anmerkung 13 zu § 100 a). Gleiches dürfte grundsätzlich (im Zusammenhang mit § 12 FAG) auch für die dauerhafte Speicherung von Verbindungsdaten über Verteidigergespräche gelten, aus denen sich entnehmen läßt, wann, wie oft und wie lange derartige Gespräche geführt worden sind.

Der Europäische Gerichtshof für Menschenrechte hat dieses Recht auch dann für unverzichtbar erklärt, wenn ein Untersuchungshäftling zu Beginn seiner Untersuchungshaft mit seinem Pflichtverteidiger sprechen will. Der Gerichtshof hat betont, daß das Recht des Angeklagten auf von Dritten nicht erfaßbare Kommunikation mit seinem Anwalt zu den wesentlichen Erfordernissen eines fairen Verfahrens in einer demokratischen Gesellschaft gehöre. Es sei damit ohne weiteres aus Artikel 6 Abs. 3 c der Europäischen Menschenrechtskonvention abzuleiten, in dem die Ausprägung des allgemeinen Grundsatzes eines fairen Verfahrens zu sehen sei (Urteil des EGMR vom 28. November 1991, NJW 92,3090).

Die praktischen Bedingungen beim Abhören scheinen eine lückenlose Realisierung der allgemein anerkannten rechtlichen Anforderung in bezug auf Verteidigergespräche nicht zu erlauben.

- So weiß die abhörende Polizeidienststelle nicht in jedem Fall, ob die abgehörte Person einen Verteidiger beauftragt hat und, wenn ja, wer dies ist.
- Bei den bisher eingesetzten technischen Geräten ist – unter der Bedingung von analogen Telefonnetzen – die Anzeige und Speicherung der Verbindungsdaten beschränkt: derzeit ist wohl nur die Anzeige und Aufzeichnung der vom abgehörten Anschluß aus angerufenen Nummern möglich, nicht aber der Nummer des Anrufers, wenn dieser den abgehörten Anschluß anwählt. Dies bedeutet, daß Verteidigergespräche, die auf Initiative des Verteidigers von seinem Apparat aus zustandekommen, auch dann nicht gesondert behandelt werden können – zumindest auf der Ebene des Aufzeichnens auf dem Magnetband –, wenn der Verteidiger und sein Telefonanschluß bekannt sind.

Unüberwindbare technische Schwierigkeiten dürften aber – entgegen einer 1990 geäußerten Auffassung des Ministeriums der Justiz sowie des Ministeriums des Innern und für Sport – jedenfalls nach dem heutigen Stand der Technik einem Unterdrücken der Aufzeichnung auf dem Magnetband dann nicht entgegenstehen, wenn die Nummer des Verteidigers den abhörenden Stellen bekannt ist und wenn der Abgehörte selbst seinen Verteidiger anruft. Dies dürfte eine erhebliche Zahl der Verteidigergespräche betreffen.

Aus datenschutzrechtlicher Sicht sollten alle Anstrengungen unternommen werden, die tatsächlichen Verhältnisse dem rechtlich Gebotenen so nahe wie möglich anzugleichen. Auch wenn derzeit – solange die digitalen Netze nicht flächendeckend betrieben werden – nur ein Teil der Verteidigergespräche technisch so behandelt werden kann, wie es von der Rechtslage her geboten erscheint, sollte zumindest dieser relevante Teil der gesamten in Rede stehenden Gespräche den rechtlichen Anforderungen entsprechend behandelt werden. Auch die Verbindungsdaten über Verteidigertelefonate sollten dann unmittelbar gelöscht werden, wenn klar ist, daß es sich um ein Verteidigertelefonat gehandelt hat.

Aus der Stellungnahme des Ministeriums ergibt sich, daß es technisch möglich ist, eine Software zu entwickeln, die es zuläßt, gezielt die Aufzeichnung bestimmter Gespräche (hier: Verteidigergespräche) im Rahmen von Telefonabhörmaßnahmen zu unterdrücken.

Daß hierbei einmalige Entwicklungskosten „bis zu DM 100 000,–" entstehen könnten (und kleine Beträge für die ergänzende Geräteausstattung, deren Höhe noch unabgeklärt ist, hinzukämen), kann aus datenschutzrechtlicher Sicht kein Hinderungsgrund sein, diese technische Möglichkeit zu entwickeln und dann auch tatsächlich einzusetzen: Die Alternative, eine rechtsstaatsgemäße Durchführung der Telefonabhörmaßnahmen zu gewährleisten, würde darin bestehen, auf die automatisierten Aufzeichnungen zu verzichten und Polizeibeamte konkret einzusetzen, die jeweils die einzelnen Gespräche mithören und dann, wenn ein Verteidigertelefonat geführt wird, manuell die Aufzeichnung abbrechen. Bei dieser Vorgehensweise würden mit Sicherheit unvergleichbar höhere Kosten entstehen.

Der LfD hat deshalb empfohlen, ein konkretes Angebot der Herstellerfirma zur Realisierung des in Rede stehenden Leistungsmerkmales unter Einbeziehung aller Kostenfaktoren einzuholen und die Angelegenheit weiter zu verfolgen.

7.3.4.4 Die Verwertung von Erkenntnissen für die Gefahrenabwehr

Fraglich ist, ob es zulässig ist, die Erkenntnisse aus den Telefonabhörmaßnahmen, die zum Zweck der Verfolgung von Straftaten gewonnen wurden, auch für Gefahrenabwehrmaßnahmen zu verwerten. Um es an einem Beispiel zu verdeutlichen: Wenn anläßlich von Telefonabhörmaßnahmen, die gemäß § 100 a StPO angeordnet worden sind, deutlich wird, daß ein Diebstahl geplant wird, ist es dann zulässig, zum Schutz des bedrohten Eigentums Maßnahmen zu ergreifen und etwa die zuständige Polizeibehörde über die Vorbereitung einer entsprechenden Straftat zu informieren?

Der LfD hat sich bemüht, bis zu einer gesetzlichen Regelung hier durch die zuständigen Ressorts die Formulierung möglichst klarer Maßstäbe zu erreichen, die der Praxis die Entscheidung erleichtern, vor allem aber erkennbar machen, welche Möglichkeiten die Strafverfolgungsbehörden haben. Das Bundesverfassungsgericht hat eine solche Transparenz grundsätzlich gefordert.

Der LfD hat deshalb den Minister des Innern und für Sport sowie den Minister der Justiz aufgefordert, eine entsprechende Verwaltungsvorschrift zu erlassen. Die Hessische Landesregierung hat im Grundsatz diesen Weg gewählt. Sie hat in Abstimmung mit dem dortigen LfD eine entsprechende Regelung getroffen.

Die angesprochenen Ministerien haben sich dem jedoch verschlossen und auf die ausstehende Novellierung der StPO verwiesen. Dies ist nach der Auffassung des LfD unzureichend. Er wird sich weiter um die Verwirklichung seiner Anregung bemühen.

7.3.4.5 Weitere Probleme

Folgende Fragen haben sich bei der näheren Betrachtung von konkreten Abhörmaßnahmen ebenfalls als klärungsbedürftig erwiesen:

a) Dürfen die Ermittlungsbehörden Tonbänder abgehörter Gespräche, die in wenig gebräuchlichen Fremdsprachen erfolgt sind, sprachkundigen Privatpersonen informatorisch zur Kenntnis geben, um kostengünstig zu erfahren, ob strafrechtlich Relevantes besprochen wurde, oder dürfen in diesem Zusammenhang nur gerichtlich bestellte und vereidigte Übersetzer und Sachverständige in das Verfahren einbezogen werden?

b) Darf bei der Löschung von Unterlagen aus der Telefonüberwachung differenziert werden zwischen den Tonbändern und den dazugehörigen schriftlichen Aufzeichnungen?

c) Hat bei der Löschung von Tonbändern ein Staatsanwalt der Vernichtung persönlich beizuwohnen?

d) Sind in Rheinland-Pfalz bei den Strafverfolgungsbehörden ausreichende Vorkehrungen getroffen, daß die Löschung von Tonbändern technisch sicher und ausreichend schnell erfolgen kann? Diese Frage stellte sich in einem Verfahren, in dem 99 Bänder von je mehrstündiger Laufzeit zu vernichten waren.

Diese Fragen sind derzeit noch Gegenstand der Erörterungen mit den zuständigen Ressorts. Angesichts der wachsenden Zahl von Telefonüberwachungsmaßnahmen sind solche Fragen sicherlich gerade angesichts der Zahl der mitbetroffenen unbeteiligten Dritten bedeutsam.

7.3.5 Die Bekanntgabe der HIV-Infektion in der Hauptverhandlung

Das Schreiben eines Caritasverbandes gab dem LfD Veranlassung, sich unmittelbar an den Minister der Justiz zu wenden. Der Verband hatte folgenden Vorgang geschildert: Eine Klientin des Caritas-Verbandes sei als Zeugin in einem Strafverfahren geladen worden. Als sie nicht zur Hauptverhandlung erschienen sei, habe der Richter öffentlich erklärt, nach seiner Kenntnis sei die Zeugin HIV-positiv und daher sei ihr Fernbleiben verständlich.

Eine konkrete Einflußnahme auf derartige richterliche Vorgehensweisen ist dem LfD wegen der Unabhängigkeit der Gerichte verwehrt. Trotz der eingeschränkten Möglichkeiten der unmittelbaren Einflußnahme im Bereich der Rechtsprechung muß es allerdings möglich sein, vor dem geschilderten Hintergrund in allgemeiner Form (etwa im Rahmen der Richterfortbildung oder vergleichbarer Aktivitäten) auf die hier deutlich werdende Problematik hinzuweisen. Deshalb hat der LfD den Minister gebeten, aufgrund des geschilderten Beispiels zu einer Sensibilisierung der Gerichte in diesem Zusammenhang beizutragen.

Der Minister hat mit folgendem Inhalt Stellung genommen: Bei dem in Rede stehenden Vorgang habe es sich um einen Einzelfall gehandelt. Die Richterschaft sei sich der datenschutzrechtlichen Problematik bewußt. Er wolle daher der Anregung, hierauf – etwa im Rahmen der Richterfortbildung – allgemein hinzuweisen, vorerst nicht folgen. Er erwarte, daß es eines derartigen Hinweises nicht bedürfe.

Dem LfD ist kein weiterer derartiger Fall bekannt geworden, so daß er keinen Anlaß hat, die Richtigkeit der Einschätzung des Justizministers zu bezweifeln.

7.3.6 Opferschutz: Was darf der Beschuldigte über den Anzeigeerstatter erfahren?

Das Akteneinsichtsrecht des Beschuldigten gem. § 147 StPO kann möglicherweise zu schwerwiegenden Beeinträchtigungen des Opfers bzw. Anzeigeerstatters führen. Durch folgenden Fall, der dem LfD aufgrund einer Eingabe bekannt geworden ist, ist dies deutlich geworden: Die Beschwerdeführerin hatte einen Arbeitskollegen wegen sexueller Nötigung angezeigt. Dieses Ermittlungsverfahren wurde wegen Nichtnachweisbarkeit der Tat eingestellt. Im Rahmen dieses Ermittlungsverfahrens hat die Staatsanwaltschaft folgende Unterlagen beigezogen:

a) Scheidungsakten des Opfers;

b) familiengerichtliche Akten des Opfers, die das Sorgerecht bezüglich ihrer Kinder betrafen;

c) Akten über ein staatsanwaltschaftliches Ermittlungsverfahren, das fünf Jahre zuvor gegen einen Bekannten des Opfers ebenfalls wegen versuchter Vergewaltigung bei der Staatsanwaltschaft eines anderen Bundeslandes durchgeführt wurde.

Folgende Informationen, die sich zum Teil in den oben genannten Akten befunden haben, hat die Staatsanwaltschaft in der Ermittlungsakte aktenkundig gemacht:

a) Selbstmordversuch des Opfers vor sechs Jahren im Zusammenhang mit ihrer Ehescheidung, Einlieferung in das Kreiskrankenhaus;

b) staatsanwaltschaftliches Ermittlungsverfahren gegen das Opfer wegen Kindesmißhandlung, erstattet durch den geschiedenen Ehegatten im Zuge der Sorgerechtsauseinandersetzungen, sechs Jahre zurückliegend;

c) Ermittlungsverfahren wegen der Anzeige eines Nachbarn wegen angeblichen Diebstahls, Verfahren eingestellt, fünf Jahre zurückliegend;

d) Erkrankung des Opfers vor drei Jahren an Depressionen sowie nervenärztliche Behandlung und stationäre Klinikunterbringung;

e) Durchführung eines staatsanwaltschaftlichen Ermittlungsverfahrens gegen den geschiedenen Ehemann des Opfers wegen fortgesetzten sexuellen Mißbrauchs der Tochter, zwei Jahre zurückliegend;

f) Aussagen der Kinder des Opfers in mehreren richterlichen Vernehmungen im Zusammenhang mit den familiengerichtlichen Auseinandersetzungen.

Die Beschwerdeführerin erklärte, alle diese Informationen seien dem Beschuldigten in dem gegen ihn angestrengten Strafverfahren zur Kenntnis gegeben worden. Sie ist der Auffassung, diese Angelegenheiten beträfen ihre Intimsphäre und hätten mit dem Vorwurf gegen den Beschuldigten nichts zu tun. Der Beschuldigte sei ihr Arbeitskollege und habe nun Informationen erhalten, die er zu ihrem Nachteil an der Arbeitsstelle verbreiten könne. Sie als Opfer einer Straftat werde damit zusätzlich bestraft.

Aus Anlaß dieses Falles hat der LfD gegenüber dem Ministerium der Justiz folgende Auffassung vertreten: Bei der Gewährung von Akteneinsicht können im Rahmen des § 147 StPO auch Gesichtspunkte des Opferschutzes Bedeutung erhalten. Die Grundrechte der Betroffenen haben bei der Auslegung des einfachen Gesetzesrechts ein besonderes Gewicht. Wenn sich der Sinn und Zweck einer gesetzlichen Norm auf einem Weg erreichen läßt, der die Grundrechte der betroffenen Bürger in geringerem Maß beeinträchtigt, als dies bei einer vordergründigen wörtliche Auslegung der Vorschrift der Fall wäre, ist zu prüfen, ob nicht eine teleologische Reduktion der Norm aus Gründen der verfassungskonformen Anwendung des Gesetzes vorzunehmen ist.

§ 147 StPO soll eine effektive und wirksame Interessenwahrnehmung des Beschuldigten ermöglichen. In den Fällen, in denen das Interesse des Beschuldigten an einer effektiven Verteidigung stark reduziert ist, wenn z. B. die Staatsanwaltschaft die Einstellung des Verfahrens beschlossen und der Anzeigeerstatter dagegen kein Rechtsmittel eingelegt hat, dürfte eine umfassende Akteneinsichtsgewährung unter Beifügung aller Beiakten, die auch bereits abgeschlossene Strafverfahren betreffen, unverhältnismäßig sein. Dann ist § 147 StPO verfassungskonform einschränkend auszulegen.

Außerdem ist Nr. 187 Abs. 2 RistBV zu berücksichtigen. Danach darf in Akten einer anderen Verwaltung durch die Staatsanwaltschaft dritten Stellen gegenüber nur mit der ausdrücklichen Genehmigung der Verwaltung Einsicht gewährt werden, von der die Akten stammen. Dies betrifft auch solche Akten, die im Rahmen eines Strafverfahrens von einer Stelle außerhalb der Strafjustiz beigezogen worden sind. Diese Regelung ist auch im Rahmen des § 147 StPO beachtlich.

7.3.7 Formulareinwilligungen für Ermittlungsmaßnahmen?

Durch die Staatsanwaltschaften des Landes Rheinland-Pfalz ist das Bedürfnis formuliert worden, mit Hilfe eines Einwilligungsvordruckes die Einwilligung von Beschuldigten, Zeugen und sonstigen Personen im Rahmen von Strafermittlungsverfahren dafür einzuholen, sich Auskünfte bei verschiedenen Stellen (je nach der Fallgestaltung bei Arbeitgebern, Sozialleistungsträgern, Banken etc.) erteilen zu lassen.

Zunächst sind nach Auffassung des LfD für datenschutzrechtlich wirksame Einwilligungserklärungen in die Übermittlungen durch Sozialleistungsträger sowohl die Voraussetzungen des § 67 SGB X wie die des allgemeinen Datenschutzrechtes (§ 4 Abs. 2 BDSG; § 5 Abs. 2 LDatG R-P) zu beachten. Danach ist insbesondere die Person, die um Einwilligung ersucht wird, in geeigneter Weise über die Bedeutung der Einwilligung, den Verwendungszweck der Daten und den möglichen Empfängerkreis aufzuklären. Der Betroffene ist auch unter Darlegung der Rechtsfolgen darauf hinzuweisen, daß die Einwilligung verweigert und mit Wirkung für die Zukunft widerrufen werden kann.

Bereits diese Informationen fehlten in dem vorgelegten Formular.

Es hat sich aber auch eine Grundsatzfrage in diesem Zusammenhang ergeben: Es ist durchaus zweifelhaft, ob die bei der Durchführung von Strafermittlungsverfahren geforderten Einwilligungen im Regelfall wirklich freiwillig sind. Dies hängt wohl von der jeweiligen Fallkonstellation ab. Wenn beispielsweise Zeugen, die selbst nicht im Verdacht einer Straftat stehen und die die Einwilligung nur zur Erleichterung und Beschleunigung des Verfahrens abgeben, betroffen sind, bestehen an der Freiwilligkeit unter der Voraussetzung der oben angesprochenen hinreichenden Aufklärung grundsätzlich keine Bedenken.

Wenn jedoch der Beschuldigte selbst um Einwilligung ersucht wird, ist diese Frage anders zu beurteilen. Aus dessen Sicht ist häufig eine Zwangssituation gegeben. Er wird jedenfalls nicht selten den auch tatsächlich naheliegenden Eindruck gewinnen, daß ihm eine Verweigerung wohl mehr schadet als nützt, daß er sich z. B. bei einer Verweigerung der Einwilligung verstärkt verdächtig macht.

Aus der Sicht des LfD sollte deshalb gegenüber den Beschuldigten im Regelfall von der Einholung einer solchen Einwilligungserklärung abgesehen werden. Falls dies im Einzelfall bei besonderen Umständen auch unter Einbeziehung der genannten Gesichtspunkte unbedenklich wäre, könnte dies ohne formblattmäßige Gestaltung erfolgen.

Das Innenministerium hat zwar vorerst von der Einführung des Formblatts Abstand genommen, weil nach seiner Auffassung im Rahmen der Beratungen des 2. SGB-Änderungsgesetzes für den Inhalt des Formulars wesentliche Änderungen gesetzlich verankert werden könnten. Sein Ziel, ein entsprechendes Formular nach Beendigung dieses Gesetzgebungsverfahrens einzuführen, hat es aber nicht aufgegeben.

Der LfD wird sich, wenn diese Frage erneut aufgeworfen würde, dafür einsetzen, daß auch künftig nicht auf der Basis einer nur scheinbar gegebenen Freiwilligkeit in das informationelle Selbstbestimmungsrecht eingegriffen wird.

7.3.8 Was dürfen gemeinnützige Institutionen über den Geldbußen-Zahler erfahren?

Es kommt häufig vor, daß Gerichte die Einstellung des Verfahrens von der Zahlung einer Geldbuße abhängig machen. Dies ist dann zulässig, wenn nur eine geringe Schuld des Beschuldigten vorliegt und dieser zustimmt (§ 153 a Abs. 1 StPO).

Als Empfänger dieser Geldbußen werden regelmäßig privatrechtlich organisierte gemeinnützige Institutionen vorgeschlagen. In Rheinland-Pfalz handelt es sich um ca. 600 verschiedene Institutionen, von der Initiative Abenteuerspielplatz Worms bis zur Zoologischen Gesellschaft Frankfurt am Main. Dabei ist es nicht selten, daß bereits vor der Zustimmung der Betroffenen zur Zahlung der Geldbuße diese privatrechtlichen Vereine über die Person des Beschuldigten und die ihm gegenüber beabsichtigte Geldbuße informiert werden. Dies hat der LfD für unzulässig erachtet. Aber auch in den Fällen, in denen der Beschuldigte in die

Zahlung der Geldbuße einwilligt, hält er es nicht für erforderlich, den Empfänger der Geldbuße über die Identität des Beschuldigten, die Tatsache, daß dieser eine Geldbuße zu zahlen hat und das Aktenzeichen des Verfahrens zu informieren. Bezüglich beider Fallgestaltungen hat sich allerdings eine Kontroverse mit dem Ministerium der Justiz entwickelt.

Zunächst hat das Justizministerium zwar erklärt, es teile die Auffassung des LfD, daß die Unterrichtung des Zahlungsempfängers vor Zustimmung des Beschuldigten unter datenschutzrechtlichen Gesichtspunkten bedenklich sei. Es hat daher eine Änderung des entsprechenden Vordrucksatzes erwogen. Nach weiterer Prüfung hat es jedoch mitgeteilt, dies komme in der Praxis nur sehr selten vor. Außerdem sei es unabdingbar, in den Fällen, in denen die Zustimmung des Beschuldigten vorliege, der privatrechtlichen Empfängerorganisation das Aktenzeichen und die Höhe der erwarteten Geldbuße mitzuteilen. Dies sei datenschutzrechtlich nicht bedenklich. Es solle allerdings eine gesetzliche Ermächtigungsgrundlage in die Strafprozeßordnung eingefügt werden, um die bisherige Praxis auch gesetzlich abzusichern. Damit würden die datenschutzrechtlichen Bedenken ausgeräumt werden.

Dieses ist nicht zutreffend: Auch bei einer gesetzlichen Regelung des derzeit befolgten Verfahrens würde der LfD seine datenschutzrechtlichen Bedenken aufrechterhalten müssen. Eine Notwendigkeit, die gemeinnützigen Empfänger von Geldbußen über die Identität von Zahlungspflichtigen zu informieren, ist nicht erkennbar. So ist z. B. denkbar, daß der Zahlungspflichtige die Vorgabe erhält, die zu zahlende Geldbuße an die Justizkasse mit dem Hinweis auf den vorgesehenen Letztempfänger zu entrichten. Die Justizkasse ihrerseits würde dann die eingegangenen Zahlungen an die gemeinnützigen Institutionen weiterreichen. Damit wäre gewährleistet, daß keine Spendenquittungen ausgestellt werden; außerdem wäre eine effektive und zeitnahe Kontrolle des Zahlungseingangs möglich. Auch die verwaltungstechnische Umsetzung dieses Verfahrens dürfte aufgrund der bei den Justizkassen eingesetzten automatisierten Verfahren keine übergroßen Aufwendungen verursachen.

Unter Berufung auf haushaltsrechtliche Vorschriften und den mit dieser Lösung verbundenen Sach- und Personalaufwand hält das Ministerium der Justiz diese Vorgehensweise nicht für vertretbar. Der LfD ist nach wie vor von diesen Argumenten nicht überzeugt. Er bemüht sich, gemeinsam mit den anderen Datenschutzbeauftragten hier eine Verfahrensänderung der Justizverwaltungen zu erreichen.

7.3.9 Der Verdächtige in Spuren-Akten

Ein Sportler nahm an einem Marathon-Lauf teil. Der Start und die Rückkunft am Ziel wurden durch Urkunden und Teilnehmerausweise des Veranstalters bestätigt.

Monate später wurde der Marathon-Läufer von der Kriminalpolizei zu einem Mordfall, der sich acht Tage nach dem Wettkampf in diesem Gebiet ereignet hatte, verhört. Aus diesem Anlaß wurde eine Spurenakte angelegt, die der Hauptermittlungsakte beigefügt war und die von der Polizei an die Staatsanwaltschaft übermittelt wurde. Der Marathon-Läufer erfuhr davon und wollte vom LfD folgendes wissen:

- Wie lange bleibt die Spurenakte in der Hauptakte?
- Wie lange werden seine Fingerabdrücke und die von ihm zur Verfügung gestellten Urkunden (Nachweise über die Teilnahme am Marathon-Lauf) aufgehoben?
- Besteht eine Pflicht der Ermittlungsbehörden, ihn von der Vernichtung der Spuren-Akte zu unterrichten?

Es ergab sich folgendes:
Das Fahrzeug des Sportlers war einige Tage vor dem Mordfall wohl anläßlich des Marathonlaufes von einem Zeugen in der Nähe des Tatorts gesehen worden. Es war allerdings eindeutig festgestellt worden, daß der Marathon-Läufer als Täter nicht in Betracht kam. Da die Täterschaft definitiv ausgeschlossen werden konnte, hat aufgrund der Anfrage des LfD die zuständige Staatsanwaltschaft bzw. in ihrem Auftrag die tätig gewordene Polizei die Spuren-Akte insoweit vernichtet.

Spurenakten betreffen häufig Personen, gegen die kein hinreichender Verdacht besteht, um sie als Verdächtige oder Beschuldigte zu bezeichnen. Diese Personen stehen allerdings in einer losen Beziehung zu einer Straftat. Häufig erfahren sie weder von der Speicherung sie betreffender Informationen noch von der Vernichtung der Unterlagen in den Akten. Dies ist ein allgemeines Problem, das nicht ausdrücklich geregelt ist. Der LfD beabsichtigt, insoweit anzuregen, daß die Ermittlungsbehörden allgemein gültige Vorgaben erhalten, woraus sich insbesondere ergeben sollte, daß bei einem definitiven Täterschaftsausschluß entsprechende Spurenakten unverzüglich zu vernichten sind. Eine Unterrichtung des Betroffenen sollte immer dann erfolgen, wenn er von den ihn betreffenden Ermittlungsvorgängen Kenntnis erhalten hat. Diese Thematik steht im Zusammenhang mit einer generellen Erscheinung, die in letzter Zeit zunehmend an Bedeutung gewinnt: der Durchführung von Ermittlungen im Vorfeld, in bezug auf Straftaten, die nur vermutet werden können, gegenüber Personen, von denen möglich oder wahrscheinlich ist, daß sie beispielsweise dem organisierten Verbrechen nahestehen, bezüglich derer aber keine konkreten Verdachtsmomente vorliegen. Die hier erforderliche Abwägung zwischen Grundrechtsschutz des Individuums und Sicherheitsinteressen der Allgemeinheit ist schwierig und muß aus der Sicht des LfD – möglichst durch Gesetz – konkretisiert werden.

7.3.10 Die historische Aufarbeitung justitiellen NS-Unrechts

Im Zusammenhang mit der Überprüfung der NS-Sondergerichtserfahren hat das JM beabsichtigt, eine Dokumentation zu veröffentlichen, in der unter anderem personenbezogene Daten von Richtern und Staatsanwälten enthalten sein sollten, die an derartigen Verfahren mitgewirkt haben. Dabei sollten einzelne Urteile mit den Namen der mitwirkenden Richter und Staatsanwälte abgedruckt werden, es sollten aber auch weitere Angaben über die betroffenen Amtsträger (insbesondere die Mitteilung ihres Werdeganges in der Zeit des Dritten Reiches sowie während der Zeit nach dem Zweiten Weltkrieg) veröffentlicht werden.

Nach der Auffassung des LfD unterscheidet sich die datenschutzrechtliche Beurteilung der Veröffentlichung von Informationen grundsätzlich, je nachdem ob diese Informationen unmittelbare nach außen wirkende amtliche Tätigkeiten der betroffenen Amtsträger oder ob sie eher das beamten- oder richterrechtliche Grundverhältnis zu ihrem Dienstherrn zum Gegenstand haben. Im ersten Fall ist der LfD der Auffassung, daß das informationelle Selbstbestimmungsrecht grundsätzlich keine Wirksamkeit entfaltet (vgl. 13. Tb., Tz. 17.3).

Im zweiten Bereich ist zugunsten des Amtsträgers das informationelle Selbstbestimmungsrecht in vollem Umfang zu beachten.

Als Vorfrage war nach Auffassung des LfD zudem zu klären, ob die entsprechenden Informationen nur Personen betreffen, die inzwischen verstorben sind. In diesem Fall wäre dem vom Ministerium der Justiz betonten Gedanken der zeitabhängigen Verringerung des Schutzbedürfnisses auch aus der Sicht des LfD maßgebliche Bedeutung zugekommen.

Wenn die betroffenen Amtsträger allerdings nicht verstorben waren, ist der LfD der Auffassung, daß Angaben zu ihrem persönlichen beruflichen Werdegang nur mit ihrer Einwilligung veröffentlicht werden dürften, solange hierfür keine ausdrückliche gesetzliche Grundlage besteht.

Das Ministerium der Justiz hat dieser Auffassung nicht widersprochen.

7.4 Strafvollzug

7.4.1 Das Strafvollzugsgesetz läßt die Datenschutzfragen noch immer ungeregelt

Der LfD beklagt, daß bezüglich des Erlasses datenschutzrechtlicher Ergänzungen des Strafvollzugsgesetzes nach wie vor kein Fortschritt festzustellen ist. Er hatte bereits im 13. Tätigkeitsbericht Veranlassung, das gesetzgeberische Unterlassen in diesem Bereich festzustellen. An der seinerzeit geschilderten Situation hat sich leider in den vergangenen zwei Jahren nichts geändert.

7.4.2 Wie vertrauenswürdig ist der LfD?

Die Frage, ob der Schriftwechsel von Gefangenen mit der Datenschutzkontrollinstitution unter Umgehung der anstaltsinternen Postkontrolle zulässig sein soll sowie ob und unter welchen Voraussetzungen dieser die Justizvollzugsanstalten besuchen darf, waren solange nicht weiter regelungsbedürftig, wie die DSK die Aufgabe der unabhängigen Datenschutzkontrolle in Rheinland-Pfalz wahrgenommen hat. Diese Kommission war beim Landtag angesiedelt und bestand zum überwiegenden Teil aus Abgeordneten. Die für den Schriftverkehr mit Abgeordneten bzw. die für den Petitionsausschuß geltenden Regelungen dürften in diesem Zusammenhang auf die DSK anzuwenden gewesen sein. In der Praxis haben sich hier keine Probleme ergeben.

Mit der Einrichtung der Institution des LfD, der zwar beim Landtag angesiedelt ist, der jedoch als oberste Landesbehörde unabhängig und nicht Teil der Legislative ist, hat sich aus der Sicht des LfD ein Klarstellungsbedarf ergeben, auch wenn es bislang hier noch nicht zu praktischen Problemen gekommen ist.

Er hat deshalb angeregt, den LfD genau wie schon bislang den Bürgerbeauftragten sowohl in den Bereich der Regelungen einzubeziehen, die die Überwachung des Schriftwechsels betreffen, wie in die Regelungen, die die Besuche von Justizvollzugsanstalten durch anstaltsfremde Personen zum Gegenstand haben. In diesem Zusammenhang sollte in gleicher Weise auch die Überwachung des Schriftwechsels von Untersuchungsgefangenen mit dem LfD geregelt werden.

Die Auffassung des Ministeriums der Justiz zu dieser Anregung ist dem LfD derzeit noch nicht bekannt.

7.4.3 Wissenschaftliche Forschung in Justizvollzugsanstalten

Eine Bedienstete einer JVA wollte in der Anstalt, in der sie dienstlich tätig war, eine wissenschaftliche Befragung zur Situation der Partnerinnen von Inhaftierten durchführen.

Dieses Projekt machte erneut deutlich, wie problematisch es aus datenschutzechtlicher Sicht ist, wenn Bedienstete einer JVA wissenschaftliche Untersuchungen an der Vollzugsanstalt durchführen, in der sie auch ansonsten tätig sind.

Datenschutzrechtlich problematisch erschien bereits die Erhebung von Namen und Anschriften der Partnerinnen einsitzender Gefangener in der JVA bei den Gefangenen. Eine solche, wissenschaftlichen Zwecken dienende Datenerhebung ist auch im Bereich der JVA nur auf der Basis der völligen Freiwilligkeit zulässig. Dies ergibt sich aus dem auch für Gefangene insoweit geltenden Grundrecht auf informationelle Selbstbestimmung. In der JVA besteht jedoch gegenüber Bediensteten, auch gegenüber Mitarbeitern des Sozialdienstes, grundsätzlich eine Situation, in der nur schwer eine echte Freiwilligkeit in diesem Zusammenhang angenommen werden kann. Es besteht immer die Gefahr, daß Gefangene befürchten, daß eine Verweigerung der Preisgabe entsprechender Angaben gegenüber einem Bediensteten der JVA als Akt der Konfrontation und des fehlenden Willens zur Zusammenarbeit aufgefaßt wird. Damit könnte für den Gefangenen die Befürchtung verbunden sein, daß er bei der Beantragung von Vergünstigungen benachteiligt wird, wenn er nicht auch im Zusammenhang mit solchen Datenerhebungen kooperiert. An die Freiwilligkeit der Datenerhebung sind deshalb – worauf die DSK in der Vergangenheit bereits hingewiesen hat (vgl. 12. Tb., Tz. 7.4.2.2) – dann besondere Anforderungen zu stellen, wenn Bedienstete der JVA einbezogen sind. Als taugliche Maßnahme in diesem Zusammenhang wäre beispielsweise anzusehen, daß nur solche Gefangene von Bediensteten befragt werden, die in keinem denkbaren Zusammenhang mit diesen in dienstlichen Kontakt kommen können.

Ein zweiter im Zusammenhang mit der Nutzung der bei den befragten Lebensgefährtinnen erhobenen Daten stehender Aspekt ließ die Befragung in der beabsichtigten Weise zusätzlich problematisch erscheinen. Zweck der Nutzung der erhobenen Daten sollte ausschließlich die Gewinnung wissenschaftlicher Erkenntnisse sein.

Auf der Basis der erhobenen Daten war es jedoch praktisch nicht ausgeschlossen, daß der Bedienstete Informationen über die Lebensumstände einsitzender Gefangener gewann, die auch für seine dienstliche Tätigkeit im Rahmen des Sozialdienstes Bedeutung hätten gewinnen können. Beispielsweise ist daran zu denken, wenn eine der befragten Lebensgefährtinnen angibt, sie wolle sich von ihrem einsitzenden Partner trennen, daß diese Information im Rahmen einer Sozialprognose bei anstehenden Entscheidungen (etwa Aussetzung des Strafrestes zur Bewährung, Urlaubsgewährung o.ä.) bedeutsam sein kann. Da die ausgefüllten Fragebogen auch Angaben zum einsitzenden Partner enthalten und insoweit für denjenigen relativ leicht reidentifizierbar gewesen wären, der in der JVA Zugang zu entsprechenden Informationen über die Gefangenen besitzt (wie dies bei einem Mitarbeiter des Sozialdienstes der Fall sein dürfte), wäre der Bedienstete möglicherweise in die grundsätzlich datenschutzrechtlich unerwünschte Konfliktlage geraten, entweder seine aus der wissenschaftlichen Untersuchung erlangten Kenntnisse entgegen dienstlicher Notwendigkeiten nicht zu verwerten oder die grundsätzlich bestehende Zweckbindung zu durchbrechen. Es ist ein datenschutzrechtliches Anliegen, solche Konfliktlagen für öffentlich Bedienstete nicht entstehen zu lassen.

Bei der Durchführung einer entsprechenden Befragung bei einer anderen JVA würden sich entsprechende Probleme – wenn überhaupt – in sehr viel geringerem Umfang stellen.

Das Ministerium der Justiz hat aufgrund dieser Überlegungen des LfD die Untersuchung an der Anstalt, in der der Bedienstete tätig war, nicht genehmigt.

Im Zusammenhang mit Befragungen von Gefangenen anläßlich wissenschaftlicher Forschungsvorhaben ist es grundsätzlich datenschutzrechtlich bedeutsam, in welcher Form die Bediensteten der Justizvollzugsanstalten in die Befragung einbezogen werden. Dabei ist insbesondere für die datenschutzrechtliche Beurteilung von Interesse, ob Bedienstete der Justizvollzugsanstalt bei der Erstellung der Interviews beteiligt sind, ob sie die ausgefüllten Interviewfragebogen zur Kenntnis erhalten (u. U. im Zusammenhang mit der Ausgangskontrolle von schriftlichem Material), ob sie – ggf. in welcher Form – Informationen über die Gefangenen (z. B. Namen und Straftat) an die Wissenschaftler übermitteln und ob dies ggf. auf einer informierten Einwilligung der betroffenen Gefangenen beruht.

Außerdem ist klärungsbedürftig, in welcher Form und mit welchem Inhalt die Einwilligung der Gefangenen eingeholt wird. Wenn die Datenerhebung durch Interviews erfolgen soll, ist grundsätzlich eine Einwilligung unabdingbar. Ob die Schriftform erforderlich ist, dürfte in erster Linie davon abhängen, ob die erhobenen Daten in personenbeziehbarer Form automatisiert gespeichert werden (§ 5 Abs. 3 LDatG). Zur Beurteilung dieser Frage ist regelmäßig die Vorlage des entsprechenden Interviewfragebogens erforderlich. Darauf hat der LfD bei verschiedenen Anmeldungen wissenschaftlicher Forschungsvorhaben in Justizvollzugsanstalten hingewiesen.

Bei der Beurteilung eines Forschungsvorhabens der Kriminologischen Zentralstelle e. V. in Wiesbaden war insbesondere problematisch, ob die Mitarbeiter der Kriminologischen Zentralstelle wirksam nach dem Verpflichtungsgesetz verpflichtet worden sind, wie das Ministerium der Justiz behauptete. Dann würden sie bei unbefugten Datenweitergaben strafrechtlich wie Beamte zu behandeln sein. Zweifel an einer wirksamen Verpflichtung ergaben sich insbesondere daraus, daß nicht geklärt ist, welche Behörde von welcher (zuständigen) Landesregierung durch Rechtsverordnung dazu bestimmt worden ist, die Verpflichtung vorzunehmen. Eine solche in einer Rechtsverordnung getroffene Bestimmung ist im vorliegenden Zusammenhang aber nach dem Wortlaut des Verpflichtungsgesetzes erforderlich, weil die Kriminologische Zentralstelle privatrechtlich organisiert ist. Im konkreten Fall konnte der LfD auf eine abschließende Klärung dieser Frage verzichten, weil dieser Aspekt für die Beurteilung der datenschutzrechtlichen Zulässigkeit der Durchführung der in Rede stehenden Befragung nicht entscheidend

war. Eine strafrechtliche Gleichsetzung der betroffenen Bediensteten der Kriminologischen Zentralstelle mit Amtsträgern ergab sich bereits aus § 11 Abs. 1 Nr. 2 c StGB. Dennoch hält es der LfD für wünschenswert, daß auch in Rheinland-Pfalz durch die Schaffung entsprechender Rechtsgrundlagen in derartigen Fällen wirksame Verpflichtungen nach dem Verpflichtungsgesetz erfolgen können.

7.4.4.1 Eine Liste der islamischen Gefangenen

Im Jahr 1992 fand in einer JVA das islamische Opferfest unter Beteiligung der benachbarten türkischen Moschee statt. Die Initiative zur Durchführung dieses Festes ging von türkischen Gefangenen aus. Die Organisation des Festes innerhalb der Anstalt wurde unter Aufsicht der Vollzugsdienstleitung von einigen türkischen Gefangenen durchgeführt. Es war erforderlich, daß die teilnehmenden Gefangenen einen Geldbeitrag leisteten.

Die Anstalt hat einem Gefangenen zum Zweck der Befragung über die Teilnahme und des Geldeinsammelns eine Namensliste der moslemischen Gefangenen nach Schwärzung weiterer personenbezogener Daten überlassen.

Aus der Sicht des LfD war diese Angelegenheit wie folgt zu beurteilen:

Die in Rede stehende Liste der Gefangenen islamischen Glaubens war deutlich erkennbar aus einem System der automatisierten Datenverarbeitung ausgedruckt worden. Damit waren die formellen Anwendungsvoraussetzungen des Landesdatenschutzgesetzes gegeben. Informationen aus einem automatisierten System dürfen nur dann an private Dritte übermittelt werden, wenn dies gesetzlich ausdrücklich zugelassen ist oder wenn die Betroffenen eingewilligt haben (§ 7 Abs. 1 LDatG). Eine gesetzliche Grundlage für die Übermittlung einer Liste, wie sie vorliegend in Rede steht, an einen Mitgefangenen zum Zweck der Durchführung eines religiösen Festes ist nicht ersichtlich. Auch eine Einwilligung der betroffenen Gefangenen im Sinne des § 5 Abs. 3 LDatG lag nicht vor.

Veranstaltungen, wie sie mit Hilfe dieser Liste durchgeführt werden sollten, sind sicherlich förderungswürdig. Es dürfte zu ihrer Organisation jedoch nicht unabdingbar sein, solche Listen ohne Einwilligung der Betroffenen an Mitgefangene auszuhändigen. Falls jedoch aus anstaltsinternen Gründen nur der im vorliegenden Fall beschrittene Weg in Betracht kommt, um derartige Veranstaltungen durchzuführen, bedürfte es einer normenklaren gesetzlichen Regelung (etwa im Strafvollzugsgesetz), die solche Datenübermittlungen regelt und rechtfertigt. Wegen der Gefahr der zweckwidrigen Verwendung solcher Listen erscheint dieses Ergebnis auch angemessen.

Der LfD hat das Ministerium der Justiz über diese datenschutzrechtliche Würdigung informiert.

7.4.4.2 Die verschwundene Gefangenenpost

Aus einem Beschluß des Landgerichts Koblenz (Az.: 7 StVK 555/92), auf den der LfD von einem Gefangenen hingewiesen wurde, ergab sich folgender Sachverhalt: In den vergangenen Monaten hätten sich vor der Strafvollstreckungskammer die Verfahren, in denen es darum ging, daß die JVA ohne Rechtsgrundlage den Schriftwechsel der Gefangenen überwachte, gehäuft. Bei dem Schriftwechsel habe es sich insbesondere um Hauspost, aber auch um Verteidigerpost gehandelt. Stets habe die JVA angeführt, daß bedauerliche Versehen im Einzelfall vorlägen, weshalb ein prozessuales Feststellungsinteresse aus dem Gesichtspunkt der Wiederholungsgefahr nicht vorliege. Dem sei das Landgericht auch bislang gefolgt, was jedoch im Hinblick auf die immer wieder neu auftretenden „Einzelfälle" nicht mehr haltbar sei. Außerdem liege ein Feststellungsinteresse auch unter dem Gesichtspunkt der Schwere der Rechtsverletzung vor. Mit der gebotenen Sorgfalt bei der Behandlung eingehender Post, insbesondere der Verteidigerpost, die einer Kontrolle entzogen sei, könne es nicht vereinbart werden, wenn gleich mehrere Briefe unbemerkt aus der Telefonzentrale verschwinden würden, sodann geöffnet würden und schließlich an einen völlig falschen Platz, nämlich in einen Aktenverteilerraum, gelangten, ohne daß die JVA in der Lage sei, die näheren Umstände des Geschehens aufzuklären. Dies gelte um so mehr deshalb, weil mit der Behandlung der Post bis zu deren Öffnung nur wenige Beamte befaßt seien. In dem vom Landgericht entschiedenen Fall sei der ursprünglich verschwundene Brief nach dem Öffnen wieder mit einer Verschlußmarke versehen in den gewöhnlichen Geschäftsgang gelangt.

Vor diesem Hintergrund hat die Strafvollstreckungskammer im Tenor des zitierten Beschlusses festgestellt, daß die Öffnung von zwei für den Antragsteller eingegangenen Briefen rechtswidrig gewesen sei.

In Anbetracht der Tatsache, daß es sich offensichtlich bei dem entschiedenen Fall nicht um eine Ausnahme gehandelt hat, hat der LfD das Ministerium der Justiz um Mitteilung gebeten, welche Vorkehrungen seitens der JVA bzw. seitens des Ministeriums der Justiz getroffen wurden bzw. getroffen werden, um Vorgänge wie den vom Landgericht entschiedenen künftig möglichst auszuschließen.

In seiner Antwort erklärte das Ministerium, es seien organisatorische Maßnahmen getroffen worden, die es künftig ausschlössen, daß ein Bediensteter, der Verteidigerpost versehentlich öffne, nicht mehr zu ermitteln sei. Dies wurde nicht näher konkretisiert. Der LfD hat die Antwort als unzureichend angesehen und deshalb örtliche Feststellungen durchführen lassen.

Diese haben folgendes ergeben:

Täglich erreichen die JVA ca. zwei große Körbe voll Post. Es wird geschätzt, daß dies etwa 500 bis 600 Sendungen seien. Von montags bis freitags sei der Abteilungsdienstleiter verantwortlich, der die Eingangspost sortiere, in solche, die der Briefkontrolle unterliege und solche, die kontrollfrei sei. Die sortierten Briefe würden durch eine andere Stelle (wohl jeweils stockwerksweise) erneut durchgesehen. Andere Probleme gäbe es am Samstag, da die eingearbeiteten Bediensteten an diesem Tag grundsätzlich nicht zur Verfügung stünden und andere Kräfte dann verantwortlich seien. Es werde überlegt, die Samstagspost erst am Montag zu verteilen. Außerdem seien Plakate mit Informationen über die kontrollfreie Post in der Poststelle ausgehängt. Schließlich werde künftig ohne Zeitdruck in diesem Zusammenhang gearbeitet, die Post werde erst im Spätdienst ausgegeben.

Dies dürfte zumindest die Anfälligkeit für fahrlässig begangene Fehler herabsetzen.
Aus datenschutzrechtlicher Sicht konnte das jetzige Verfahren aber akzeptiert werden.

7.5 Gerichtliche Register

7.5.1 Welches datenschutzrechtliche Gefährdungspotential liegt in den gerichtlichen Registern?

Zu den gerichtlichen Registern gehören das Grundbuch, das Vereinsregister, das Genossenschaftsregister, das Handelsregister, das Schiffahrtsregister, das Schuldnerverzeichnis, das Konkursregister.

In den Genossenschaftsregistern sind beispielsweise auch die Namen und Anschriften der „Genossen" der Genossenschaftsbanken verzeichnet. Im Vereinsregister sind die Gründungsmitglieder der jeweiligen Vereine (mindestens sieben) sowie die Funktionsträger (Vorsitzender, Kassierer) regelmäßig vermerkt. Der Inhalt des Grundbuches (Eigentümer von Grundstücken sowie Belastungen, die auf dem Grundstück ruhen) ist bekannt. Aus dem Handelsregister ergeben sich die wirtschaftlichen Aktivitäten der Einzelkaufleute, bei Gesellschaften enthält das Register u. a. die Namen der haftenden Personen (bei der GmbH der Geschäftsführer).

Da in diesen Registern auch fortlaufend die Veränderungen verzeichnet werden, ergibt sich über einen längeren Zeitraum hin weg insbesondere auch bei den Handelsregistern ein interessantes Bild der Entwicklung einzelner gewerbetreibender Personen. Wenn man sich vorstellt, daß alle diese Register bundesweit in automatisierter Form zentralisiert geführt werden würden und es möglich wäre, auf Knopfdruck alle in gerichtlichen Registern gespeicherten Informationen zu bestimmten natürlichen Personen abzurufen, könnten sich interessante und vielfältig verwendbare Persönlichkeitsprofile ergeben.

So wäre z. B. erkennbar, wenn Herr Meier Gründungsmitglied eines Vereins für die Unterstützung Behinderter e. V. geworden ist, daß er zum dritten Mal die Geschäftsführertätigkeit gewechselt hat und daß seine Grundstücke erheblich überschuldet sind.

Auf die Verwechslungsgefahr aufgrund der unzureichenden Speicherung von Identitätsmerkmalen (Geburtsdatum) hat der LfD im 13. Tb., Tz. 7.5, hingewiesen. Diese Gefahr erhöht sich, je umfangreicher die Zahl der gespeicherten Personen wird; sie kann bei bundesweiten Registern nicht hoch genug eingeschätzt werden.

Ein verantwortungsbewußter Umgang mit den hier gespeicherten Informationen ist also aus datenschutzrechtlicher Sicht unabdingbar. Maßstab darf nicht sein, was technisch möglich ist, sondern was unabdingbar erforderlich ist, um die Zwecke der gerichtlichen Register zu erfüllen. Der Einsatz der Automation allein bewirkt in diesem Bereich bereits eine qualitative Änderung der Informationslandschaft, deren Folgen derzeit noch gar nicht abschätzbar sind und die aus der Sicht des LfD zunächst das Tätigwerden des Gesetzgebers erfordert. Vom Gesetzgeber sind Sensibilität und Weitblick zu verlangen.

7.5.2 Registerverfahrensbeschleunigungsgesetz

Die Bundesregierung hat einen Gesetzentwurf vorgelegt, der die Automation und die zentralisierte Speicherung einiger gerichtlicher Register (einschließlich des Grundbuchs) ausdrücklich erlaubt (BR-Drs. 360/93). Die datenschutzrechtlichen Aspekte sind dabei aus der Sicht des LfD allerdings nicht ausreichend einbezogen worden. Er hat gegenüber dem Minister der Justiz und dem Bundesbeauftragten für den Datenschutz auf folgendes hingewiesen:

a) Zur Frage der Protokollierung der Einsichtnahme in Grundbücher:

   Das im derzeit vorliegenden Entwurf verfolgte Anliegen, die Einsichtnahmen in das Grundbuch durch eine Protokollierung nachvollziehbar zu gestalten, wird nachdrücklich unterstützt. Es entspricht einer seit langem erhobenen Forderung der Datenschutzbeauftragten.

Aufgrund einer größeren Zahl von Eingaben hatte sich bereits in der Vergangenheit für die Datenschutzbeauftragten die Notwendigkeit ergeben, für eine Protokollierung entsprechender Einsichtnahmen einzutreten (10. Tb., Tz. 6.3). Weitere Probleme im Zusammenhang mit der Grundbuchführung und dem informationellen Selbstbestimmungsrecht sind in der Fachliteratur dargestellt worden (z. B. Böhringer in „Der Deutsche Rechtspfleger" 1989, S. 309 bis 313).

Ursprünglich sah der Gesetzentwurf folgendes Protokollierungsverfahren vor: Der Bedienstete des Grundbuchamts sollte den Vorgang der Einsichtnahme mit einer Verfügung in der Grundakte bearbeiten. Darin sollte zunächst festgehalten werden, wer Einsicht genommen habe. Der Eigentümer hätte jederzeit Gelegenheit, dies zur Kenntnis zu nehmen. Dieses Verfahren ist zu begrüßen, allerdings widerspricht der derzeitige Text, insbesondere der Begründung, dieser Verfahrensweise; das geschilderte Verfahren sollte im Gesetzestext selbst deutlich Ausdruck finden. Die Alternative, entsprechende Listen über die Einsichtnahmen zu führen („Berliner Lösung"), ist datenschutzrechtlich mindestens gleichwertig. Da sich diese Verfahrensweise in der Praxis zu bewähren scheint und – nach dem hier bestehenden Kenntnisstand – von der Berliner Justizverwaltung bislang nicht belegt wurde, daß ein zu großer Verwaltungsaufwand entstünde, tritt der LfD für diese Lösung ein und appelliert an das Ministerium der Justiz, sie zu unterstützen. Zwischenzeitlich haben die Justizressorts der Länder allerdings mehrheitlich sogar für eine Streichung der Protokollierungsregelung plädiert. Eine ersatzlose Streichung der Protokollierungsregelung aus dem Entwurf könnte keinesfalls hingenommen werden.

b) Automatisierte Grundbuchführung

Für die Protokollierung von Einsichtnahmen bei der automatisierter Führung des Grundbuchs dürften besondere Regelungen erforderlich sein. Die Zentralisierung automatisiert geführter Grundbücher ist in § 126 Abs. 4 der Grundbuchordnung in der Entwurfsfassung nur in der Form angesprochen, daß eine Auftragsdatenverarbeitung durch andere öffentliche Stellen zulässig sein soll, daß aber Zugriffsmöglichkeiten davon nicht betroffen sein sollen (so jedenfalls S. 128 f. der Begründung). Der LfD geht davon aus, daß eine zentrale (landes- oder bundesweite) Grundbuchführung mit entsprechend erweiterten Auswertungsmöglichkeiten nach dem Entwurf ausgeschlossen ist. Dies sollte allerdings im Gesetzestext deutlich werden. Es sollten auch die datenschutzrechtlichen Chancen bei einer Automation der Grundbücher genutzt werden. So ließen sich Probleme der Streichung von Eintragungen sicher datenschutzgerecht dadurch lösen, daß für gelöschte Daten gesonderte Dateien eingerichtet werden, auf die auch nur dann Zugriff gestattet wird, wenn gerade an deren Kenntnis ein berechtigtes Interesse besteht. Gleiches gilt für Eintragungen von Belastungen etc., die Miteigentümer betreffen.

c) Online-Anschlüsse

Im Bereich der automatisierten Registerführung ist die Regelung der Online-Anschlüsse von besonderem Interesse. § 133 befaßt sich mit entsprechenden Zugriffen auf das Grundbuch, § 9 a des HGB-Änderungsentwurfs mit Online-Zugriffen auf das Handelsregister (mit entsprechender Geltung für das Genossenschaftsregister), § 79 Abs. 3 BGB-Änderungsentwurf mit Online-Zugriffen auf das Vereinsregister.

aa) Grundsätzlich ist der Online-Anschluß Privater an öffentliche Register aus datenschutzrechtlicher Sicht bedenklich und nur ausnahmsweise bei Regelung wirksamer Begleitmaßnahmen des technischen und organisatorischen Datenschutzes akzeptabel. Unabdingbare Forderung in diesem Zusammenhang ist in jedem Fall eine lückenlose Protokollierung der Zugriffe und eine damit einhergehende praktische Kontrollmöglichkeit. Dies betrifft auch die automatisierten Zugriffe anderer Behörden als der Grundbuchämter. Die allgemeine Regelung der Nr. 6 der Anlage zu § 9 Satz 1 BDSG reicht in diesem Zusammenhang nicht aus. Danach ist nur eine nachträgliche generelle Überprüfung und Feststellung des Zugriffsumfangs bei Online-Abrufen vorgesehen. Eine Kontrollmöglichkeit einzelner konkreter Abrufe ist danach nicht vorgesehen. Besonders bedenklich wäre dies, wenn sich aus der Verweisung auf § 9 BDSG in dem Gesetzentwurf ergeben soll, daß weitergehende landesrechtliche Vorschriften insoweit keine Anwendung finden sollen.

bb) Von besonderer Bedeutung ist sicherlich in diesem Zusammenhang der Online-Zugriff auf das Grundbuch. Nach dem Entwurf können auch Private diese Möglichkeit nutzen, wenn sie dinglich Berechtigte sind. Deren Zugriffsmöglichkeit soll auf „eigene Rechte" beschränkt sein. Soweit technisch sichergestellt werden kann, daß nur tatsächlich im Grundbuch eingetragene dinglich Berechtigte auch eine faktische Zugriffsmöglichkeit, beschränkt auf den sie betreffenden Datenbestand, haben, wäre eine solche Regelung akzeptabel.

cc) Die Online-Anschlüsse zum Handelsregister für private Stellen sind in der vorgesehenen Form aus der Sicht des LfD zu weitgehend. Die vorgeschlagene Generalklausel, die für die Zulassung eines Online-Anschlusses allein auf die Erfüllung gesetzlich zugewiesener Aufgaben (bei öffentlich-rechtlichen Datenempfängern) sowie die Wahrnehmung berechtigter beruflicher oder gewerblicher Interessen bei privaten Datenempfängern abstellt, wird insbesondere den unten genannten qualitativ neuen Bedingungen bei einer zentralen Registerführung nicht gerecht. Außerdem ist auch hier die Regelung einer umfassenden Protokollierung der Abrufe zu fordern.

d) Im Entwurf (Artikel 6, § 125 Abs. 4 FGG, Begründung S. 188) ist vorgesehen, eine bundesweit zentralisierte Handelsregisterführung zu ermöglichen. Die dafür vorgeschlagenen Vorgaben sind minimal („im Auftrag des zuständigen Amtsge-

richts", „wenn die ordnungsgemäße Erledigung der Registersachen sichergestellt ist"). Angesichts der qualitativ neuen Möglichkeiten der Auswertung bei einem bundesweit zentral geführten Register ist dies eine unzureichende Regelung. Hier ist an Namensauswertungen zu denken, die für eine unbegrenzte Vielzahl von Fällen der gesetzmäßigen Aufgabenerfüllung vieler unterschiedlicher Behörden dienen könnten (Finanzämter, Ordnungsbehörden, Strafverfolgungsbehörden, Vollstreckungsorgane etc.), die aber die wirtschaftliche Betätigung der Bürger in einem bisher faktisch nicht erreichten Maß durchsichtig machen (bei einer Erstreckung dieser Möglichkeiten auf das Genossenschaftsregister wäre dieser Überblick noch umfassender). Es gibt sicherlich eine Vielzahl legitimer Zwecke in diesem Zusammenhang, es ist aber zu beachten, daß die Informationslandschaft im Bereich der wirtschaftlichen Betätigung damit praktisch erheblich verändert wäre. Die Erwägungen des BGH zu einem zentralen Handelsregister (die er einer Stellungnahme des Hessischen Ministers der Justiz entnommen hat, Beschluß vom 12. Juli 1989, NJW 89, 2818) sollten nicht in Vergessenheit geraten. Er führt aus: „Mit der zentralen Datenbank ... könnten Informationsprofile erstellt werden, die möglicherweise den Kernbereich der informationellen Selbstbestimmung tangieren." Diese Nutzung der EDV berühre „das informationelle Selbstbestimmungsrecht der Betroffenen in einem wesentlich größeren Ausmaß als die bisher mögliche Einsicht in das Handelsregister ... ". Der Gesetzgeber sollte deshalb hier ausdrücklich entscheiden, welche Zwecke zulässigerweise mit diesem neuen Informationssystem verfolgt werden dürfen; diese Zwecke müssen enumerativ genannt und klar beschränkt sein. Außerdem sind wirksame Vorkehrungen auf der Ebene des Gesetzes gegen Gefahren zu treffen: Verwechslungsgefahren müssen minimiert werden (Vorbild: Bundeszentralregister), Zweckdurchbrechungen müssen zumindest nachträglich überprüfbar sein.

Der LfD hat das Ministerium der Justiz gebeten mitzuteilen, ob und in welchem Umfang es seine Empfehlungen aufgreifen und im Bundesrat vorbringen werde.

8 Kultusbereich

8.1 Datenverarbeitung in Schulen

8.1.1 Vordringen der automatisierten Datenverarbeitung in Schulen

Inzwischen liegen ca. 400 Anmeldungen automatisierter Anwendungen von Schulen vor. Bei einer Gesamtzahl von ca. 1 600 allgemeinbildenden Schulen (Grund- und Hauptschulen, Sonderschulen, Realschulen, Gymnasien, Integrierte Gesamtschulen und Privatschulen) nutzt ein erheblicher Prozentsatz die automatisierte Datenverarbeitung zu Schulverwaltungszwecken. Ein Schwerpunkt ist dabei der Gymnasialbereich: Von 138 Gymnasien hat nahezu jedes die Nutzung der automatisierten Datenverarbeitung angemeldet.

Dabei kommen sehr unterschiedliche Systeme zur Anwendung:
Zentral entwickelte Verfahren in diesem Bereich, d. h. Verfahren, die in einer Vielzahl von Schulen angewendet werden, gibt es für die Studenplanerstellung sowie für die allgemeine Schulverwaltung. In erster Linie handelt es sich dabei um folgende Anwendungen (Zahlen aus dem Jahr 1992):

- Das System „AUSTER" (Automatische Stundenplanerstellung) wenden 175 Schulen an (78 Gymnasien, 48 Realschulen, 30 Hauptschulen, vier Gesamtschulen, sechs Berufsschulen, neun Privatschulen).
- Für den Bereich der allgemeinen Schulverwaltung existiert das System „SCHUD" (Schuldatei). Es ist von 195 Schulen (53 Gymnasien, 40 Realschulen, 76 Hauptschulen, vier Gesamtschulen, 13 Privatschulen und neun Berufsschulen) angemeldet worden.
- Das System „VEPLA" (Vertretungsplan) wird von 26 Schulen eingesetzt (17 Gymnasien, sechs Realschulen, zwei Hauptschulen, eine Gesamtschule).

Die sonstigen Anmeldungen beziehen sich in erster Linie auf eigene Software-Anwendungen der betroffenen Schulen, die individuell entwickelt worden sind. Der LfD hat in diesem Zusammenhang auch die Aufgabe, jeweils auf die Einhaltung datenschutzrechtlicher Vorschriften, insbesondere zum technischen und organisatorischen Datenschutz, hinzuwirken. Zweifelsfragen ergeben sich häufig bei der Entscheidung, ob bestimmte Schülermerkmale gespeichert werden dürfen.

Die Hardware in Schulen besteht im Regelfall aus Arbeitsplatzrechnern. Im Gegensatz beispielsweise zur früher üblichen Diskettenverarbeitung, bei welcher ein unbefugter Zugriff durch sichere Aufbewahrung der Datenträger verhindert werden konnte, erfordern die aufgrund der technischen Entwicklung gestiegenen Nutzungs- und Auswertungsmöglichkeiten beim Einsatz von Plattenspeichern neue Überlegungen hinsichtlich der Sicherstellung datenschutzrechtlicher Anforderungen.

Weiterhin haben sich in Gesprächen mit betroffenen Anwendern Fragen zur erforderlichen Absicherung und Betreuung der eingesetzten Systeme sowie im Hinblick auf die Vorgehensweise in bestimmten Wartungs- und Reparaturfällen ergeben. Auch einige Fälle von Diebstählen solcher PC, auf deren Speicherplatte Verwaltungsdaten gespeichert waren, aus Schulen sind vorgekommen.

Der LfD hat deshalb gegenüber den Bezirksregierungen sowie dem Ministerium angeregt, die Schulen auf folgende Maßnahmen hinzuweisen:

a) Absicherung der Systeme (Zugangs- und Zugriffskontrolle)

Als Arbeitsplatzrechner werden überwiegend sogenannte IBM-kompatible Geräte mit dem Betriebssystem MS-DOS oder entsprechenden Derivaten eingesetzt. Diese Systeme besitzen standardmäßig keinen oder nur unzureichenden Schutz gegen eine mißbräuchliche Nutzung. Die Verarbeitung personenbezogener Daten wie Schüler-/Lehrerverwaltung oder Zeugniserstellung ist ohne Verstoß gegen datenschutzrechtliche Bestimmungen nur auf der Grundlage einer angemessenen Datensicherheit zulässig (vgl. Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 10. Oktober 1988). Neben organisatorischen Maßnahmen sind daher entsprechende technische Möglichkeiten bereits bei der Beschaffung der Systeme vorzusehen. In Betracht kommen hierbei der Einsatz von Sicherheitssoftware (Zugangs- und Zugriffsschutz, Verschlüsselung, Protokollierung) oder entsprechende Hardware-Lösungen.

Soweit personenbezogene Daten verarbeitet werden, sollte der Einsatz derartiger Produkte mit der gleichen Selbstverständlichkeit erfolgen wie der einer Textverarbeitungs- oder Datenbanksoftware. Die Angemessenheit solcher Maßnahmen auch unter Kostengesichtspunkten ist – neben dem vergleichsweise geringen Anteil an den Gesamtkosten – nicht zuletzt dadurch gegeben, daß aufgrund der allgemeinen Preisentwicklung im PC-Bereich freigewordene Mittel zur Verfügung stehen. Für bestimmte Produkte bestehen zudem im Bereich der Landesregierung rabattierte Rahmenverträge.

b) Betreuung der eingesetzten Systeme

Der Einsatz von Sicherheitssoftware erfordert je nach Produkt Kenntnisse hinsichtlich Installation und Konfiguration, wie sie vergleichbar auch für Anwendungsprogramme erforderlich sind. Die Frage der Betreuung stellt sich daher allgemein für die eingesetzten Systeme und ist im Einzelfall unterschiedlich geregelt. Hinsichtlich Fragen der Datensicherheit ergeben sich unseres Erachtens verschiedene Möglichkeiten. Zum einen ist als zentrale betreuende Stelle für den COSIS-Einsatz die „Informationsstelle Schule und Computer" vorgesehen, so daß, ggf. als Alternative einer Betreuung durch die IT-Gruppen der Bezirksregierungen als zuständige Schulaufsichtsbehörden, hier Ansprechpartner eingerichtet werden könnten. Zum andern ist bei der Schulträgerschaft durch die jeweilige Kreisverwaltung in vielen Fällen bereits hier entsprechender Sachverstand vorhanden.

c) Verhalten bei Wartung und Reparatur

Die bei Wartung und Reparatur bestehenden datenschutzrechtlichen Risiken lassen sich über entsprechende organisatorische Maßnahmen (Beaufsichtigung des Wartungspersonals, Regelung zur Nutzung von Diagnosedisketten etc.) im allgemeinen abdecken. Soweit eine Reparatur vor Ort nicht möglich ist, ist vor der Herausgabe der Geräte die physikalische Löschung der gespeicherten personenbezogenen Daten, die Quittierung des Verbleibs der Geräte sowie die Verpflichtung des Wartungspersonals auf Einhaltung der datenschutzrechtlichen Bestimmungen erforderlich. Problematisch ist die Löschung in den Fällen, in welchen aufgrund des Defekts ein Zugriff auf die Datenbestände nicht mehr möglich ist; die technisch dann noch bestehenden Möglichkeiten der Löschung bedingen zum Teil erheblichen Aufwand.

Um die Gefahr einer unbefugten Kenntnisnahme möglichst auszuschließen, kommt daher als Alternative die grundsätzliche Verschlüsselung der Datenträger in Betracht. Die mittlerweile verfügbaren Sicherheitsprodukte (vgl. oben Nr. 1) unterstützen in vielen Fällen einen zum Teil benutzertransparenten, d. h. für den Anwender nicht erkennbaren verschlüsselten Betrieb. Aufgrund des im Hinblick auf Manipulationsversuche möglicherweise kreativeren Umfelds Schule ist außer für Wartungs- und Reparaturfälle die Verschlüsselung auch unter den Aspekten der Zugriffskontrolle sowie der Virenabwehr von Bedeutung. Gleiches gilt für in letzter Zeit häufiger zu verzeichnende Diebstähle von Arbeitsplatzrechnern aus Schulen.

d) Abschließend hat der LfD das Ministerium um Mitteilung gebeten, in welchem Umfang bereits jetzt gesonderte Sicherungssoftware oder sonstige vergleichbare Lösungen in den Schulen zum Einsatz kommt, und ob es hierfür Beschaffungsempfehlungen seitens der Schulaufsicht bzw. der Schulträger gibt.

Die Schaffung eines Bewußtseins für sich ergebende Abhängigkeiten beim Einsatz von IT-Systemen und die damit erforderlichen Maßnahmen des Datenschutzes und der Datensicherheit erscheint dem LfD von besonderer Bedeutung. Er hat daher gebeten, die Empfehlungen in geeigneter Weise bekanntzugeben.

8.1.2 Die Erhebung und Speicherung von Informationen über den Aufenthaltsstatus von ausländischen Schulkindern

Eine Schule und auch eine Bezirksregierung vertraten die Auffassung, es sei erforderlich, in der Schule zwischen Asylberechtigten, Asylbewerbern und abgelehnten Asylbewerbern zu unterscheiden; die Schule sei deshalb auch berechtigt, entsprechende Informationen automatisiert zu speichern.

Diese Auffassung kann der LfD auch unter Zugrundelegung der Ausführungen der Bezirksregierung nicht teilen.

Für die Schule ist allein wesentlich, ob die betroffenen Schüler schulbesuchspflichtig sind oder nicht. Nach den Ausführungen der Bezirksregierung ergibt sich danach folgende Differenzierung:

Nicht schulbesuchspflichtig sind Asylbewerber und abgelehnte Asylbewerber. Schulbesuchspflichtig sind Deutsche oder Ausländer, die ihren gewöhnlichen Aufenthaltsort im Bereich der Bundesrepublik haben, sowie Asylberechtigte.

Warum ein Ausländer sich in der Bundesrepublik aufhält, ist für die Schule unerheblich; ob dies aufgrund eines begründeten Asylantrags erfolgt oder aufgrund sonstiger Umstände (etwa wegen eines Aufenthaltsrechtes als EG-Ausländer), ist für die Schule ohne Belang.

Auch die Frage, ob ein Asylantrag eines Asylbewerbers abschlägig beschieden ist oder ob das Verfahren noch schwebt, ist für die Schule ohne Bedeutung: In beiden Fällen besteht keine Schulbesuchspflicht. Dementsprechend hat die Schule auch keine Befugnis, den Status des Kindes und seiner Eltern insoweit zu erforschen. Bedeutsam ist für die Schule nur, wenn sich der Status des Asylbewerbers insoweit ändert, als ein gewöhnlicher Aufenthalt im Bereich des Landes Rheinland-Pfalz begründet wird. Dies ist dann der Fall, wenn ein Recht zum länger dauernden Aufenthalt entsteht. In diesen Fällen genügt es aber, die Information darüber, daß der betreffende Schüler nicht schulbesuchspflichtig ist, zu löschen. Dann nämlich ist er unter dem Gesichtspunkt der Schulpflicht genauso wie alle anderen Ausländer und deutschen Kinder zu behandeln.

Gleiches gilt unter dem Aspekt der Schulstatistik: Die ursprünglich auf den entsprechenden Erhebungsbögen geforderten Eintragungen zum Aufenthaltsstatus hatten keine ausreichende gesetzliche Grundlage und sind auf dem aktuellen Formblatt nicht mehr enthalten.

Das Ministerium für Bildung und Kultur hat dieser Auffassung zugestimmt.

8.1.3 Kindesmißhandlungen außerhalb der Schule: Wen darf die Schule informieren?

Das Ministerium plant, eine Handreichung für Lehrer herauszugeben, die diesen Hilfestellung geben soll, wenn sie den Verdacht haben, daß ein Schulkind außerschulisch mißhandelt oder sexuell mißbraucht wird. Datenschutzrechtlich bedeutsam ist hier, unter welchen Voraussetzungen Lehrer entsprechende Informationen in personenbezogener Form an Stellen außerhalb der Schule übermitteln dürfen, um für die betroffenen Kinder Hilfe zu bewirken.

Im Entwurf dieses Rundschreibens werden die Lehrer aufgefordert, mit Einwilligung des betroffenen Kindes eine Beratungsstelle oder einen Fachdienst aufzusuchen, wenn der Verdacht einer Kindesmißhandlung oder eines sexuellen Mißbrauchs vorliegt. Eltern bzw. Erziehungsberechtigte dürfen dann nicht informiert werden, wenn diese in das Geschehen involviert sind. Nicht angesprochen wurde, wie in den Fällen, in denen dies nicht der Fall ist, zu verfahren ist.

Mit dem Besuch einer Beratungsstelle oder eines Fachdienstes geht regelmäßig die Offenbarung personenbezogener Informationen bezüglich des Kindes und seiner Eltern bzw. seiner Erziehungsberechtigten einher. Damit sind solche Übermittlungen nur beim Vorliegen der Voraussetzungen des § 54 a Abs. 1 oder des Abs. 2 Schulgesetz zulässig.

Im Ergebnis bedeutet dies aus der Sicht des LfD:

- Mit Einwilligung des einsichtsfähigen Kindes und mit Einwilligung der Eltern können Beratungsstellen bzw. Fachdienste informiert und mit dem Kind besucht werden, unabhängig davon, ob es sich hierbei um private oder öffentliche Stellen handelt.
- Ohne Einwilligung der Eltern dürfen aus datenschutzrechtlicher Sicht allein die Jugendämter oder die Stellen, die in deren Auftrag Aufgaben nach dem Kinder- und Jugendhilfegesetz wahrnehmen (oder die Polizei bzw. Staatsanwaltschaft) informiert werden. Eine Einschaltung anderer Stellen durch Lehrer ist datenschutzrechtlich unzulässig und hat zu unterbleiben. Auch über die Einschaltung dieser Stellen sind die Eltern bzw. Erziehungsberechtigten zumindest zu informieren, es sei denn, sie stehen selbst im Verdacht der Beteiligung an den Mißhandlungen oder am sexuellen Mißbrauch.

In diesem Sinne wird das genannte Faltblatt Klarstellungen enthalten.

8.1.4 Übermittlungen von Schulanfängerdaten an die Deutsche Verkehrswacht e.V.

Aufgrund einer Eingabe hat der LfD von folgendem Sachverhalt Kenntnis erhalten:

Die Namen und Anschriften der Schulanfänger wurden in einer Stadt durch sämtliche Grundschulen an die Deutsche Verkehrswacht e.V. übermittelt. Die Deutsche Verkehrswacht führt die Aktion „Gib acht – Schulanfänger" durch. Um diese Aktion in einem gewissen größeren Rahmen zu gestalten, nahm die Deutsche Verkehrswacht e.V. die finanzielle Unterstützung der örtlichen Sparkasse in Anspruch.

Im Verlauf der Aktion wurden alle ABC-Schützen von der Verkehrswacht e. V. persönlich schriftlich eingeladen. Sie wurden kostenlos mit Bussen von der Schule in Räume der Sparkasse gefahren. Dem Einladungsschreiben lagen ein von der Polizei ausgearbeiteter Schulwegplan sowie ein Gutschein der Sparkasse über 5,00 DM bei.

Die Übermittlung der Daten erfolgte, ohne daß die Eltern vorher über die Übermittlung und die dann folgende Verwendung dieser Daten durch die Deutsche Verkehrswacht e. V. informiert und um ihre Einwilligung gebeten wurden.

Aus datenschutzrechtlicher Sicht dürfte die hier in Rede stehende Übermittlung gem. § 54 a Abs. 2 Satz 2 Schulgesetz nur dann zulässig sein, wenn die betroffenen Eltern eingewilligt haben.

Der LfD hat die zuständige Bezirksregierung gebeten, die Grundschulen auf diese gesetzliche Regelung hinzuweisen und künftig deren Einhaltung sicherzustellen. Dem ist die Bezirksregierung gefolgt.

8.1.5 Der „gläserne Bewerber" um eine Schulleiterstelle

Gemäß § 21 Abs. 4 Schulgesetz in der Fassung vom 17. März 1992, GVBl. S. 62, ist der Schulleiter bei staatlichen Schulen im Benehmen mit dem Schulträger sowie dem Schulausschuß zu bestellen.

Fraglich ist, in welchem Umfang aufgrund dieser Regelung Informationen über den neuen Schulleiter und dessen Mitbewerber an die beteiligten Stellen (Schulträger und Schulausschuß) zu übermitteln sind.

Aus Kreisen der betroffenen Lehrer sowie der Schulträger ist die Bitte an den LfD herangetragen worden, aus datenschutzrechtlicher Sicht zu klären, welche Informationsübermittlungen in diesem Zusammenhang zulässig sind.

Das Problem hat deshalb an Relevanz gewonnen, weil im Schulausschuß neben den Lehrern auch die Schüler und Eltern paritätisch (pro Gruppe jeweils zwischen drei und neun Personen) vertreten sind (§ 38 Schulgesetz). Bei berufsbildenden Schulen kommt je ein Vertreter der Arbeitnehmer und der Arbeitgeber hinzu.

a) Umfang der zu übermittelnden Informationen

Als Rechtsgrundlage für die Übermittlungen ist § 54 a Abs. 1 Schulgesetz heranzuziehen. Danach gilt der Erforderlichkeitsgrundsatz: Daten dürfen übermittelt werden, soweit dies zur Erfüllung der dem Empfänger durch Rechtsvorschrift zugewiesenen schulbezogenen Aufgaben erforderlich ist. Die Herstellung des Benehmens bei der Bestellung des Schulleiters bedeutet, daß vor der Ernennung des Schulleiters die zu beteiligenden Stellen über die Person des zu Bestellenden informiert werden und Gelegenheit zur Erörterung sowie zur Stellungnahme haben. Im Unterschied zum Einvernehmen und zur Mitbestimmung ist keine förmliche Einflußnahme auf den Bestellungsvorgang außerhalb des Geltendmachens von Argumenten bzw. der Abgabe von Empfehlungen möglich.

Aus der Sicht des LfD folgt daraus, daß zur Herstellung des Benehmens Daten zur Qualifikation und zum beruflichen Werdegang des von der Schulbehörde vorgeschlagenen Schulleiters auch in personenbezogener Form übermittelt werden müssen. Angaben über Mitbewerber dürften allerdings nur dann erforderlich sein, wenn nähere Begründungen benötigt werden. Dann aber wäre es ausreichend, solche Informationen über die Konkurrenten in anonymisierter Form zu übermitteln. Insoweit ist die Situation grundsätzlich anders als bei der Information der Personalräte nach dem Personalvertretungsgesetz. Dort ist zur Durchführung der Mitbestimmung die Einsicht in Personalunterlagen auch von Konkurrenten erforderlich (vgl. BAG NZA 86, 335). Die Mitbestimmung ist jedoch mit dem Herstellen des Benehmens nicht vergleichbar. Die deutlich schwächere Einflußmöglichkeit der zu beteiligenden Institutionen erfordert auch eine Beschränkung des Informationsflusses. Das in diesem Zusammenhang an die Regierungspräsidenten gerichtete Rundschreiben des Ministeriums für Bildung und Kultur von 19. Dezember 1991 (Az.: 947 QA-10-Tgb.Nr. 1398) wird dem nicht in vollem Umfang gerecht.

b) Verschwiegenheitspflichten der Datenempfänger

Im Zusammenhang mit der Information des Schulausschusses ergibt sich die Frage, welchen Verschwiegenheitspflichten dessen Mitglieder unterliegen. Bei den Lehrern folgen die Verschwiegenheitspflichten aus der Beamtenstellung (§ 70 Landesbeamtengesetz, § 203 Abs. 2 Strafgesetzbuch). Bei Eltern und Schülern sowie den Arbeitnehmer- und Arbeitgebervertretern fehlt jedoch die Anknüpfung der Geheimhaltungspflichten an eine Amtsträgereigenschaft. Die Mitglieder des Schulausschusses nehmen jedoch bei einer öffentlichen Stelle Aufgaben der öffentlichen Verwaltung wahr. Deshalb sind sie gemäß § 11 Abs. 1 Nr. 2 Buchst. c StGB strafrechtlich wie Amtsträger zu behandeln, ohne daß es einer förmlichen Verpflichtung bedürfte. Fragen, die sich daran anknüpfen, daß im Schulausschuß auch minderjährige Schüler vertreten sind, sind allein über das Institut der Strafmündigkeit zu lösen. Die Mitglieder des Schulausschusses sollten darüber ausdrücklich belehrt werden.

c) Verfahrensweise bei der Empfängerstelle (Schulträger, Schulausschuß)

Bei den Empfängern personenbezogener Informationen im Zusammenhang mit der Bestellung von Schulleitern ist so zu verfahren, daß den Datenschutzbelangen auch in organisatorischer und technischer Hinsicht Rechnung getragen wird. Dazu gehört insbesondere, schriftlich niedergelegte personenbezogene Informationen den Empfängern erst während der Sitzung zur Verfügung zu stellen und die entsprechenden Unterlagen nach erfolgter Erörterung einzusammeln und zu vernichten.

8.1.6 Öffentlichkeitsarbeit im Schulbereich

Aus vielfältigen Kontakten mit Lehrern und Eltern wurde dem LfD bekannt, daß Unklarheiten darüber bestehen, welche Informationen über Schüler und Eltern durch Lehrer und Schulverwaltungen erhoben und in Akten aufgenommen bzw. in Computern gespeichert werden dürfen. Auch die Rechte der Schüler und Eltern (z. B. Recht auf Auskunft, Einsicht, Löschung) sind in diesem Zusammenhang Gegenstand von Anfragen. Ebenso erreichten ihn Anfragen von Lehrern, die die Verarbeitung ihrer eigenen Daten durch die Schulbehörden für datenschutzrechtlich zweifelhaft hielten. Aus diesen Gründen hat der LfD im Berichtszeitraum in der Schriftenreihe „Informationen zum Datenschutz" ein Heft 6 „Datenschutz in der Schule" veröffentlicht und an alle Grund- und Realschulen, Gymnasien und Berufsschulen versandt.

Der erste Teil dieses Heftes besteht aus einer Sammlung von Vorschriften, die unter datenschutzrechtlichen Gesichtspunkten Bedeutung für das Verhältnis der Schüler und Eltern zur Schule haben oder die die datenschutzrechtlichen Beziehungen zwischen Lehrern und ihrer Dienstbehörde betreffen.

Der zweite Teil enthält Auszüge aus den bisherigen Tätigkeitsberichten der DSK sowie des LfD zu den genannten Bereichen.

Aufgrund dieser Informationsbroschüre sind über 70 Anmeldungen der automatisierten Verarbeitung personenbezogener Daten an Schulen eingegangen. Aus den Anmeldungen war ersichtlich, daß diese Verfahren bereits längere Zeit im Einsatz sind und die nach § 9 LDatG vorgeschriebene Dienstanweisung über technische und organisatorische Datensicherungsmaßnahmen nicht immer erstellt wurde. Die betroffenen Schulen wurden auf diese Mängel hingewiesen. Zwischenzeitlich sind diese Beanstandungen zum Teil behoben.

Daß Aufklärungsarbeit des LfD in diesem Bereich erforderlich ist, wurde z. B. auch aus der Anfrage einer Schule deutlich, ob der LfD den Einsatz des privaten PC eines Lehrers zu dienstlichen Zwecken genehmigen könne. Die Antwort des LfD fiel negativ aus: Er habe keine Befugnis, Genehmigungen entsprechender Nutzungen von privaten Datenverarbeitungsgeräten zu dienstlichen Zwecken auszusprechen.

Diese Befugnis steht vielmehr dem Schulleiter zu. Dies ergibt sich aus § 76 Abs. 3 der Schulordnung für die öffentlichen Hauptschulen, Realschulen, Gymnasien und Kollegs in Rheinland-Pfalz. Voraussetzung einer entsprechenden Genehmigung ist, daß das Einverständnis der betroffenen Lehrer dafür vorliegt, daß das eingesetzte Datenverarbeitungsgerät unter den gleichen Bedingungen wie dienstliche Geräte kontrolliert werden kann sowie daß die Nutzer der privateigenen Datenverarbeitungsgeräte Vorkehrungen getroffen haben, um in der häuslichen Umgebung den erforderlichen organisatorischen und technischen Datenschutz zu gewährleisten. Beide Voraussetzungen sind vom Schulleiter vor Erteilung seiner Genehmigung zu prüfen.

Diese schulordnungsrechtlichen Regelungen waren der anfragenden Schulleitung offensichtlich unbekannt.

Mitarbeiter des LfD haben schließlich auch wiederholt an Besprechungen mit Mitgliedern von Lehrplankommissionen, die das Thema „Datenschutz" im Unterricht behandeln lassen wollen, teilgenommen.

8.2 Hochschulen/Fachhochschulen

8.2.1 Diplomarbeiten-Datenbank

An einer Fachhochschule wurde eine Diplomarbeiten-Datenbank entwickelt, die über Bildschirmtext bundesweit abrufbar ist. Die Datenbank, die auf einem Rechner dieser Fachhochschule geführt wird, enthält derzeit zwar in erster Linie Diplomarbeiten der Fachhochschule Rheinland – Pfalz. Es sollen jedoch künftig auch Diplomarbeiten der Hochschulen und Fachhochschulen anderer Bundesländer einbezogen werden. Ziel ist ein bundesweiter Nachweis von geplanten und tatsächlich gefertigten Diplomarbeiten.

Für die datenschutzrechtliche Beurteilung waren nach Ansicht des LfD folgende Gesichtspunkte bedeutsam:

a) Es dürfte ein Unterschied zwischen Diplomarbeiten und solchen wissenschaftlichen Arbeiten bestehen, die zur Veröffentlichung bestimmt sind, die ihrer Bestimmung nach Gegenstand einer breiten wissenschaftlichen Diskussion sein sollen. Dies ist bei Veröffentlichungen aller Art der Fall; insbesondere trifft dies auf schriftliche Promotionsarbeiten zu, bezüglich derer die Promotionsordnungen der Hochschulen regeln, daß sie in einer Vielzahl von Exemplaren abzuliefern sind, um die interessierte Öffentlichkeit auch tatsächlich informieren zu können.

Bei Diplomarbeiten dürfte die Situation jedoch anders sein. Hier handelt es sich wohl um Prüfungsleistungen, die ausschließlich für Prüfungszwecke bestimmt sind. Dementsprechend ist die Information darüber, daß ein bestimmter Student eine Prüfungsleistung in Form einer Diplomarbeit zu einem bestimmten Thema erbracht hat, grundsätzlich als personenbezogenes Datum, das nicht zur Veröffentlichung bestimmt ist, anzusehen. Es ist außerdem zu berücksichtigen, daß das Thema und insbesondere auch der Inhalt von Diplomarbeiten von Geheimhaltungsinteressen Dritter betroffen sein kann (etwa eines Unternehmens, mit dessen Unterstützung die Arbeit entstanden ist).

b) Die Weitergabe der in Rede stehenden Informationen an die Diplomarbeiten-Datenbank, zumindest aber die Speicherung in dieser Datenbank zum Zweck des Bereithaltens zum Abruf über Btx, bedarf einer bereichsspezifischen Rechtsgrundlage in den Hochschulgesetzen (ob schon eine Ergänzung der Prüfungsordnungen ausreichen würde, ist zweifelhaft); ohne eine solche Regelung ist dies nur auf der Basis der informierten Einwilligung der Betroffenen zulässig. Die allgemeinen Regelungen des nach dem Volkszählungsurteil des Bundesverfassungsgerichts noch nicht novellierten Landesdatenschutzgesetzes zur Übermittlung und Speicherung (§§ 6, 5 LDatG) können grundsätzlich im Hinblick auf die verfassungsrechtliche Lage nicht mehr als ausreichende Rechtsgrundlage für Informationseingriffe, wie sie hier vorliegen bzw. beabsichtigt sind, angesehen werden.

c) Eine schriftliche Einwilligung ist nur dann wirksam, wenn sie auf der Basis der völligen Freiwilligkeit erfolgt.

   - Dies bedeutet, daß die Studenten darauf hinzuweisen sind, daß ihnen bei Nichterteilung der Einwilligung keinerlei Nachteile entstehen.
   - Dies bedeutet auch, daß durch das Verfahren der Einholung der Einwilligung nicht der Eindruck erweckt werden darf, die Erteilung der Einwilligung sei in irgendeiner Form mit dem Prüfungsverfahren und damit auch mit der Möglichkeit des Prüfungserfolges gekoppelt. Daraus folgt, daß eine Einwilligung erst nach Abschluß des Prüfungsverfahrens gesondert eingeholt werden sollte. Daraus folgt, daß Diplomvorhaben nicht gespeichert werden können.

d) Bezüglich der Altfälle, die im Register möglicherweise ohne Einholung der Einwilligung der betroffenen Studenten gespeichert sind, sind – wenn die nachträgliche Einholung der Einwilligung aus praktischen Gründen nicht möglich sein sollte – die Namen der Verfasser der Diplomarbeit in der Datenbank zu löschen und nur die Themen sowie die Angaben über die Betreuer aufzunehmen.

e) Bezüglich der Angaben über die betreuenden Hochschullehrer ist aus der Sicht des LfD keine förmliche schriftliche Einwilligung in dem genannten Sinne erforderlich, wenn die Führung der Diplomarbeitendatenbank als Aufgabe der Hochschulen angesehen werden kann. Dann ist zur Erfüllung dieser Aufgabe die Angabe der Betreuernamen in der Datenbank erforderlich. Das informationelle Selbstbestimmungsrecht der Bediensteten, die hier als Amtsträger mit Außenwirkung tätig geworden sind, ist nicht berührt oder wird zulässigerweise eingeschränkt.

Da die hier aufgeworfenen Fragen sowohl bei einer Datenübermittlung durch Hochschulen anderer Bundesländer an die hier in Rede stehende Datenbank Bedeutung haben, solche Fragen aber auch bei der Einrichtung vergleichbarer Datenbanken in anderen Bundesländern entstehen würden, hat der LfD die anderen Datenschutzbeauftragten um die Mitteilung ihrer Auffassung hierzu gebeten. Sie haben dieser Beurteilung grundsätzlich zugestimmt.

8.2.2 Noten für Professoren?

Mehrfach wurde die Frage gestellt, ob Studenten Umfragen veranstalten dürfen, in denen sie ihre Kommilitonen nach der Lehrqualität ihrer Professoren fragen.

Bedeutsam ist in diesem Zusammenhang aus hochschulrechtlichen Gründen, ob die Befragung der Studenten durch ein Organ der verfaßten Studentenschaft erfolgt ist oder durch eine anders oder gar nicht organisierte Gruppe von Studenten.

Unabhängig von dieser Frage läßt sich hierzu allgemein folgendes ausführen:

Soweit eine Veröffentlichung nur Informationen enthält, welche die amtliche Tätigkeit von Amtsträgern gegenüber den Betroffenen dieser amtlichen Tätigkeit betreffen, ist das Grundrecht auf informationelle Selbstbestimmung dieser Amtsträger grundsätzlich nicht berührt. Der Schutzbereich dieses Grundrechts reicht bei Amtsträgern nach Auffassung des LfD jedenfalls nicht soweit, daß sie gegenüber den betroffenen Bürgern die freie Verfügung über Informationen besäßen, die ihr dienstliches Handeln betreffen. Das informationelle Selbstbestimmungsrecht steht grundsätzlich dem Bürger gegenüber dem Staat, nicht aber dem Staat und seinen Funktionsträgern gegenüber dem Bürger zu. Daraus folgt, daß der Amtsträger, der im Rahmen seiner amtlichen Tätigkeit nach außen für Dritte erkennbar handelt, den Bürgern gegenüber nicht durch ein eigenes informationelles Selbstbestimmungsrecht geschützt ist. Daraus folgt auch, daß Bürger und Behörden auch öffentlich über die amtliche Tätigkeit von Amtsträgern berichten können und – im Rahmen der allgemein dafür geltenden Gesetze, insbesondere auch der Vorschriften, die dem Ehrenschutz dienen – öffentlich ihre Ansichten äußern dürfen. Wie bereits durch den Hinweis auf den Ehren-

schutz angedeutet, hat die Beschränkung des Schutzbereichs des informationellen Selbstbestimmungsrechts in diesem Sinne keinesfalls die Folge, daß die betroffenen Amtsträger schutzlos wären. Ihr allgemeines Persönlichkeitsrecht mit den für den Ehrenschutz maßgeblichen Auswirkungen ist auch im vorstehend genannten Zusammenhang zu beachten. Sie brauchen weder Verunglimpfungen noch Verleumdungen oder falsche Tatsachenbehauptungen hinzunehmen. Rechtsgrundlagen für die Geltendmachung von Ansprüchen gegenüber den Urhebern entprechender Datenübermittlungen wären zum einen § 823 BGB (mit der Folge von Schadensersatzansprüchen), u. U. auch § 1004 BGB analog mit der Folge von Unterlassungsansprüchen gegen die Personen, die das allgemeine Persönlichkeitsrecht verletzen.

Diese Überlegungen gelten auch, wenn keine Tatsachen über das amtliche Handeln der Amtsträger, sondern Ansichten und Meinungen darüber von den Adressaten dieses Handelns in Rede stehen.

Wieder anders ist zu beurteilen, wenn die Hochschule selbst in ihrer Eigenschaft als Dienstbehörde entsprechende Datenerhebungen durchführen würde. Sie hat gegenüber ihren Bediensteten das informationelle Selbstbestimmungsrecht zu beachten. Außerdem würden in diesem Zusammenhang auch personalvertretungsrechtliche bzw. hochschulverfassungsrechtliche Mitwirkungsbefugnisse berührt sein (vgl. hierzu das Urteil des OVG Berlin vom 18. Juli 1991, JPC 3,92 S. 1493).

Der LfD hat diese Auffassung den anfragenden Stellen und Personen mitgeteilt.

8.2.3 Ärztliche Atteste als Nachweis der Prüfungsunfähigkeit

Ein Arzt fragte an, ob sein Patient – ein Student im Prüfungsverfahren – von der Universität aufgefordert werden durfte, seine krankheitsbedingte Prüfungsunfähigkeit durch die Vorlage von Attesten unter Angabe der Diagnose und der genauen Daten der Arztbesuche nachzuweisen.

Der LfD hat hierzu wie folgt Stellung genommen:

Wenn der Prüfling Prüfungsunfähigkeit geltend macht, muß er diese nachweisen. Für die Beurteilung einer Prüfungsunfähigkeit aus gesundheitlichen Gründen ist die Vorlage eines ärztlichen Attestes als erste Bedingung erforderlich. Die Bescheinigung eines Arztes über die Arbeits- oder Prüfungsunfähigkeit eines Prüflings ist als Privaturkunde im Sinne von § 416 ZPO anzusehen. Diese Regelung ist gem. § 98 VwGO auch auf das verwaltungsgerichtliche Verfahren anzuwenden und ist insoweit auch für das Verwaltungsverfahren von Bedeutung.

Nach der gesetzlichen Beweisregel des § 416 ZPO begründet ein solches ärztliches Attest vollen Beweis nur dafür, daß die in der Bescheinigung enthaltene Erklärung vom Arzt abgegeben worden ist. Für die Richtigkeit dieser Erklärung gilt demgegenüber die Regelung der freien Beweiswürdigung: Dies bedeutet, daß die Prüfungsbehörde alle für den Einzelfall bedeutsamen Umstände zu berücksichtigen und nach freier Überzeugung zu entscheiden hat, ob sie eine darin enthaltene tatsächliche Behauptung für wahr hält. Die Prüfungsbehörde kann sich zwar an den Inhalt eines solchen Attestes halten. Ist sie jedoch von der Wahrheit und Vollständigkeit nicht überzeugt, so kann und muß sie selbst weiter ermitteln.

Bei der Würdigung des Beweiswertes einer ärztlichen Bescheinigung ist zu berücksichtigen, daß Ärzte in aller Regel keine Veranlassung haben, an der Wahrheit dessen zu zweifeln, was der Prüfling vorträgt. Im Gegensatz zur Prüfungsbehörde müssen sie bei der Beurteilung nicht stets wägend prüfen, ob sie nicht Opfer einer Täuschung werden sollen, sondern sie dürfen und müssen von der Hilfsbedürftigkeit ihrer Patienten ausgehen und ihre ärztlichen Maßnahmen an den geklagten Beschwerden ausrichten.

Der Beweiswert ärztlicher Bescheinigungen läßt sich daher nur feststellen, wenn sich aus dem vorgelegten Attest mindestens Art und Umfang der vom Arzt aufgrund eigener Wahrnehmung getroffenen Tatsachenfeststellungen ergeben und nicht erkennbar ist, daß der Arzt bei seiner Beurteilung Rechtsbegriffe verkannt hat. So muß aus dem ärztlichen Attest zu ersehen sein, ob es sich beispielsweise um ein Dauerleiden handelt, das bei der Leistungsbeurteilung grundsätzlich nicht berücksichtigt werden kann, oder ob es sich um eine Erkrankung handelt, deren Folgen durch geeignete Maßnahmen in der Prüfung ausgeglichen werden können. So können auch Bescheinigungen, in denen lediglich Arbeitsunfähigkeit bescheinigt wird, nicht für die Beurteilung einer Prüfungsfähigkeit herangezogen werden, da sich die Begriffe Arbeits- und Prüfungsunfähigkeit nicht decken.

Selbst wenn man von einer engeren Auffassung ausgeht, wonach der ärztlichen Bescheinigung ein hoher Beweiswert zuzumessen ist und diese grundsätzlich auch die tatsächliche Vermutung inhaltlicher Richtigkeit für sich hätte, ist eine öffentliche Stelle, die eine ärztliche Bescheinigung im konkreten Fall nicht gegen sich gelten lassen will oder die zur Überprüfung der Richtigkeit zusätzliche Angaben zum gewöhnlichen Inhalt einer ärztlichen Bescheinigung fordert, dann hierzu berechtigt, wenn besondere Umstände vorliegen, die zu ernsthaften Zweifeln an der behaupteten Erkrankung Anlaß geben.

Selbst bei Zugrundelegung dieser Maßstäbe waren im zu beurteilenden Fall die zusätzlichen Aufklärungsmaßnahmen der Universität gerechtfertigt. Auch aus datenschutzrechtlicher Sicht verdient das Geheimhaltungsbedürfnis der betroffenen Prüflinge im Interesse einer Gleichbehandlung aller Prüflinge nicht in jedem Fall den absoluten Vorrang vor anderen Rechtsgütern. Dies ist vielmehr – nach Maßgabe der genannten Kriterien – abhängig vom jeweiligen Einzelfall.

8.3 Datenschutz in der Forschung: Der Plan für ein epidemiologisches Krebsregister

Die im 13. Tb. erwähnte Absicht, ein epidemiologisches Krebsregister für das Land zu schaffen, ist bislang nicht nennenswert vorangeschritten. Nach der Vorlage eines entsprechenden Referentenentwurfs, der ausführlich mit dem LfD erörtert wurde, sind keine Weiterentwicklungen ersichtlich.

Allerdings hat der Bund zwischenzeitlich den Entwurf eines Bundeskrebsregistergesetzes vorgelegt. Dieser lehnt sich in seinen wesentlichen Grundzügen an den rheinland-pfälzischen Diskussionsstand an.

Aus der Sicht der hier geführten Diskussionen erscheinen allerdings insbesondere folgende Regelungen in dem vorgelegten Bundesgesetzentwurf erörterungsbedürftig:

a) Unklar ist, in welchem Umfang Datenübermittlungen durch die Registerstellen an die beim Bundesgesundheitsamt eingerichtete „Dachdokumentation Krebs" erfolgen sollen. Dem Entwurfsverfasser dürfte deutlich sein, daß die sog. „epidemiologischen Daten" nach wie vor jedenfalls in Ausnahmefällen personenbeziehbare Informationen enthalten. Nur dadurch wird § 6 Abs. 2 des Entwurfs verständlich, wonach die Daten von den Registerstellen vor ihrer Übermittlung zu anonymisieren sind. Dennoch ist wohl vorgesehen, an das Bundesgesundheitsamt sämtliche epidemiologische Daten, einschließlich der für eine Reidentifizierung geeigneten Informationen, regelmäßig in vollem Umfang ohne weitergehende Anonymisierungsmaßnahmen zu übermitteln.

   Wenn dies tatsächlich gewollt ist, so ist zumindest im Bundeskrebsregistergesetz deutlicher zu regeln, unter welchen Bedingungen entsprechende Daten bei der „Dachdokumentation Krebs" genutzt werden dürfen. Hierzu enthält der Gesetzentwurf nur eine sehr marginale Regelung (§ 10), in der insbesondere keine Bestimmung enthalten ist, die der Regelung des § 6 Abs. 2 Satz 1 entspricht; dort wird die Verarbeitung durch die Registerstellen selbst konkretisiert. Es ist auch unklar, ob die Strafvorschriften auf eine zweckwidrige Nutzung beim Bundesgesundheitsamt anwendbar wären.

b) Zentral bedeutsam ist die Frage, wer für die Entwicklung und den Einsatz der Verschlüsselungsverfahren verantwortlich ist. Hier dürfte gem. § 7 Abs. 1 des Entwurfs das Bundesamt für Sicherheit in der Informationstechnik eine Schlüsselstellung haben. Es ist allerdings unklar, wer verbindlich über den Einsatz der Verfahren entscheidet und ihren Einsatz organisatorisch überwacht. Diese Aufgabe sollte im Gesetzentwurf zumindest in der Form angesprochen werden, daß dem Landesgesetzgeber eine entsprechende Regelung auferlegt wird.

c) Zur organisatorischen Zuordnung von Register- und Vertrauensstelle ist im Entwurf nichts gesagt. In Anlehnung an die Statistikregelungen sollten Abschottungsvorschriften aufgenommen werden. Es ist bei der landesrechtlichen Umsetzung darauf zu achten, daß bei der Beleihung einer privatrechtlichen Stelle mit Funktionen in diesem Zusammenhang die Aufsichtsfunktionen geregelt werden.

8.4 Das Archivgesetz in der Praxis

8.4.1 Handreichung zur kommunalen Archivpflege

Der Gemeinde- und Städtebund erstellt derzeit eine Handreichung für kommunale Archive. Der LfD hat empfohlen, die datenschutzrechtlich relevanten Aspekte hierin wie folgt thesenartig zusammenzufassen:

a) Das Landesarchivgesetz gilt für Gemeinden und öffentliche Stellen (vgl. § 1 Abs. 1 Satz 1 LArchG) unabhängig davon, ob sie Bundes- oder Landesrecht ausführen.

b) Alle Unterlagen, die zur Aufgabenerfüllung nicht mehr benötigt werden, sind dem zuständigen Landesarchiv oder kommunalen Archiv anzubieten.

c) Die Archive übernehmen Unterlagen von bleibendem Wert; die Übernahme von Unterlagen, die besonderen bundesrechtlichen oder landesrechtlichen Geheimhaltungsbestimmungen unterliegen (z. B. Sozialgeheimnis, Steuergeheimnis, Meldegeheimnis) ist nur zulässig, wenn es sich um Archivgut von herausragender Bedeutung handelt.

d) Die Entscheidung, ob die Übernahmevoraussetzungen vorliegen, treffen die Archive innerhalb von sechs Monaten nach der Anbietung.

e) Unterlagen, die nicht durch ein Archiv übernommen werden, sind unter Beachtung der gesetzlichen Bestimmungen zu löschen oder, soweit dies durch Gesetz zugelassen ist, zu sperren (beisp. § 66 SGB VIII).

f) Die Anbietungs- und Übernahmeregelungen gelten für kommunale Archive nur dann, wenn diese den archivfachlichen Anforderungen an Personal, Räumen und Einrichtungen genügen und sie hinsichtlich der Sicherung, Erhaltung und Nutzung des Archivguts die für die staatlichen Archive geltenden Grundsätze beachten (§ 2 Abs. 2 LArchG).

g) Besondere bundes- oder landesrechtliche Geheimhaltungsbestimmungen sind sind auch vom übernehmenden Archiv zu beachten (§ 9 Abs. 3 LArchG).

h) Nutzungsbedingungen:
- generell ist ein berechtigtes Interesse Voraussetzung;
- Fristen:
  bei Unterlagen ohne Bezug auf einzelne Bürger: 30 Jahre nach Entstehen der Unterlagen;
  bei Unterlagen mit Bezug auf einzelne Bürger: 30 Jahre nach Tod oder 110 Jahre nach Entstehung;
  bei Unterlagen, die besonderen Geheimhaltungsbestimmungen unterworfen sind: 80 Jahre nach Entstehung.
- Fristverkürzung möglich gem. § 3 Abs. 4 LArchG.

8.4.2 Dürfen Gerichte archivierte Akten ohne Einwilligung der Betroffenen erhalten?

Ein Rentner, der vor dem Sozialgericht klagte, beschwerte sich über folgenden Vorgang: Über ihn wird eine Gefangenenakte im Archiv aufbewahrt, die Informationen über seine Haftzeit in den Jahren 1944 und 1945 enthält.

Er hat vor dem Sozialgericht geltend gemacht, ihm sei für die genannte Haftzeit eine Quittungskarte der Landesversicherungsanstalt ausgestellt worden, die sich möglicherweise in dieser Gefangenenakte befinde. Aus diesem Grund hat das Sozialgericht das Archiv darum gebeten, in seinen Unterlagen nach einer Quittungskarte zu forschen, die die Beiträge an die Landesversicherungsanstalt betreffe. Das Sozialgericht bat weiter darum, falls das Archiv auf Unterlagen stoßen sollte, die den Hintergrund der Haft des Klägers aufhellen (Urteil u. ä.), auch diese Unterlagen zu übersenden.

Daraufhin hat das Archiv dem Sozialgericht mitgeteilt, daß die gesuchten Gefangenenakten bei ihm vorlägen: Zur Verschaffung eines vollständigen Überblicks werde der gesamte Aktenband an das Stadtarchiv übersandt, wo das Sozialgericht Einblick nehmen könne. Der Aktenband wurde dementsprechend an das Stadtarchiv versandt, das seinerseits den Band unmittelbar an das Sozialgericht weiterleitete.

Der Beschwerdeführer wandte sich zunächst dagegen, daß das Gericht Einsicht in die genannte Archivalie bekommen hat, insbesondere aber auch dagegen, daß die Mitarbeiter der beklagten Landesversicherungsanstalt entsprechende Akteneinsicht erhalten hätten. Er selbst sei demgegenüber zur Einsichtnahme auf eine Fahrt zum Archiv verwiesen worden.

Zur Frage der Zulässigkeit der Übersendung der in Rede stehenden Gefangenenakte führte das Archiv aus, der Beschwerdeführer hätte in dem fraglichen Rechtsstreit auf eine Quittungskarte der LVA verwiesen, die in der fraglichen Gefangenenakte vermutet worden sei. Da somit aus seinem Sachvortrag schlüssig hervorgegangen sei, daß die Einsicht in die Gefangenenakte ihn in die Lage versetzen würde, den Beweis zu führen, daß eine Versicherungsmeldung vorgenommen wurde, sei konkludent davon auszugehen gewesen, daß er auch in die Aktenvorlage an das Sozialgericht eingewilligt habe. Es wäre unverständlich gewesen, wenn er zu der vor dem Gericht aufgestellten Behauptung den Weg zur Nachprüfung aufgezeigt, letztlich aber die Nachprüfung verweigert hätte.

Aus datenschutzrechtlicher Sicht war die Übersendung der in Rede stehenden Archivalie an das Sozialgericht wie folgt zu beurteilen:

Im Zeitpunkt der Aktenübersendung (Juli 1990) war noch die Benutzungsordnung für die Landesarchive vom 28. März 1979 (Staatsanzeiger S. 255) in Kraft. Danach konnten Archivalien für dienstliche Zwecke der Gerichte benutzt werden (amtliche Benutzung, § 3 a). Allerdings war die Vorlage von Archivalien dann abzulehnen, wenn berechtigte Interessen Dritter zu wahren waren. Dies galt in der Regel für personenbezogene Einzelakten, die jünger als 50 Jahre waren, gerechnet vom jüngsten in der Archivalieneinheit enthaltenen Schriftstück (§ 5 Abs. 1 Nr. 3 c).

Diese Regelvermutung traf im vorliegenden Fall zu. Es war also zu prüfen, ob ausnahmsweise die berechtigten Interessen des Betroffenen einer Übersendung nicht entgegenstanden.

Dafür könnte die Konstellation sprechen, wonach die Aktenübersendung an das Sozialgericht im Interesse des Beschwerdeführers gelegen hätte.

Dies trifft jedoch nicht für die Übersendung der gesamten Archivalie an das Sozialgericht zu. Der Beschwerdeführer hatte zweifellos ein eigenes Interesse daran, daß die von ihm erwähnte Quittung von Beitragszahlungen an eine Landesversicherungsanstalt dem Sozialgericht vorgelegt wurde. Eine Übersendung der Quittung durch das Archiv an das Sozialgericht hätte also ohne Zustimmung des Betroffenen erfolgen können. Die Gesamtübersendung der in Rede stehenden Gefangenenakte ist hiervon jedoch deutlich zu unterscheiden. In dieser Gefangenenakte waren sehr viel mehr Informationen enthalten, als zum Nachweis einer erfolgten Beitragszahlung erforderlich gewesen wären. Das Archiv hätte keinesfalls davon ausgehen können, daß berechtigte Interessen des Betroffenen an einer Geheimhaltung auch gegenüber dem Sozialgericht überhaupt nicht mehr bestehen.

Auch das Schreiben des Sozialgerichts, mit dem ausdrücklich die Vorlage des Strafurteils verlangt wurde, hat für das Archiv eine entsprechende eigene Prüfung nicht entbehrlich werden lassen. Vor einer Übersendung wäre eine Rückfrage bei dem betroffenen Beschwerdeführer angemessen und erforderlich gewesen.

Der LfD hat das Archiv und den Beschwerdeführer über seine Auffassung in diesem Zusammenhang unterrichtet.

8.4.3 Veröffentlichungen aus dem Gebäudebuch bzw. der Gebäudesteuerrolle einer Gemeinde

Eine Gemeinde hat etwa im Jahr 1910 ein „Gebäudebuch" oder eine „Gebäudesteuerrolle" des Gemeindebezirks angelegt. Dieses Verzeichnis enthält neben den Hausnummern die Namen der jeweiligen Besitzer mit den zugehörenden Wohn- und Nebengebäuden; die Besitzänderungen wurden bis in die neuere Zeit erfaßt, ebenso die Um- oder Neubauten. Außerdem sind im Gebäudebuch die Gebäudeflächen, der Nutzungswert und die veranlagte Gebäudesteuer verzeichnet. Aus diesem Gebäudebuch sollte nun in einer Chronik anläßlich des 700jährigen Jubiliäums ein Auszug aufgenommen werden. Dieser Auszug sollte die Angabe der Hausnummer und der Straße, die Bezeichnung der Bebauung sowie die jeweiligen Besitzer enthalten. Ob das Verzeichnis derzeit noch im Gebrauch ist, war unklar.

Aus datenschutzrechtlicher Sicht war die Angelegenheit wie folgt zu beurteilen:

a) Wenn das Gebäudebuch nach wie vor als Grundlage der Realsteuerfestsetzung durch die Gemeinde genutzt wird, ist für Übermittlungen aus dem Gebäudebuch die Abgabenordnung (§ 30) maßgeblich, die entweder unmittelbar oder aufgrund der Verweisung in §§ 1,39 KAG anzuwenden ist. Eine Rechtsgrundlage für eine Veröffentlichung ist daraus nicht zu entnehmen. Es bliebe nur die Einwilligung der Betroffenen, soweit sie leben. Für die Verstorbenen wäre an eine Einwilligung der Erben zu denken.

b) Soweit das Gebäudebuch der Gemeinde nicht mehr genutzt wird, ist für die Frage der Veröffentlichung das Landesarchivgesetz heranzuziehen. Danach wären die Aufzeichnungen zunächst nach dem Ablauf der gewöhnlichen Aufbewahrungsfristen (in der Regel spätestens 30 Jahre nach Entstehung der Vorgänge) dem zuständigen Archiv anzubieten. Wenn das zuständige Archiv eine Übernahme ablehnt, wären die Unterlagen zu vernichten. Die im Archiv gelagerten Vorgänge, die sich auf natürliche Personen beziehen, dürfen genutzt werden, wenn 30 Jahre nach deren Tod vergangen sind. Wenn das Todesjahr dem Archiv nicht bekannt ist, sind 110 Jahre nach der Geburt des Betroffenen anzusetzen. Unterlagen, die dem Steuergeheimnis unterliegen, dürfen erst 80 Jahre nach ihrer Entstehung benutzt werden. Eine Verkürzung auf Antrag ist nur zulässig, wenn die Betroffenen eingewilligt haben (§ 3 Abs. 4 Nr. 1 und 3 Landesarchivgesetz). Auch bei einer analogen Anwendung dieser Bestimmungen auf eigentlich abzulieferndes Archivgut, das noch im Gewahrsam der ursprünglichen Behörde lagert, war also im vorliegenden Fall keine Veröffentlichung zulässig, wenn die Betroffenen nicht eingewilligt haben.

Die Gemeinde wurde entsprechend informiert.

9 Umweltschutz

9.1 EG-Umweltrecht

Richtlinien der Europäischen Gemeinschaften auf dem Gebiet des Umweltschutzes zwingen den nationalen Gesetzgeber immer wieder zu Eingriffen in bestehende Regelungssysteme. Am 7. Juni 1990 hat der Rat der Europäischen Gemeinschaften die Richtlinie 90/313/EWG über den freien Zugang zu Informationen über die Umwelt erlassen, die von den Mitgliedstaaten bis zum 31. Dezember 1992 in nationales Recht umgesetzt werden sollte. Bis zum Inkrafttreten der Einheitlichen Europäischen Akte (EEA) kamen als Rechtsgrundlage für gemeinschaftseigene Rechtsetzungen im Umweltbereich lediglich die Artikel 100 und 235 i. V. m. Artikel 2 des Vertrages zur Gründung der Europäischen Wirtschaftsgemeinschaft (EWGV) in Betracht. Danach war Umweltschutzpolitik unter Wahrung der Kompetenzgrenzen der EG nur als Annex zur Verfolgung der wirtschaftspolitischen Zwecke des EWGV statthaft, auch wenn der Europäische Gerichtshof (EuGH) im Umweltschutz ein „wesentliches Ziel der Gemeinschaft" erkannt hatte. Erst mit der Einfügung der Artikel 130 r bis t EWGV durch die EEA wurde der Umweltschutz als originäre Aufgabe und eigenständiges Vertragsziel der Gemeinschaft festgeschrieben. Der Rat der EG beschloß daher auf der Grundlage des Artikels 130 s EWGV die „Richtlinie über den freien Zugang zu Informationen über die Umwelt".

Nach ihrem Artikel 1 ist es das Ziel der Richtlinie, den freien Zugang zu den bei den Behörden vorhandenen Informationen über die Umwelt sowie die Verbreitung dieser Informationen zu gewährleisten. Die Richtlinie knüpft somit an Ziele und Bedeutung des gemeinschaftsrechtlichen Umweltschutzes im Sinne des Artikels 130 r EWGV an.

Die Richtlinie verpflichtet die Mitgliedstaaten, Zugang zu ermöglichen zu

- Zustands- und Prognosedaten über den gegenwärtigen und künftigen Zustand von Tieren, Pflanzen und der Umweltgüter Luft, Wasser, Boden, Klima, Landschaft,
- Informationen über die Auswirkungen der vorgenannten Umweltgüter auf Menschen, Kultur- und sonstige Sachgüter,

- Informationen über Tätigkeiten und Maßnahmen, welche die Umweltgüter beeinträchtigen oder die Auswirkungen auf die Umweltgüter haben,
- Informationen über Tätigkeiten oder Maßnahmen zum Schutz der Umweltgüter.

Die Informationen müssen in Schrift-, Bild-, Ton- oder DV-Form vorliegen. Das neue Recht führt mithin nicht zu einer Beschaffungspflicht für die Behörden, wenn die geforderten Informationen nicht erhoben sind.

In der Richtlinie wird eine Reihe von Ausnahmeregelungen definiert, welche die Mitgliedstaaten vorsehen können. Beispielsweise besteht nicht der Anspruch auf Zugang zu Umweltinformationen, sofern durch das Bekanntwerden der Informationen personenbezogene Daten oder Betriebs- und Geschäftsgeheimnisse offenbart werden.

Es gibt keine Beschränkungen für den Kreis der Personen, die Zugang verlangen können. Deshalb dürfen alle (nicht nur EG-Bürger) sich Informationen zur Umwelt bei einer Behörde beschaffen; mithin auch außerhalb des eigenen Landes. Praktische Bedeutung könnte dies bei grenzüberschreitenden und in Grenzgebieten liegenden Projekten erlangen, beispielsweise bei Atomkraftwerken oder Müllverbrennungsanlagen in der Nähe von Staatsgrenzen.

Es ist die Aufgabe der nationalen Gesetzgebung, die Art des Zugangs zu regeln. Zu dem Entwurf des Bundesministers für Umwelt, Naturschutz und Reaktorsicherheit für ein Umweltinformationsgesetz (UIG-E) hat der LfD gegenüber dem rheinland-pfälzischen Ministerium für Umwelt Stellung genommen.

Gemäß § 1 des Entwurfs vom 8. März 1993 soll es Zweck des geplanten Gesetzes sein, für jeden „den freien Zugang" zu Umweltinformationen zu gewährleisten. Der Richtlinientext spricht in Artikel 3 Abs. 1 Satz 1 indes davon, daß die Mitgliedstaaten ihre Behörden zu verpflichten haben, natürlichen oder juristischen Personen auf Antrag „ohne Nachweis eines Interesses" Informationen über die Umwelt zur Verfügung zu stellen. Der LfD hat empfohlen, diesen Zusatz an geeigneter Stelle in § 1 zu übernehmen und auf diese Weise zu verdeutlichen, daß vom Verwaltungsverfahrensgesetz (VwVfG) abweichende verwaltungsverfahrensrechtliche Bestimmungen der Richtlinie als inhaltsgleiche oder entgegenstehende Bestimmungen i. S. v. § 1 VwVfG dem Akteneinsichtsrecht nach § 29 VwVfG vorgehen. Es besteht nämlich ein Zugangsanspruch. Angemerkt sei in diesem Zusammenhang, daß auch nach dem Text des Entwurfes der Zugang ohnehin nicht „frei" ist, da ein zu bescheidender Antrag gestellt werden muß.

Aus der Sicht des Datenschutzes geht es um die Sicherung des Rechts auf informationelle Selbstbestimmung. Umweltbezogene Informationen können sensible personenbezogene Daten enthalten. Das Bundesverfassungsgericht hat in seiner grundlegenden Entscheidung zum Grundrecht auf informationelle Selbstbestimmung aus dem mit Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG gewährleisteten Recht die Befugnis des einzelnen abgeleitet, über die Preisgabe und Verwendung seiner persönlichen Daten grundsätzlich selbst zu bestimmen. Eine Beschränkung dieses informationellen Selbstbestimmungsrechts ist nur bei überwiegendem Allgemeininteresse zulässig und bedarf einer verfassungsmäßigen gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht. Einschränkungen des Rechts auf informationelle Selbstbestimmung sind zulässig, weil das Recht im Hinblick auf die Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person nicht schrankenlos gewährleistet ist. Dem Gemeinschaftsinteresse kann deswegen unter bestimmten Voraussetzungen Vorrang vor dem Einzelinteresse eingeräumt werden, wobei im vorliegenden Fall der Schutz der natürlichen Lebensgrundlagen der Anknüpfungspunkt für die Abwägung sein sollte. In diesem Zusammenhang ist mit § 8 des Entwurfs eine in der Praxis wohl schwer zu handhabende Regelung vorgeschlagen worden. Der Zugangsanspruch wird im Grundsatz ausgeschlossen, soweit durch das Bekanntwerden der Informationen personenbezogene Daten oder Betriebs- oder Geschäftsgeheimnisse offenbart werden. Die Frage, ob personenbezogene Umweltdaten offenbart werden dürfen, würde sich – abgesehen von speziellen Regelungen im Abfallwirtschafts- und Altlastengesetz – wie bisher nach den Regelungen des LDatG richten. Der anfragende Bürger müßte also weiterhin ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft machen. Ein Umweltinformationsgesetz sollte deshalb den Bereich der personenbezogenen Umweltdaten in angemessener Weise regeln, indem es, der Intention der Richtlinie entsprechend, auch bei personenbezogenen Umweltdaten einen grundsätzlichen Zugangsanspruch unabhängig vom Nachweis eines Interesses gewährt. Das Zugangsrecht ist durch die schutzwürdigen Belange der Betroffenen begrenzt. Darüber, wann dies anzunehmen ist, sollte der Gesetzgeber genaue Vorgaben machen, indem er Regelbeispiele nennt. So könnte als Regelbeispiel für die Verletzung schutzwürdiger Belange die Offenbarung von Daten über Rechtsverhältnisse, insbesondere Rechte an Grundstücken, genannt werden.

Gemäß § 7 Abs. 4 UIG-E dürfen Informationen über die Umwelt, die ein privater Dritter der Behörde ohne rechtliche Verpflichtung übermittelt hat, nur mit Zustimmung des Dritten zugänglich gemacht werden. Wünschenswert wäre hier jedoch eine Klarstellung dahin gehend, daß die Begriffe „Betroffener" und „Dritter" identisch sind. Dies kommt aufgrund der Formulierung in § 8 Abs. 3 Satz 1 und Satz 2 des UIG-E zum Ausdruck. So sind nach Satz 1 die Betroffenen anzuhören. Nach Satz 2 hat die Behörde in der Regel von der Betroffenheit eines Dritten unter bestimmten Voraussetzungen auszugehen. Also kann ein

Dritter Betroffener und auch ein Betroffener Dritter sein. Im Richtlinientext ist übrigens an keiner Stelle von dem „Betroffenen" die Rede; lediglich einmal von dem „Dritten" in Artikel 3 Abs. 2, 6. Spiegelstrich. Die sprachliche Unterscheidung zwischen „Dritten" und „Betroffenen" in der deutschen Übersetzung ist problematisch. Es ist zu fordern, daß durch Verwendung eines einheitlichen Begriffs Klarheit geschaffen wird.

Es ist nicht gelungen, die Richtlinie zeitgerecht bis zum 31. Dezember 1992 umzusetzen. Der EuGH vertritt jedoch in ständiger Rechtsprechung die Auffassung, daß EG-Richtlinien nach Ablauf der Umsetzungsfrist unter bestimmten Voraussetzungen von den Behörden und Gerichten der Mitgliedstaaten ganz oder in Teilen unmittelbar anzuwenden sind.

Die unmittelbare Anwendung einer Richtlinie setzt nach der Rechtsprechung des EuGH voraus, daß sich ihre Regelungen als „inhaltlich unbedingt" und „hinreichend genau" darstellen und damit ohne weitere Zwischenakte des nationalen Gesetzgebers oder eines Gemeinschaftsorgans anwendungsfähig sind (vgl. etwa EuGH, Sammlung 1982, 53 [71]; EuGH, Sammlung 1989, 1925 [1955]; ebenso BVerfGE 75, 223; sowie die herrschende Rechtslehre, vgl. statt aller: Pescatore, Recueil Dalloz 1980, S. 171 ff.) und daß gleichzeitig keine Rechte Dritter beeinträchtigt werden (EuGH, Sammlung 1990, 495).

Vorliegend könnte die inhaltliche Unbedingtheit fraglich sein, für die der EuGH voraussetzt, daß die Richtlinie „ihrem Wesen nach keiner weiteren Maßnahme der Gemeinschaftsorgane oder der Mitgliedstaaten bedarf". Die unmittelbare Anwendung kann in bestimmten Fällen nach der Rechtsprechung auch entfallen, wenn eine Richtlinie den Mitgliedstaaten im Hinblick auf das „Wie" ihrer Umsetzung einen Ermessensspielraum gewährt. In diesem Zusammenhang hat der EuGH wiederholt festgestellt, daß eine Ermessensnorm unmittelbar anwendungsfähig bleibt, soweit sie dem Mitgliedstaat bei der Umsetzung hinreichend genaue Grenzen setzt.

Die Ausgestaltung des Zugangsrechts ist in der vorliegenden Richtlinie nicht abschließend geregelt. Den Mitgliedstaaten wird ein Freiraum bei der Festlegung der Modalitäten des Informationszugangs eingeräumt. Im Hinblick auf die Art des Zugangs gibt die Richtlinie jedoch einen nicht zu unterschreitenden Mindeststandard vor.

Der Rechtsprechung des EuGH liegt das Prinzip zugrunde, daß ein Mitgliedstaat, der eine EG-Richtlinie nicht fristgerecht umsetzt, aus seiner Säumnis keine Vorteile ziehen darf. Andererseits dürfen einzelne Bürger, die auf die Umsetzung keinen Einfluß haben, durch die unmittelbare Wirkung von EG-Richtlinien nicht belastet werden. Eine Richtlinie ist nur dann inhaltlich bedingt, wenn sie den Mitgliedstaaten einen Entscheidungsspielraum hinsichtlich des Setzens von Rechtsfolgen eröffnet. Besteht ein Ermessen jedoch nur in der Wahl der Mittel, ist aber das Ziel der Richtlinie hinreichend deutlich, so ist die Richtlinie hinsichtlich des Ziels unmittelbar wirksam (vgl. EuGH, Sammlung 1986, 3855 [3875]). Nach der aktuellen Rechtsprechung des EuGH (vgl. Sammlung 1991, 5357) kann sich ein Mitgliedstaat nicht auf Gestaltungsmöglichkeiten berufen, wenn aus der Richtlinie wenigstens eine Mindestverpflichtung abzuleiten ist. Auf jeden Fall ist aus der Richtlinie über den freien Zugang zu Informationen über die Umwelt die Mindestverpflichtung der Behörden abzuleiten, nach pflichtgemäßem Ermessen zu bestimmen, auf welche Weise (z. B. durch Akteneinsicht, Übermittlung von Kopien, durch schriftliche oder mündliche Auskunft) die Informationen dem Bürger im Einzelfall zugänglich gemacht werden. Nach Artikel 3 Abs. 1 Satz 2 der Richtlinie legen die Mitgliedstaaten die praktischen Regeln für das Zugänglichmachen der Informationen fest. Aufgrund der Option der Mitgliedstaaten handelt es sich um eine bedingte Regelung. Dies steht dem Anspruch auf Zugang zu Informationen über die Umwelt indes nicht entgegen, da nach der Rechtsprechung des EuGH praktische Verfahrensschwierigkeiten, die in Folge einer säumigen Umsetzung von Richtlinien entstehen, der Mitgliedstaat zu tragen hat (vgl. EuGH, Sammlung 1982, 53 [76]). Auch stellt die Option der Mitgliedstaaten, nach Artikel 3 Abs. 2 Ausschlußgründe für den Anspruch festzulegen, keine Bedingung für den Zugangsanspruch dar. Ein säumiger Mitgliedstaat kann sich nämlich der unmittelbaren Wirkung einer Richtlinie nicht allein deshalb entziehen, weil die Richtlinie Ausnahmeregelungen vorsieht (vgl. EuGH, Sammlung 1986, 3855 [3876]). Ebenso sind die Ausschlußgründe des Artikels 3 Abs. 2 unmittelbar wirksam. Denn nach der Rechtsprechung des EuGH kann der Bürger begünstigende Regelungen nur geltend machen, soweit die Rechte Dritter nicht verletzt werden. Der Schutz von personenbezogenen Daten sowie Geschäfts- und Betriebsgeheimnissen ist zwingend geboten, da eine unmittelbare Anwendung der Richtlinie, die diesen Schutz nicht gewähren würde, für die betroffenen Dritten belastende Wirkungen hätte.

Auch der Schutz Dritter, deren Rechte durch laufende Gerichts-, Ermittlungs-, Disziplinar- und Verwaltungsverfahren im Sinne von § 9 VwVfG betroffen sind, ist wichtig. Es besteht nämlich die Gefahr, daß Verfahrensbeteiligte Nachteile dadurch erleiden, daß Informationen zur Unzeit offenbart werden, die aufgrund laufender Verfahren entstanden sind. Die Konferenz der Datenschutzbeauftragten hält es für geboten, die Arbeit am Entwurf eines UIG zügig zum Abschluß zu bringen (vgl. Anlage 8).

Bis zur Umsetzung der EG-Umweltinformationsrichtlinie durch ein Umweltinformationsgesetz hat das Ministerium für Umwelt Rheinland-Pfalz Vollzugshinweise zur unmittelbaren Anwendung der Richtlinie in Form einer Verwaltungsvorschrift erlassen.

9.2 Anhörungsverfahren Müllheizkraftwerk Pirmasens

Vertreter von Bürgerinitiativen hatten gegen die geplante Müllverbrennungsanlage des Zweckverbandes Abfallbeseitigung Südwestpfalz zwischen November 1991 und Januar 1992 rund 43 000 Einwendungen der Bezirksregierung Rheinhessen-Pfalz übergeben. Im Rahmen des gesetzlich vorgeschriebenen Planfeststellungsverfahrens war ein Anhörungsverfahren durchzuführen. Die Daten einer so großen Zahl von Einwendern können nur dann zuverlässig, überschaubar und schnell genug erfaßt und bearbeitet werden, wenn ein EDV-System eingesetzt wird. Dazu ist eine Datenspeicherung naturgemäß erforderlich.

Seitens der Bezirksregierung war beabsichtigt, die Datenerfassung einem privaten Unternehmen zu übertragen, da diese Arbeiten aus personellen Gründen nicht in der Behörde zu bewältigen seien. Grundsätzlich ist eine solche Vorgehensweise nach den Bestimmungen zur Verarbeitung personenbezogener Daten im Auftrag gem. § 4 Abs. 1 LDatG zulässig. Der LfD hat die beiden von der Bezirksregierung benannten Privatfirmen unter Datenschutzaspekten überprüft.

Bei dem ersten Unternehmen bestanden aus der Sicht des technischen und organisatorischen Datenschutzes im Bereich der Zugangskontrolle (§ 9 Abs. 1 Ziff. 1 LDatG) Bedenken. Ziel der Zugangskontrolle ist es, Unbefugten den Zugang zu Datenverarbeitungsanlagen und Dateien zu verwehren, in denen personenbezogene Daten verarbeitet werden. Dies war vorliegend aufgrund der äußeren Gebäudebeschaffenheit unter besonderer Berücksichtigung der Situation während der Umbauarbeiten nicht gewährleistet.

Auch war die Beschäftigung freier Mitarbeiter als Subunternehmer problematisch, weil die Frage der Zuverlässigkeit nur sehr schwer zu beurteilen war. Bei Zuwiderhandlungen gegen datenschutzrechtliche Vorschriften stellen sich Haftungsfragen. Grundsätzlich kann bei der Erfassung und Verarbeitung sehr empfindlicher Daten – wie sie beabsichtigt war – eine Beschäftigung von Personen, die an den Auftragnehmer nicht arbeitsvertraglich gebunden sind, nicht in Betracht kommen.

Bei dem zweiten Unternehmen konnte zwar davon ausgegangen werden, daß dieses über genügend DV-Erfahrung verfügt, um den Auftrag auszuführen. Aufgrund der Größe des Unternehmens (38 Mitarbeiter, davon etwa 25 mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt) war allerdings die Bestellung eines Beauftragten für den Datenschutz nach § 36 Abs. 1 BDSG zwingend erforderlich. Es sprach indes nicht für eine besondere Aufgeschlossenheit gegenüber Datenschutzfragen, daß dieser gesetzlichen Verpflichtung nicht entsprochen wurde. Ebenso war die Tatsache zu werten, daß aus einem Einbruch keine Folgerungen für die Verbesserung des technischen und organisatorischen Datenschutzes gezogen wurden. Das Fehlen eines Alarm- bzw. Raumüberwachungssystems war bei einem DV-Unternehmen dieser Größe als Merkmal für unzureichende Datensicherheit zu werten.

Nach allem konnte auch dieses Unternehmen nicht als geeignet für die Erfassung der Einwenderdaten angesehen werden.

Daraufhin hat die Bezirksregierung die Erfassung der Einwendungen selbst übernommen.

Der LfD hat hinsichtlich der Ausgestaltung des Anhörungsverfahrens mit Schreiben vom Januar 1992 die Auffassung vertreten, daß grundsätzlich auf die Weitergabe personenbezogener Daten an den Antragsteller (Träger des Vorhabens) verzichtet werden sollte. Das entspricht der Haltung der DSK im Genehmigungsverfahren für das Kernkraftwerk Mülheim-Kärlich (vgl. 12. Tb., Tz. 8.5).

Die Grundsätze des Genehmigungsverfahrens sind in der Neunten Verordnung zur Durchführung des Bundesimmissionsschutzgesetzes (9. BImSchV) geregelt. Nach § 12 Abs. 2 Satz 1 der 9. BImSchV ist der Inhalt der Einwendungen dem Antragsteller bekanntzugeben. Nach Meinung des LfD sind Name und Anschrift von Einwendern nicht „Inhalt" der Einwendung im Sinne der genannten Vorschrift. Die Weitergabe der Namen und Anschriften von Personen, die Einwendungen erhoben haben, ist ein Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen. Dieser Eingriff bedarf einer gesetzlichen Grundlage, die dem Gebot der Normenklarheit entsprechen und den Verhältnismäßigkeitsgrundsatz beachten muß. Eine generelle Weitergabe von Namen und Anschriften der Einwender könnte nur dann auf die Vorschrift des § 12 Abs. 2 Satz 1 der 9. BImSchV gestützt werden – so der LfD in seinem Schreiben vom Januar 1992 – wenn sie für den Bürger klar und erkennbar die Zulässigkeit der Weitergabe dieser Daten vorsehen würde. Dies war indes nicht der Fall. Darüber hinaus würde eine generelle Weitergabe der Namen und Anschriften aller Einwenderinnen und Einwender auch gegen den Verhältnismäßigkeitsgrundsatz verstoßen. Dieser gebietet, die Weitergabe auf jene Fallgestaltungen zu beschränken, in denen die Kenntnis der Daten zur Erfüllung des Zwecks erforderlich ist.

Es war aber auch in diesem Zusammenhang darauf hinzuweisen, daß sich in der Praxis häufig erst aus der Anschrift Rückschlüsse auf die Lage eines Nachbargrundstücks, die mögliche Betroffenheit und damit den materiellen Gehalt der Einwendung ziehen lassen. In derartigen Fällen könnte die Übersendung einer vollständigen Ablichtung des Einwendungsschreibens notwendig sein. Bei dieser Konstellation ist es zur sachgerechten Vorbereitung des Erörterungstermins erforderlich, dem Antragsteller bekanntzugeben, wo und bei wem schädliche Auswirkungen seiner Anlage befürchtet werden. Die Bekanntgabe sollte allerdings auf solche Fälle beschränkt bleiben, in denen es nach dem Zweck der Vorschrift keinem vernünftigen Zweifel

mehr begegnet, daß der Antragsteller bereits zu diesem Zeitpunkt die Daten zu einer sachgerechten Vorbereitung des Erörterungstermins benötigt. Nur in diesen Fällen kann davon ausgegangen werden, daß die vorgesehene Bekanntgabe des „Inhalts" der Einwendungen auch die Anschrift und, soweit erforderlich, den Namen eines Einwenders umfaßt. Denn bei der Auslegung von Rechtsvorschriften ist nach der Rechtsprechung des Bundesverfassungsgerichts derjenigen Interpretation der Vorzug zu geben, die den Grundrechten, hier dem Recht auf informationelle Selbstbestimmung, zu einer größtmöglichen Wirksamkeit verhilft. Eine etwaige Verfahrensweise, wonach generell dem Antragsteller Ablichtungen der Einwendungen übersandt werden, konnte damit nicht vereinbar sein.

Es wurde auch mitunter die Auffassung vertreten, aus § 1 Landesverwaltungsverfahrensgesetz (LVwVfG) i. V. m. § 29 des Bundesverwaltungsverfahrensgesetzes (VwVfG) und aus den §§ 99 und 100 der Verwaltungsgerichtsordnung (VWGO) könne der allgemeine Rechtsgrundsatz abgeleitet werden, in einem rechtsförmlichen Verfahren hätten Beteiligte keinen Anspruch darauf, daß ihre Identität gegenüber anderen am Verfahren Beteiligten verborgen bleibt. Ein solcher allgemeiner Rechtsgrundsatz würde jedoch den Anforderungen des Volkszählungsurteils an die erforderliche gesetzliche Grundlage für einen Eingriff in das Recht auf informationelle Selbstbestimmung nicht entsprechen. Denn hier würde der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit nicht beachtet, was Eignung und Erforderlichkeit zur Erreichung des Zwecks sowie die Zumutbarkeit für den Betroffenen anbelangt. Weder die Verpflichtung, den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist (§ 29 VwVfG), noch das Recht der Beteiligten auf Einsicht in die dem Gericht vorgelegten Akten (§ 100 VwGO) ließ es gerechtfertigt erscheinen, dem Antragsteller bereits bei der Bekanntgabe des Inhalts der Einwendungen die Namen und Anschriften der Einwender von Amts wegen mitzuteilen. Nach Auffassung des LfD sollte den Einwenderinnen und Einwendern die Möglichkeit erhalten bleiben, bis zum Erörterungstermin ihre Einwendungen zurückzunehmen, ohne daß die Behörde ihre Identität gegenüber dem Antragsteller preisgibt.

Nicht zuletzt diese datenschutzrechtliche Betrachtungsweise dürfte dazu geführt haben, daß § 12 der 9. BImSchV durch den Verordnungsgeber eine entsprechende Änderung erfahren hat. Seit Mai 1992 ist die Frage der Anonymisierung gegenüber dem Antragsteller neu in § 12 Abs. 2 Satz 3 geregelt. Auf Verlangen des Einwenders soll dessen Name und Anschrift vor der Bekanntgabe unkenntlich gemacht werden, wenn diese Daten zur ordnungsgemäßen Durchführung des Genehmigungsverfahrens nicht erforderlich sind. Auf diese Möglichkeit ist in der öffentlichen Bekanntmachung hinzuweisen.

9.3 Altlastenkataster

Die Einrichtung und den Betrieb von Altlastenkatastern regelt § 27 Landesabfallwirtschafts- und Altlastengesetz (LAbfWAG). Es handelt sich um Verzeichnisse, in denen unter Einsatz der automatisierten Datenverarbeitung Informationen über Altablagerungen und Altstandorte erfaßt und verarbeitet werden. Erfaßt werden u. a. die Betreiber, die räumliche Lage einer Fläche und die gegenwärtige Nutzung. Dabei fallen personenbezogene Daten an; denn die gespeicherten Daten sind Einzelangaben über persönliche und sachliche Verhältnisse. Die Grundstücksbezogenheit führt in der Regel dazu, daß eine bestimmte oder bestimmbare natürliche Person betroffen ist. Die Daten fallen demzufolge in den Schutzbereich des Rechts auf informationelle Selbstbestimmung.

Es sind drei Fälle der Datenübermittlung vorgesehen.

9.3.1 Übermittlung an öffentliche Stellen

Die Datenweitergabe ist in Übereinstimmung mit den allgemeinen datenschutzrechtlichen Bestimmungen des LDatG zulässig, soweit dies zur Wahrnehmung der Aufgaben dieser Stellen, z. B. auf dem Gebiet der Gefahrenermittlung, Gefahrenabwehr, Überwachung oder Planung erforderlich ist.

9.3.2 Bekanntgabe gegenüber der Öffentlichkeit

Hierbei dürfen grundsätzlich keine personenbezogenen Daten zugänglich gemacht werden. Etwas anderes gilt nur dann, wenn solche Angaben offenkundig sind oder ihre Bekanntgabe zur Abwehr von Gefahren oder aus anderen überwiegenden Gründen des Gemeinwohls erforderlich ist.

9.3.3 Übermittlung an einen Dritten bei berechtigtem Interesse

Wenn der Empfänger ein berechtigtes Interesse an der Einsichtnahme hat, ist stets zu fragen, ob durch eine Datenübermittlung schutzwürdige Belange des Betroffenen tangiert werden. Um die Frage beantworten zu können, muß eine am Verhältnismäßigkeitsprinzip orientierte Abwägung stattfinden. In den meisten Fällen wird es darum gehen, den möglichen Wertverlust eines Grundstücks, der aus dem Bekanntwerden einer Eintragung resultieren kann, in Beziehung zu setzen zu dem Interesse des Dritten an der Einsichtnahme.

Es ist unschwer vorstellbar, daß Eintragungen in das Altlastenkataster mitunter existenzgefährdend sein können. Grundstückseigentümer oder Nutzungsberechtigte können daher verlangen, daß die sie betreffenden Daten im Kataster berichtigt werden, soweit deren Unrichtigkeit erwiesen ist.

9.4 Interdisziplinäre Nutzung der raum- und bodenbezogenen Basisdaten

Im Mai 1993 ist dem LfD der Entwurf eines Ministerratsbeschlusses zugegangen, wonach alle raum- und bodenbezogenen Fachdaten, die von Stellen der Landesverwaltung in bereits bestehenden oder geplanten Fachinformationssystemen gespeichert werden, durch die jeweils originär zuständige Stelle zu erfassen, zu führen und zu aktualisieren sind und in ihrer Datenstruktur, ihrem Dateninhalt sowie ihrem geometrischen Raumbezug auf eine bereichsübergreifende Verknüpfung und interdisziplinäre Auswertung ausgerichtet werden. Die auf diese Weise aufbereiteten Daten sollen dann fachübergreifend zur Verfügung gestellt werden. Die Auswertung und aktuelle, interdisziplinäre Verfügbarkeit aller entscheidungsrelevanten Daten mit Mitteln der Informations- und Kommunikationstechniken ist natürlich mit datenschutzrechtlichen Risiken behaftet.

Es ist sicherlich sinnvoll, bei der Einrichtung raumbezogener Informationssysteme die amtlichen Daten der Vermessungs- und Katasterverwaltung als Basisdaten zu verwenden. Einer gebotenen Verbesserung der Entscheidungsgrundlagen sind inkompatible Insellösungen auch nicht zuträglich.

Aus der Sicht des Datenschutzes sind allerdings bei der fachübergreifenden Datennutzung und dem Austausch personenbezogener oder personenbeziehbarer Daten insbesondere folgende Anforderungen zu beachten:

- Sicherstellung, daß die fachlich zuständige Stelle auch speichernde Stelle bleibt.
- Regelung im Hinblick auf den schreibenden Zugriff im Online-Verfahren. Für den lesenden Zugriff sind die Regelungen im Katastergesetz (KatG) i. V. m. der Durchführungsverordnung (KatGDVO) einschlägig.
- Insbesondere hinsichtlich des verändernden Zugriffs sollte sichergestellt sein, daß die eingebende Stelle feststellbar ist. Die Verantwortung als speichernde Stelle gegenüber dem Betroffenen sollte auch in einem solchen Fall die Stelle tragen, die für die Führung des Informationssystems zuständig ist.

Darauf hat der LfD das Ministerium des Innern und für Sport hingewiesen.

10 Gesundheitswesen

10.1 Transplantationsgesetz für das Land Rheinland-Pfalz

Der Sozialpolitische Ausschuß des Landtags Rheinland-Pfalz führte Anfang Juni 1993 ein Anhörverfahren zu dem im Landtag eingebrachten Entwurf eines Transplantationsgesetzes für das Land Rheinland-Pfalz (Gesetzentwurf der Fraktion der SPD – Drs. 12/2094 –) sowie dem Antrag der Fraktion der SPD – Entschließung – (Drs. 12/2095) und dem Antrag der Fraktion der CDU – Entschließung – (Drs. 12/2124) durch. Der LfD äußerte sich in diesem Anhörverfahren durch schriftliche Stellungnahme (Vorlage 12/1415) und durch Sachvortrag.

Ein Kernproblem liegt darin, daß das Transplantationsgesetz, auch soweit es Informationsvorgänge regelt, als Strafgesetz konzipiert ist, daß aber die strafbewehrten Tatbestände recht ungenau beschrieben sind. Nach dem Gesetz soll beispielsweise bestraft werden, wer Entnahmen durchführt, ohne daß die in dem Gesetz geregelten Voraussetzungen vorliegen. Zu diesen Voraussetzungen gehört die Information der nächsten Angehörigen über die Absicht der Entnahme „in geeigneter Form und mit angemessener Bedenkzeit", die Eilkompetenz, die in Verbindung mit anderen Maßnahmen u. a. die Information der Angehörigen über die beabsichtigte Entnahme substituiert, wenn ein Angehöriger oder Lebenspartner „nicht innerhalb von fünf Stunden erreichbar ist" oder die Einwilligung des Verstorbenen zu Lebzeiten in die Entnahme „schriftlich oder in anderer Form".

Der LfD hält es für äußerst problematisch, derart wenig präzise beschriebene Tatbestände mit einer Strafandrohung zu belegen. Welche andere Form als die Schriftform der Einwilligung sollte beispielsweise akzeptabel sein? Genügt die mutmaßliche Einwilligung und ist damit dem explantierenden Arzt grundsätzlich ermöglicht, sich der strafrechtlichen Verantwortung zu entziehen? Wann ist die den Angehörigen eingeräumte Bedenkzeit unangemessen und damit strafbar, und was muß unternommen werden, um den nächsten Angehörigen oder Lebenspartner innerhalb der Fünfstundenfrist zu erreichen?

Unbestreitbar fehlt es in Bereichen, die den Persönlichkeitsschutz betreffen, nicht an Beispielen für Regelungen, die ebenso oder vielleicht noch deutlicher mit dem Bestimmtheitsgebot für strafbewehrte Normen kollidieren. Dementsprechend gering ist die Zahl der Verfahren und noch weitaus geringer die Zahl der Verurteilungen. Im Ergebnis führen derartige „weiche Strafvorschriften" zu einem Bedeutungsverlust für die zu schützenden Rechtsgüter und sind deshalb abzulehnen (so im Ergebnis Lemke: Stand der Diskussion zum Entwurf eines Transplantationsgesetzes; MedR 91, S. 281 ff.)

10.2 Datenschutzfolgen der Entscheidung des Bundesverfassungsgerichts zum Schwangerschaftsabbruch

Das Urteil des Bundesverfassungsgerichts zum Schwangerschaftsabbruch vom 28. Mai 1993 – 2 BvF 2/90, 4/92, 5/92 – ist unter Datenschutzgesichtspunkten von erheblicher Bedeutung. Dies gilt insbesondere für die Beratung, die auf Wunsch der schwangeren Frau anonym durchgeführt wird. Die Anonymität darf auch nicht durch die Erteilung einer namentlichen Bescheinigung über die stattgefundene Beratung aufgehoben werden.

In einem Schreiben an das Ministerium für Arbeit, Soziales, Familie und Gesundheit wies der LfD auf die Notwendigkeit hin, den Beratungsstellen Verfahrenshinweise für die anonyme Beratung von Schwangeren mit folgenden Schwerpunkten zu geben:

- Die Schwangeren müssen in der Beratungsstelle auf die Möglichkeit der anonymen Beratung hingewiesen werden. Es liegt in der freien Entscheidung einer Schwangeren, ob sie in einem Beratungsgespräch ihren Namen nennt.
- Bescheinigungen über anonyme Beratungen sind nicht von der beratenden Person, sondern von einer anderen schweigepflichtigen Person zu erteilen. Der Name der Schwangeren darf nur auf dem Original der Bescheinigung erscheinen, das ihr ausgehändigt wird. Für die Zuordnung der Vorgänge innerhalb der Beratungsstelle sind Kennummern zu verwenden.
- In Beratungsprotokollen dürfen die Namen von Schwangeren und anderen beratenen Personen nicht erscheinen.
- Schwangere sollten wissen, daß es kaum möglich ist, die Anonymität der Beratung aufrechtzuerhalten, wenn von der gleichen Beratungsstelle Unterstützung bei der Geltendmachung von Ansprüchen, bei der Wohnungssuche, bei der Suche nach einer Betreuungsmöglichkeit für das Kind oder bei der Fortsetzung der Ausbildung erbeten wird.
- Die beratenden Personen sind auf ihre besonderen Verschwiegenheitspflichten und die Strafbarkeit von Verstößen nach § 203 StGB hinzuweisen.

Der LfD verkennt nicht die Schwierigkeiten, die einer Realisierung dieser Hinweise in sehr kleinen Beratungsstellen entgegenstehen. Dennoch müssen auch diese Beratungsstellen angemessene Vorkehrungen zum Schutze der Persönlichkeitsrechte schwangerer Frauen treffen.

Der Minister für Arbeit, Soziales, Familie und Gesundheit hat veranlaßt, daß die anerkannten Schwangerenberatungsstellen über die datenschutzrechtlichen Verfahrenshinweise informiert werden.

10.3 Gesundheitsämter

10.3.1 Datenübermittlung zur Erstellung eines werksinternen Krebsregisters

Durch Pressemeldungen wurde bekannt, daß das Gesundheitsamt sowie das Standesamt einer kreisfreien Stadt an ein Unternehmen Daten zum Zwecke der Erstellung und Fortführung eines werksinternen Krebsregisters übermittelten. Diese Datenübermittlungsvorgänge wurden vom LfD mit folgenden Ergebnissen überprüft:

Grundlage der Datenübermittlung durch das Gesundheitsamt waren die sog. Leichenschauscheine, für die das Bestattungsgesetz und eine hierzu ergangene Rechtsverordnung strenge Verwendungsbeschränkungen festlegen. Eine Weitergabe personenbezogener Informationen über die Todesursache an das Unternehmen wäre auch mit der Zustimmung von Hinterbliebenen nicht zulässig gewesen.

Die Todesursachen verstorbener Werksangehöriger wurden an das Unternehmen aber nicht in personenbezogener, sondern in einer anonymisierten Form weitergegeben. Eine zuverlässige Zuordnung von Todesursachen zu vorhandenen Personaldaten war dem Unternehmen daher nicht möglich. Es konnte lediglich erkennen, in wie vielen Fällen bestimmte Arten von Krebserkrankungen zum Tode führten.

Das praktizierte Verfahren war unter datenschutzrechtlichen Gesichtspunkten nicht zu beanstanden.

Das Standesamt der Stadt teilte dem Unternehmen auf vereinzelte Anfragen mit, ob frühere Mitarbeiter verstorben sind. Derartige Auskünfte dürfen nach den Bestimmungen des Personenstandsgesetzes erteilt werden, wenn der Anfrager ein rechtliches Interesse an der Auskunftserteilung geltend machen kann. Rechtliche Interessen bestehen beispielsweise dann, wenn die Auskunftserteilung für die Verfolgung von Rechtsansprüchen genutzt werden soll. Das Forschungsinteresse der BASF ist kein rechtliches Interesse. Die Offenbarung von Personenstandsdaten war demzufolge unzulässig. Gleichwohl sah der LfD aus folgendem Grunde von einer Beanstandung ab: Nach melderechtlichen Vorschriften hätte das Meldeamt der Stadt Ludwigshafen Auskunft über den Sterbetag und -ort nach § 34 Abs. 2 Meldegesetz dann erteilen dürfen, wenn ein berechtigtes Interesse an diesen Informationen besteht. Das Forschungsinteresse des Unternehmens stellt zwar kein rechtliches Interesse im Sinne des Personenstandsgesetzes, aber ein berechtigtes Interesse im Sinne des Melderechts dar. Demzufolge wurde die Auskunft lediglich durch das falsche Amt der Stadtverwaltung Ludwigshafen erteilt. Der LfD teilte dies der Stadtverwaltung mit der Bitte um künftige Beachtung mit.

10.3.2 Adressierung von Postsendungen durch die Gesundheitsämter

Eine Behördenbedienstete mußte sich auf Veranlassung ihrer Dienstbehörde amtsärztlich untersuchen lassen. Das Gesundheitsamt sandte das erstellte Gesundheitszeugnis „zu Händen" eines bestimmten Mitarbeiters an die Dienstbehörde mit der Folge, daß es dort in der Poststelle geöffnet und dem Adressaten auf dem üblichen Postweg zugeleitet wurde.

Im Blick auf die besondere Sensitivität personenbezogener medizinischer Daten, der auch durch besondere Bestimmungen über die Behandlung von Gesundheitszeugnissen und ärztlichen Gutachten in Personalakten Rechnung getragen ist (vgl. Nr. 3.1.1 der Verwaltungsvorschrift über die Führung der Personalakten), hielt es der LfD für angezeigt, schon bei der Übersendung derartiger Schriftstücke Vorsorge zu treffen, daß sie der zuständigen Stelle innerhalb einer Behörde direkt zugeleitet werden. Seiner Empfehlung folgend forderte das Ministerium für Arbeit, Soziales, Familie und Gesundheit die Gesundheitsämter auf, Gesundheitszeugnisse und personenbezogene amtsärztliche-gutachterliche Stellungnahmen jeder Art an personalführende Stellen nur in verschlossenen Umschlägen zu versenden, die einen deutlichen (Stempel-)Aufdruck „amtsärztliches Gutachten – nur von der Personalstelle zu öffnen" tragen. Bei der Versendung personenbezogener Daten an andere als personalführende Stellen ist auf dem Umschlag ein entsprechender, den Empfänger eindeutig benennender Vermerk aufzubringen.

10.3.3 Weitergabe von Daten aus amtsärztlicher Untersuchungstätigkeit

Das Ministerium für Umwelt und Gesundheit hat in der Verwaltungsvorschrift vom 5. Februar 1986, MinBl. 1986 S. 146, 1991 S. 458, nähere Bestimmungen über die zulässige Weitergabe von Daten aus amtsärztlicher Untersuchungstätigkeit getroffen. In Nummer 2 Satz 1 dieser Verwaltungsvorschrift heißt es wörtlich: „Die Gesundheitsämter teilen den anfordernden Stellen das Untersuchungsergebnis auf dem Formblatt ‚Gesundheitszeugnis' mit." Es besteht immer wieder Veranlassung, darauf hinzuweisen, daß nur bezüglich dieses Untersuchungsergebnisses auch ohne ausdrückliche Zustimmung des zur Untersuchung Erschienenen eine Offenbarungsbefugnis gegenüber der Dienstbehörde besteht. Wiederholt wurde in Tätigkeitsberichten bemängelt, daß die Verwaltungsvorschrift von den Gesundheitsämtern nicht genügend beachtet wird (vgl. 13. Tb., Tz. 10.1).

Ein ärztlicher Mitarbeiter aus der Gesundheitsverwaltung wies aus gegebener Veranlassung darauf hin, daß eine Divergenz zwischen dem oben zitierten Text der Verwaltungsvorschrift und dem Formulartext des Gesundheitszeugnisses (Anlage 2 zur VV) besteht. In dem Formular findet sich nämlich in dem für die Beurteilung vorgesehenen Raum folgender Klammerhinweis: „(Zusammenfassende Äußerung zu den Gutachtensfragen und zur Belastbarkeit; Wertung aller Besonderheiten, die sich aus Vorgeschichte, Untersuchung im Gesundheitsamt und ggf. ergänzenden Befunden unter Berücksichtigung etwaiger vom Auftraggeber bezeichneter Anforderungen ergeben)."

Der LfD sieht dies ebenso. Der Text des Vordruckes ist mißverständlich, denn er kann den Eindruck erwecken, daß Detailangaben, auch soweit sie über das Untersuchungsergebnis hinausgehen, ohne Zustimmung des Betroffenen offenbart werden dürften. Dies ist nicht zulässig. Es empfiehlt sich deshalb, die Hinweise in dem Vordruck zu ändern.

10.3.4 Schulgesundheitspflege – ein endloses Dilemma

Erstmals im 12. Tb. der DSK wurde über die Erfassung und Verarbeitung von medizinischen Daten aus Schulgesundheitsuntersuchen auf transportablen PC, sog. Laptops, berichtet (Tz. 9.4). Es wurde darauf hingewiesen, daß die Verwendung derartiger Geräte für die Verarbeitung personenbezogener medizinischer Daten besondere Anforderungen an die Qualität des technischen und organisatorischen Datenschutzes stellt. In Zusammenarbeit mit dem Ministerium für Umwelt und Gesundheit wurde ein detaillierter Maßnahmenkatalog erarbeitet. Im 13. Tb. (Tz. 10.4) war nachzulesen, daß örtliche Prüfungen des Verfahrens bei zwei Gesundheitsämtern zu gravierenden Feststellungen führten: Die geforderte spezielle Sicherungssoftware war nicht implementiert und die geforderte – und vom zuständigen Ministerium zugesagte – Verschlüsselung der Daten war nicht durchgeführt worden.

Im Berichtszeitraum wurde die Anwendung erneut in zwei Gesundheitsämtern überprüft, wiederum mit unerfreulichen Ergebnissen.

Im einzelnen:

- Nach der Verfahrensbeschreibung sollten die Laptops im wesentlichen nur für Zwecke der Datenerhebung und -erfassung verwendet werden. Die Verarbeitung sollte in PC erfolgen, die in den Gesundheitsämtern vorhanden sind. Die örtlichen Feststellungen ergaben, daß die Gesundheitsämter über diesen Verfahrensablauf nicht informiert waren. Dementsprechend waren Untersuchungsdaten ausschließlich auf der Festplatte der Laptops und auf Sicherungsdisketten gespeichert. Die für die Datenverarbeitung in den Gesundheitsämtern installierten PC blieben zum Teil ungenutzt, zum Teil wurden sie für die Textverarbeitung, also außerhalb ihrer eigentlichen Zweckbestimmung, verwendet.

- In Schulungen wurden den in der automatisierten Datenverarbeitung tätigen Mitarbeitern der Gesundheitsämter lediglich Grundkenntnisse zum Verfahren vermittelt. Mit der vorhandenen Datensicherungssoftware waren sie nicht vertraut; die bestehenden Möglichkeiten zur Gewährleistung des technischen und organisatorischen Datenschutzes wurden deshalb nur unzureichend genutzt. So war beispielsweise die zur Verhinderung einer unbefugten Eingabe in den Speicher unabdingbare regelmäßige Änderung des Paßworts durch die Nutzer unterblieben. Es wurde weiter festgestellt, daß von beiden Gesundheitsämtern das gleiche, allen Mitarbeitern bekannte Paßwort für alle Laptops verwendet wurde. Es handelte sich um ein sog. Trivialpaßwort, das in Kenntnis des Zwecks der Anwendung leicht auszuforschen war. Die Nichtbeachtung elementarer Anforderungen an den technischen und organisatorischen Datenschutz wurde vom LfD als Verstoß gegen § 9 Abs. 1 Nr. 3 und 10 LDatG beanstandet.

- Im Mittelpunkt der vor der Verfahrenseinführung erörterten Maßnahmen zur Verbesserung des technischen und organisatorischen Datenschutzes stand die Verschlüsselung der Daten auf den Festplatten der Laptops. Diese Maßnahme der Speicherkontrolle war in der Weise realisiert, daß die Daten nach dem Programmstart entschlüsselt und bei ordnungsmäßiger Programmbeendigung wieder verschlüsselt werden. Aufgrund der Feststellungen in den beiden Gesundheitsämtern bestanden erhebliche Zweifel, ob diese Art der Verschlüsselung als Datensicherungsmaßnahme ausreicht. Nach einem – auch vorsätzlich herbeizuführenden – Programmabbruch bzw. nach dem Abschalten des Rechners in der Verarbeitungsphase waren die Daten jedenfalls unverschlüsselt auf der Festplatte abgelegt. Da kein Bootschutz realisiert war, das System also durch Einlesen einer Betriebssystemsoftware unter Umgehung der Sicherheitssoftware SAFE-Guard über das Diskettenlaufwerk wieder gestartet werden konnte, mußte davon ausgegangen werden, daß der Zugang zu den ungeschützten Daten möglich war. Abschließende Feststellungen hierzu konnten wegen der Gefahr eines Datenverlustes durch Manipulationen der geschilderten Art nicht getroffen werden. Das Ministerium für Arbeit, Soziales, Familie und Gesundheit wurde um Klärung gebeten.

- Es wurde weiter festgestellt, daß die Daten auch bei normalem Programmablauf nicht vollständig verschlüsselt werden. Ein Test ergab, daß die auf den Sicherungsdisketten gespeicherten Daten zu einem erheblichen Teil auf dem stationären PC lesbar waren, obwohl dieser nicht mit der Entschlüsselungssoftware ausgestattet war. Zu den lesbaren Daten gehörten sowohl die Namen der untersuchten Kinder wie auch Anamnese- und Diagnoseangaben, die indessen, jedenfalls im Rahmen des Tests, nicht eindeutig zugeordnet werden konnten. Von der gegebenen Möglichkeit einer Zuordnung aufgrund der Reihenfolge gespeicherter Daten und von der Möglichkeit, den Personenbezug mit selektiven Daten herzustellen, war indessen auszugehen. Aufgrund dieser Feststellungen forderte der LfD eine vollständige Verschlüsselung der auf den Laptops gespeicherten Daten sowie einen angemessenen Bootschutz.

- Die Benutzer der Laptops wurden bei den Schulungen angehalten, beim Abschluß der Arbeit an den Geräten eine Datensicherung vorzunehmen. Diese Datensicherung umfaßt jeweils den vollständigen Datenbestand. Für den genannten Zweck standen den Gesundheitsämtern jeweils zwei Sicherungsdisketten zur Verfügung. Die Möglichkeit einer Duplizierung der Sicherungsdisketten war den Anwendern unbekannt. Aus diesem Grunde wurden die vorhandenen Sicherungsdisketten während des Laptopeinsatzes mitgeführt und nach Abschluß der Datenerfassung immer wieder verwendet. Der Zweck der Datensicherung, bei Beschädigung, Diebstahl oder Verlust des Laptops eine Wiederherstellung des Datenbestandes zu ermöglichen, konnte auf diese Weise kaum erreicht werden. Außerdem war die Gefahr eines Datenmißbrauchs bei Diebstahl oder Verlust eines Laptops signifikant erhöht. Der LfD empfahl, den Mitarbeitern durch weitere Schulungsmaßnahmen die Kenntnisse zu vermitteln, die notwendig sind, um eine wirklich zuverlässige Datensicherung nach dem Mehrgenerationenprinzip vorzunehmen.

- Die Mitarbeiter der Gesundheitsämter beklagten das Fehlen einer kompetenten Beratung in Fragen des technischen und organisatorischen Datenschutzes. Das Problem wurde dadurch verschärft, daß Basisfunktionen, wie beispielsweise das Löschen von Disketten und das Einspielen von Datenbeständen aus Sicherungsdisketten, nur von einem externen Systemverwalter wahrgenommen werden konnten. Der LfD empfahl eine sorgfältige Prüfung, ob eine externe Systembetreuung beibehalten werden kann.

- Die automatisierte Verarbeitung von Daten der Schulgesundheitsuntersuchungen hat zum Ziel, die dokumentierten Untersuchungsbefunde unter Anwendung von Verfahren und Instrumenten der Medizinischen Statistik auszuwerten, um auf diese Weise schnell zu gesicherten Erkenntnissen über die gesundheitliche Verfassung von Schülern zu gelangen. Schon aufgrund früherer Prüfungen hatte der LfD bemängelt, daß keine Auswertungsprogramme existierten, um die erfaßten Daten auch tatsächlich mit dieser Zielsetzung zu nutzen. Wesentliche Fortschritte wurden aber auch in den zurückliegenden beiden Jahren nicht erzielt: In den geprüften Gesundheitsämtern war die Existenz von Auswertungsprogrammen jedenfalls nicht bekannt. Die Mitarbeiter beklagten, daß die Datenerfassung für die Gesundheitsämter mit einem erheblichen zusätzlichen Arbeitsaufwand, jedoch keinerlei Nutzen verbunden sei. Selbst einfachste Auswertungen – etwa die Erstellung schulbezogener Listen mit den Namen von Kindern, die auf ärztliches Anraten am Schulsonderturnen teilnehmen sollten – seien im automatisierten Verfahren nicht durchzuführen. Die an das Ministerium zu übermittelnden „Angaben zu den Einschulungsuntersuchungen" wurden aus handschriftlichen Aufzeichnungen und Strichlisten gewonnen, obwohl hierfür die

automatisierte Datenverarbeitung durchaus sinnvoll hätte eingesetzt werden können. An das zuständige Ministerium wurde die Frage gerichtet, ob der mit der Datenerhebung und Verarbeitung verbundene Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen vor diesem Hintergrund als verhältnismäßig angesehen wird.

- Aufgrund von Eingaben Betroffener wurde bekannt, daß einzelne Gesundheitsämter im Rahmen der Schulgesundheitsuntersuchung Datenerfassungsblätter verwendeten, die von den für das automatisierte Verfahren entwickelten einheitlichen Erhebungsmaterialien abwichen. Außerdem wurde der Hinweis auf die Freiwilligkeit der Fragenbeantwortung unterlassen. Das Ministerium, dem dies mitgeteilt wurde, veranlaßte sofort die Änderung der Verfahrensweise.

Das Ministerium für Arbeit, Soziales, Familie und Gesundheit hat, dem Prüfbericht folgend, die Feststellungen mit den betroffenen Gesundheitsämtern und der zuständigen Bezirksregierung erörtert. Eine Überprüfung des Ergebnisberichts des Pilotprojektes durch einen unabhängigen Sachverständigen ergab, daß die Umsetzung der Pilotphase in ein flächendeckendes Projekt derzeit nicht angezeigt ist. Der Minister für Arbeit, Soziales, Familie und Gesundheit hat im übrigen veranlaßt, daß Sachverständige hinzugezogen und die oben beschriebenen Mängel abgestellt werden.

10.3.5 Offenbarung der Ergebnisse von Ermittlungen nach dem Bundesseuchengesetz

Mit der wachsenden Zahl von Salmonelleninfektionen mehrten sich bei den Gesundheitsämtern Anfragen von Erkrankten und Krankenversicherungen nach den Verursachern. Bezweckt wurde damit die Verfolgung von Schadenersatz- oder Schmerzensgeldansprüchen. Zum zulässigen Umfang von Datenübermittlungen nahm der LfD wie folgt Stellung:

Ärzte und Arztgehilfen im Gesundheitsamt unterliegen grundsätzlich der ärztlichen Schweigepflicht (so der BdJ in einer Stellungnahme vom 5. März 1982 – 4047/2-2-21 080/81). Diese umfaßt sowohl Geheimnisse, die „anvertraut" wie auch solche, die „sonst bekanntgeworden" sind (§ 203 Abs. 1 StGB). Zu den Geheimnissen im Sinne dieser Vorschrift können auch die Ergebnisse von Ermittlungen nach dem Bundesseuchengesetz gehören. Daß diese Ermittlungsergebnisse Geheimnischarakter haben, steht außer Frage: Es handelt sich um Tatsachen, die nur einem beschränkten Personenkreis bekannt sind und an deren Geheimhaltung derjenige, den sie betreffen, ein von seinem Standpunkt aus sachlich begründetes Interesse hat (Schönke/Schröder, StGB, RdNr. 5 zu § 203). Die Strafvorschrift setzt allerdings voraus, daß das Geheimnis dem Täter in seiner Eigenschaft als Angehöriger einer der in der Vorschrift genannten Berufsgruppen (konkret als Arzt oder Arztgehilfen) anvertraut oder sonst bekannt geworden ist. Insoweit ist eine erste Differenzierung vorzunehmen, denn die Ergebnisse der Ermittlungen nach dem Bundesseuchengesetz erfüllen diese Voraussetzung für die Anwendung der Strafvorschrift nur zu einem Teil. Personenbezogene medizinischer Daten (etwa Untersuchungsbefunde) sind grundsätzlich durch das Arztgeheimnis geschützt. Dieses steht der Offenbarung an Dritte entgegen. Die Auskunfts-/Einsichtsgewährung an den Betroffenen selbst ist hingegen keine „Offenbarung" im Sinne der Ärztlichen Berufsordnung oder des § 203 Abs. 1 StGB.

Demgegenüber handelt es sich bei den Ergebnissen einer Überprüfung von Speisen- oder Wasserproben auf Salmonellenbefall nicht um Informationen, die dem Arztgeheimnis unterliegen, denn sie haben keinen unmittelbaren Bezug zur Arzteigenschaft. Üblicherweise werden derartige Feststellungen nicht ausschließlich von Angehörigen einer der in § 203 Abs. 1 StGB genannten Berufsgruppen getroffen.

Es stellt sich die Anschlußfrage, ob und ggf. unter welchen Bedingungen die durch das Arztgeheimnis geschützten Informationen offenbart werden dürfen. Nach § 2 Abs. 4 der Berufsordnung für die Ärzte ist der Arzt zur Offenbarung befugt, soweit er von der Schweigepflicht entbunden worden ist oder soweit die Offenbarung zum Schutze eines höherwertigen Rechtsgutes erforderlich ist. Gesetzliche Aussage- und Anzeigepflichten bleiben unberührt. In Fällen der in Rede stehenden Art kommt nur eine gesetzliche Offenbarungsbefugnis in Betracht. Dem Bundesseuchengesetz ist eine derartige Befugnis nicht zu entnehmen.

In Ergänzung des Bundesseuchengesetzes, das spezialgesetzlich Materien der Gefahrenabwehr regelt (Drews/Wacke/Vogel/Martens, Gefahrenabwehr, 9. Aufl. 1986, S. 154 ff.), können indessen die Grundsätze des allgemeinen Polizei- und Ordnungsrechts sowie das allgemeine Verwaltungsrecht herangezogen werden.

Für eine Anwendung kommt § 29 VwVfG in Betracht, der die Behörden verpflichtet, den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Zu berücksichtigen ist freilich der Ausnahmenkatalog des Absatzes 2. Hinsichtlich solcher Daten, die durch das Arztgeheimnis geschützt sind, besteht danach keine Einsichtsbefugnis, weil diese Daten ihrem Wesen nach geheimzuhalten sind und keine eindeutig überwiegenden Interessen der einsichtbegehrenden Betroffenen ersichtlich sind. Ob die Akteneinsicht schon deshalb nicht in Betracht kommt, weil die Daten „nach einem Gesetz" geheimzuhalten sind, kann demnach dahingestellt bleiben.

Dieses Ergebnis wird auch bei einer analogen Anwendung des § 7 Abs. 6 i. V. m. § 6 Abs. 3 LDatG bestätigt.

Daten, die nicht dem Arztgeheimnis unterliegen, stehen unter dem strafrechtlichen Schutz des § 203 Abs. 2 StGB. Ein Geheimhaltungsanspruch der am Verwaltungsverfahren Beteiligten ergibt sich ferner aus § 30 VwVfG. Beide Vorschriften fordern – wie auch bezüglich der dem Arztgeheimnis unterliegenden Daten – eine Offenbarungsbefugnis.

Eine Offenbarung auf der Grundlage polizeirechtlicher Vorschriften kommt nicht in Betracht. Die Anwendung der Vorschrift über die Akteneinsicht durch Beteiligte im Verwaltungsverfahren (§ 29 VwVfG) führt indessen zu einem anderen Ergebnis: Sofern Betroffene Beteiligteneigenschaft im Sinne des § 13 VwVfG haben, ist ihnen Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist.

Außerhalb eines Verwaltungsverfahrens kann eine Übermittlung von Daten, die nicht dem Arztgeheimnis unterliegen, in analoger Anwendung von § 7 Abs. 2 LDatG in Erwägung gezogen werden. Wenn der Gesetzgeber zugelassen hat, daß in Dateien gespeicherte Daten übermittelt werden dürfen, wenn das berechtigte Interesse an der Kenntnis der Daten glaubhaft gemacht und schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden, so kann davon ausgegangen werden, daß diese Abwägung eine Datenübermittlung insbesondere dann trägt, wenn Daten „nur" in Akten verarbeitet werden und damit aus der Sicht des Gesetzgebers ein geringeres Gefährdungsrisiko besteht.

Das Interesse an – durch das Arztgeheimnis nicht geschützten – Informationen zur Durchsetzung zivilrechtlicher Ansprüche ist als rechtliches Interesse besonders schutzwürdig. Eine Beeinträchtigung schutzwürdiger Belange der Betroffenen ist demgegenüber nicht erkennbar.

10.4 Krankenhäuser

10.4.1 Warndateien für „Krankenhauswanderer"

Wiederholt erhielt der LfD Hinweise, daß sich Krankenhäuser gegenseitig oder unter Einschaltung der Krankenhausgesellschaften vor Personen warnen, bei denen es nach früheren Aufenthalten Schwierigkeiten mit der Kostenabrechnung gab (sog. Krankenhauswanderer). In Rheinland-Pfalz ist das Verfahren in der Weise organisiert, daß Krankenhäuser Angaben über solche Personen an die Landeskrankenhausgesellschaft weitergeben, die dann eine Warnmeldung an andere Krankenhäuser im Verbandsbereich übermittelt.

Die Krankenhausgesellschaft Rheinland-Pfalz e. V. wies darauf hin, daß ein erhebliches rechtliches Interesse an der Beibehaltung dieses Verfahrens besteht, denn Krankenhäuser könnten nur auf diese Art und Weise davor bewahrt werden, Krankenhausbehandlung ohne entsprechende Kostenübernahme zu erbringen. Es sei zu beachten, daß Krankenhäuser in gerichtlichen Verfahren zwecks Durchsetzung von Zahlungsansprüchen gegen Krankenkassen bzw. Patienten zur Wahrung ihrer eigenen Interessen notwendigerweise personenbezogene Daten offenbaren müßten. Zur Verhinderung gerichtlicher Verfahren müsse die Offenbarung auch im Vorfeld möglich sein.

Der LfD beurteilte die rechtliche Zulässigkeit des Verfahrens wie folgt:

Das Landeskrankenhausgesetz (LKG) regelt in § 36 abschließend die Übermittlung von Patientendaten an Personen und Stellen außerhalb des Krankenhauses. Die Übermittlung von Daten zum Zwecke einer Veröffentlichung in Warndateien ist danach unzulässig, es sei denn, es läge der völlig unwahrscheinliche Fall einer Einwilligung vor. Die Übermittlung kann auch nicht auf die Bestimmung des § 36 Abs. 3 Nr. 5 LKG gestützt werden, denn sie dient nicht unmittelbar der Durchführung eines mit der Behandlung zusammenhängenden gerichtlichen Verfahrens. Der denkbare Fall, daß aufgrund der Warnhinweise ein gerichtliches Verfahren eingeleitet wird, rechtfertigt eine Offenbarung auf der Grundlage der zitierten Vorschrift jedenfalls nicht.

Im übrigen ist das Vorgehen der Krankenhäuser auch unter dem Gesichtspunkt der Verhältnismäßigkeit angreifbar. Die im Belieben eines Krankenhauses stehende, an keinerlei besondere Zulässigkeitsvoraussetzung oder Prüfung gebundene Bekanntmachung zum Zwecke der Warnung vor sog. Krankenhauswanderern ist, gemessen an dem Zweck und der Wirkung der Bekanntmachung, nicht angemessen. Dabei ist zu berücksichtigen, daß die Zugehörigkeit von Patienten zur Gruppe der Krankenhauswanderer in keinem rechtsförmlichen Verfahren festgestellt wurde. Von Bedeutung ist auch, daß Patienten ohnehin untersucht und je nach Untersuchungsergebnis behandelt werden müssen. Eine Warnmeldung kann demnach allenfalls zu einer besonders kritischen Untersuchung führen. Von fachlicher Seite wurde bestätigt, daß ein Verzicht auf Warnmeldungen die Möglichkeit der Krankenhäuser, Kostenerstattung zu erlangen, nicht beeinträchtigt.

Im Ergebnis hält der LfD die Datenübermittlung der Krankenhäuser an die Krankenhausgesellschaften oder auch ohne deren Einschaltung untereinander für unzulässig.

10.4.2 Arztbriefschreibung durch externe Schreibbüros

Die Inhaberin eines Schreibbüros fragte an, ob Krankenhausärzte befugt seien, externe Schreibbüros für die Arztbriefschreibung und andere Schreibarbeiten (z. B. Berichte, Gutachten) in Anspruch zu nehmen. Für seinen Zuständigkeitsbereich – Krankenhäuser in öffentlicher Trägerschaft – äußerte sich der LfD wie folgt:

Krankenhausärzte haben bei der Inanspruchnahme der Leistungen eines externen Schreibbüros die Datenschutzbestimmungen des Landeskrankenhausgesetzes (LKG) zu beachten. § 36 Abs. 9 dieses Gesetzes läßt zu, daß sich das Krankenhaus zur Verarbeitung von Patientendaten – hierzu zählt das Schreiben von Berichten, Gutachten und Arztbriefen – anderer Personen oder Stellen bedienen kann, wenn die Einhaltung der übrigen Datenschutzbestimmungen des Landeskrankenhausgesetzes sowie eine § 203 Strafgesetzbuch (StGB) entsprechende Schweigepflicht beim Auftragnehmer sichergestellt ist. § 203 StGB steht indessen einer Auftragsdatenverarbeitung durch externe Schreibbüros für Krankenhäuser entgegen, denn die Inhaber und Mitarbeiter von Schreibbüros sind nicht unmittelbar Angehörige einer der in § 203 Abs. 1 StGB genannten Berufsgruppen und haben, weil keine direkte Weisungsgebundenheit besteht, auch nicht den rechtlichen Status von Berufsgehilfen im Sinne des § 203 Abs. 3 StGB. Auch eine Anwendung von § 203 Abs. 2 i.V.m. § 11 StGB oder die Anwendung dieser Vorschriften aufgrund einer Verpflichtung nach dem Verpflichtungsgesetz kommt nicht in Betracht. Demzufolge ist eine Offenbarung von Patientendaten durch ein Krankenhaus an externe Schreibbüros zum Zwecke der Arztbriefschreibung usw. nur mit Zustimmung des Patienten zulässig.

10.5 Datenübermittlung durch Standesorganisationen für Werbezwecke

Ein Arzt beschwerte sich beim LfD über seine Standesorganisation. Diese hatte ohne sein Einverständnis die Praxiseröffnung einer privaten Versicherung mitgeteilt, die versuchte, ihn für den Beitritt zu einer bestehenden Gruppenversicherung zu gewinnen.

Nach Hinweis auf die fehlende Rechtsgrundlage für die Datenübermittlung wurde das Verfahren geändert. Daten werden nur noch mit Zustimmung der Betroffenen weitergegeben.

11 Sozialdatenschutz

11.1 Neuregelung des Sozialdatenschutzes

Die am 1. Januar 1981 in Kraft getretenen Vorschriften über den Sozialdatenschutz – § 35 SGB I und das Zweite Kapitel SGB X – gehören zu den wichtigsten gesetzgeberischen Leistungen im bereichsspezifischen Datenschutz. Sie weisen, wie das Bundesverfassungsgericht im Volkszählungsurteil festgestellt hat, „in die verfassungsrechtlich gebotene Richtung" (BVerfGE 65, 1, 45).

Zugleich machte das Volkszählungsurteil aber auch deutlich, daß der Sozialdatenschutz, wie auch der Datenschutz in anderen Bereichen, einer Weiterentwicklung unter Berücksichtigung der vom Bundesverfassungsgericht formulierten Grundsätze für Eingriffe in das informationelle Selbstbestimmungsrecht bedarf. Diese Weiterentwicklung hat zu berücksichtigen, daß auch im Sozialleistungsbereich die gesetzliche Regelung aller Phasen der Datenverarbeitung als Informationseingriffe verfassungsrechtlich geboten ist.

Ein erheblicher Novellierungsdruck geht aber auch von der Neufassung des Bundesdatenschutzgesetzes aus. Zum einen sind durch die Änderung der Paragraphenfolge dieses Gesetzes alle Verweisungen im Sozialgesetzbuch unrichtig geworden, zum anderen beziehen sich die §§ 79 ff. SGB X auf einen formalen Anwendungsbereich des BDSG – Dateiverarbeitung –, der durch die Neufassung im Rahmen des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20. Dezember 1990 (BGBl. I S. 2954) obsolet geworden ist.

Dementsprechend hat die Bundesregierung am 18. Juni 1993 den Entwurf eines Gesetzes zur Änderung von Vorschriften des Sozialgesetzbuchs über den Schutz der Sozialdaten sowie zur Änderung anderer Vorschriften – 2. SGBÄndG – (Drs. 12/5187) eingebracht. Dem Bundesbeauftragten für den Datenschutz wie auch den Landesbeauftragten wurde in der Vorbereitungsphase dieses Gesetzentwurfs Gelegenheit zur Stellungnahme gegeben. Die Empfehlungen wurden teilweise berücksichtigt; in mehreren Punkten weist der Entwurf, der sich gegenwärtig in den Ausschußberatungen befindet, aber noch immer Mängel auf:

- Der Entwurf sieht vor, daß die Landesbeauftragten für den Datenschutz bei der Prüfung landesunmittelbarer Sozialleistungsträger nicht die Befugnisse nach dem jeweiligen Landesdatenschutzgesetz wahrnehmen, sondern das BDSG anwenden. Im Interesse einer einheitlichen und wirksamen Kontrolle des Sozialdatenschutzes ist es erforderlich, den Datenschutzbeauftragten der Länder gegenüber den ihrer Kontrolle unterliegenden Sozialleistungsträgern die gleichen Befugnisse einzuräumen wie gegenüber den sonstigen Landes- und Kommunalbehörden.
- Die Voraussetzungen, unter denen Daten auch ohne Mitwirkung der Betroffenen erhoben werden dürfen, werden ohne überzeugenden Grund erheblich weiter gefaßt als der Katalog des § 13 Abs. 2 BDSG oder entsprechende Datenerhebungskataloge in anderen Datenschutzgesetzen.
- Die umstrittene Legitimation von Informationseingriffen – Offenbarungen – auf der Grundlage von Aufgabenzuweisen wird nach dem Entwurf beibehalten.

– Der Forderung des Bundesbeauftragten wie auch der meisten Landesbeauftragten, die Einrichtung automatisierter Abrufverfahren für Sozialdaten nur aufgrund einer Rechtsnorm zuzulassen, die zugleich die erforderlichen Schutzvorschriften enthält, wurde nicht entsprochen.

11.2 Krankenkassen, Kassenärztliche Vereinigungen, Medizinischer Dienst

11.2.1 Das Gesundheitsstrukturgesetz

Mit dem am 1. Januar 1993 in Kraft getretenen Gesundheits-Strukturgesetz 1993 reagierte der Gesetzgeber auf die dramatische Kostenentwicklung in der Krankenversicherung. Das Gesetz bezweckt kurzfristige Kosteneinsparungen und langfristig wirkende Strukturveränderungen. Unter Datenschutzgesichtspunkten ist die Erweiterung der Vorschriften im SGB V über die Erfassung und Verarbeitung, insbesondere Übermittlung, von Patientendaten (§§ 284 – 305 SGB V) von besonderer Bedeutung. Die Konferenz der Datenschutzbeauftragten hat in ihrer Sitzung am 1./2. Oktober 1992 nach eingehender Beratung eine Entschließung gefaßt und darin eine Reihe von datenschutzrechtlichen Verbesserungen gefordert (Anlage 5). Die Petita wurden im Gesetzgebungsverfahren teilweise berücksichtigt. Im Ergebnis bleibt festzuhalten, daß die gesetzlichen Neuregelungen, so wirksam sie zur Verbesserung der Situation in der gesetzlichen Krankenversicherung sein mögen, auch Möglichkeiten für eine intensivere Kontrolle des ärztlichen Handelns wie auch des Leistungsverhaltens des Patienten eröffnen.

Manche Regelungen, die auf den ersten Blick einen datenschutzrechtlichen Fortschritt zu kennzeichnen scheinen, haben eine weniger erfreuliche Kehrseite. So statuiert beispielsweise § 305 SGB V in der ab 1. Januar 1996 geltenden Fassung ein umfassendes Auskunftsrecht der Versicherten. Die Krankenkassen haben ab diesem Zeitpunkt Auskünfte über die im jeweils letzten Geschäftsjahr in Anspruch genommenen Leistungen und deren Kosten zu erteilen. Um den Krankenkassen eine Auskunftserteilung zu ermöglichen, sieht die Vorschrift eine Übermittlung von Daten durch die Kassenärztlichen Vereinigungen vor. Diese Übermittlung hat so zu erfolgen, daß die Kenntnisnahme durch die Krankenkasse ausgeschlossen ist. Insoweit ist die Regelung durchaus als eine Weiterentwicklung des Datenschutzes zu werten. Schlimm wäre es indessen, wenn dieses Auskunftsrecht etwa in der Weise mißbraucht würde, daß Arbeitgeber von Stellenbewerbern die Vorlage einer „Auskunft der Krankenkasse" verlangten, wie dies vergleichbar schon in sicherheitsrelevanten Bereichen durch das Verlangen nach Vorlage einer „polizeilichen Auskunft" geschehen ist (vgl. Tz. 5.13 Buchst. i).

Die Bemühungen des LfD um Verbesserung des Datenschutzes konzentrierten sich auf Regelungen des Referentenentwurfs über die Erfassung und Übermittlung von Versichertendaten – einschließlich der Diagnose – auf maschinell verwertbaren Datenträgern. Die Erfassung und Übermittlung von Daten in dieser Form bietet die Möglichkeit, ohne großen zusätzlichen Aufwand Gesundheitsprofile der Versicherten zu erstellen, sie auf diese Weise zu überwachen und etwa bei nicht normgerechtem Verhalten einer öffentlichen Gesundheitsvorsorge zuzuführen (z. B. Ernährungsberatung für Übergewichtige, Diabetesberatung – vgl. 12. Tb., Tz. 12.2; 13. Tb. Tz. 11.1.2 –). Für derart weitgehende Eingriffe in das Recht auf informationelle Selbstbestimmung fehlt es nach Auffassung des LfD an einer verfassungsmäßigen Grundlage.

Der LfD ersuchte die Landesregierung, die geplante Gesetzesänderungen im Bundesrat abzulehnen. Auch der Bundesbeauftragte für den Datenschutz und andere Landesbeauftragte äußerten sich ablehnend.

Das Ergebnis der Bemühungen kann nicht befriedigen. Zwar dürfen nach § 295 Abs. 2 für Abrechnungszwecke durch die Kassenärztlichen Vereinigungen an die Krankenkassen auf Datenbändern oder anderen maschinell verwertbaren Datenträgern nur fallbezogene und keine versichertenbezogene Daten übermittelt werden. § 284 läßt aber – anders als die Vorschrift in ihrer früheren Fassung – die maschinenverwertbare Erfassung zu. Noch sind die Erfassungszwecke beschränkt. Wenn aber befürchtet werden muß, daß in einer weiteren Novellierung die Verwendungsbeschränkungen aufgehoben werden, dann ist – aus der Sicht der Krankenkassen – wirklich nicht mehr einzusehen, warum die Daten zur Vermeidung von Erfassungsaufwand nicht auch für andere als Abrechnungszwecke versichertenbezogen übermittelt werden sollten.

11.2.2 Die Krankenversichertenkarte

Der durch das Gesundheitsreformgesetz neu in das Recht der Gesetzlichen Krankenversicherung (SGB V) eingefügte § 291 verpflichtete die Krankenkassen, ab 1. Januar 1992 für jeden Versicherten eine Krankenversichertenkarte auszustellen. Durch eine Änderung des Gesundheitsstrukturgesetzes wurde der Termin mittlerweile auf den 1. Januar 1995 verschoben. Die Krankenversichertenkarte soll nach dem Willen des Gesetzgebers den Krankenschein nach § 15 SGB V ersetzen; sie darf nur für den Nachweis der Berechtigung zur Inanspruchnahme von Leistungen im Rahmen der kassen- oder vertragsärztlichen Versorgung sowie für die Abrechnung mit den Leistungserbringern verwendet werden und nur ganz bestimmte, in Absatz 2 der o. a. Vorschrift im einzelnen aufgezählte Identifikationsdaten enthalten.

Eine Kassenärztliche Vereinigung erbat im Herbst 1991 die Beratung des LfD zu einem Projekt, das, aufbauend auf einem in der Schweiz entwickelten System, auf eine Ausdehnung des Anwendungsbereichs der Krankenversicherungskarte zielte. Es war beabsichtigt, die Speicherfähigkeit der Karte unter Anwendung der Chiptechnik so zu erweitern, daß sie zugleich Funktionen

als Informationsträger für medizinische Daten erfüllen kann. So sollten beispielsweise Informationen über vorhandene Risikofaktoren des Karteninhabers, über Medikamentenunverträglichkeiten oder über Röntgenbelastungen vermerkt werden und dem behandelnden Arzt, der ein Lesegerät verwendet, zur Verfügung stehen. Als weitere Gründe für die Anwendung der Chiptechnik wurde deren angeblich höhere Manipulationssicherheit genannt. Außerdem biete sie die Möglichkeit, Arztbesuche zu erfassen und der Inanspruchnahme mehrerer Ärzte innerhalb eines Quartals entgegenzuwirken.

Die Erweiterung des Informationsteils und die Funktionserweiterung der Karte sollte, weil sie von § 291 SGB V nicht gedeckt ist, nur in solchen Fällen erfolgen, in denen die Versicherten ihr Einverständnis erklären.

In seiner Stellungnahme zu dem Projekt bezeichnete es der LfD als ein datenschutzrechtliches Kernproblem, daß Versicherte verpflichtet sind, eine Karte zu benutzen, auf der sich außer solchen Daten, für die eine gesetzliche Offenbarungspflicht existiert, auch solche Daten befinden, für die eine solche Eingriffsgrundlage nicht vorhanden ist (Pflichtkarte mit freiwilligen Zusatzinformationen). Er wies darauf hin, daß der Zustimmungsvorbehalt als Voraussetzung für die Verarbeitung von Patientendaten eine Fülle von Problemen birgt, die beispielsweise im Zusammenhang mit der Verabschiedung von Krankenhausgesetzen intensiv diskutiert wurden. Unter Berücksichtigung der besonderen Patientensituation wurde die Auffassung vertreten, daß die gegenüber dem Arzt erklärte Zustimmung nur selten Ausdruck einer echten Wahl- und Entscheidungsfreiheit ist. Die Patientensituation ist geeignet, an die Stelle einer informierten Einwilligung eine „Scheinfreiwilligkeit" treten zu lassen. Als Frage ausgedrückt: Kann von einer allen gesetzlichen Anforderungen genügenden Einwilligung gesprochen werden, wenn mit einer Verweigerung dieser Einwilligung eine grundlegende Störung des Vertrauensverhältnisses zwischen Arzt und Patient einhergeht?

Der LfD vertrat die Auffassung, daß die Erweiterung des Informationsteils der Krankenversichertenkarte und eine Funktionserweiterung – auch mit Zustimmung der Betroffenen – nur dann zulässig ist, wenn dies detailliert gesetzlich geregelt wird. Im übrigen wies er darauf hin, daß Gesichtspunkte des technischen und organisatorischen Datenschutzes keineswegs zur Anwendung der Chiptechnik zwingen. Ein ausreichender Datenschutz ist auch bei Verwendung der Magnetstreifenkarte oder einer Prägekarte zu gewährleisten.

Das Projekt der Einführung einer erweiterten Chipkarte wurde von der KV nicht mehr weiterverfolgt. Ob und inwieweit hierfür Datenschutzgründe bestimmend waren, ist nicht bekannt.

Unterdessen streben die Spitzenverbände der Krankenkassen und die Kassenärztlichen Bundesvereinigungen (Vertragspartner) die Einführung der Krankenversichertenkarte auf der Basis der Chipkarte, allerdings unter Beschränkung auf den Datenkatalog des § 291 SGB V, an. Vor einem flächendeckenden Einsatz werden drei Pilotprojekte durchgeführt (in Wiesbaden, Böblingen und Weimar), um die Verwendung der Karte und die damit verbundene elektronische Informationsverarbeitung im großen Stil zu erproben.

Gegenüber dem Bundesbeauftragten für den Datenschutz haben sich die Vertragspartner bereit erklärt, in der Erprobungsphase die folgenden technischen Sicherheitsstandards zu gewährleisten:

- nur die ausstellende Krankenkasse hat Schreibzugriff,
- nur vom BSI zertifizierte Lese- und Schreibgeräte dürfen verwendet werden,
- die Vertragspartner stellen sicher, daß jeder Versicherte jederzeit sowohl den Inhalt der auf der Karte gespeicherten Daten bei einem Arzt oder einem Krankenversicherungsträger als auch den unbeschriebenen Teil der Krankenversichertenkarte bei einem Krankenversicherungsträger überprüfen kann,
- die verbleibenden, nicht benötigten Speicherplätze des Kartenchips werden mit einem definierten Zeichen belegt und dürfen nicht unbefugt beschrieben werden.

Kontrollen des BfD bei Krankenkassen ergaben, daß die Vereinbarungen nur zum geringen Teil eingehalten worden sind. So bestand nur in wenigen Fällen für die Versicherten die Möglichkeit, den Inhalt der eigenen Karte zu lesen. Der Einsatz zertifizierter Geräte war die Ausnahme.

11.2.3 Der Abrechnungsschein für den ärztlichen Notfalldienst

„Zeige mir einen Vordruck und ich sage Dir, daß er falsch ist!" So oder ähnlich könnte man – aus der Sicht des Datenschutzes – das Vordruck(un)wesen kommentieren, denn nur selten halten Vordrucke und ihre Verwendung einer datenschutzrechtlichen Prüfung stand. Abgesehen davon, daß sie häufig im Umfang der Datenerhebung weit über das Ziel hinausschießen, verleiten sie – insbesondere im Sozialleistungsbereich – zur Erhebung von Daten, die zur Erfüllung der konkreten Aufgabe nicht erforderlich sind. Im folgenden Beispiel geht es um eine dritte Gruppe von Fehlern, die speziell bei der Verwendung von Verbundvordrucken auftreten.

Die von der Kassenärztlichen Bundesvereinigung und den Spitzenverbänden der Krankenkassen abgeschlossene Vordruckvereinbarung enthält als Vordruckmuster Nummer 19 einen Abrechnungsschein für den ärztlichen Notfalldienst. Dieser Vordruck wird als dreiteiliger Durchschreibesatz hergestellt. Die erste Seite erhält die Kassenärztliche Vereinigung und später die zuständige Krankenkasse, die zweite der weiterbehandelnde Arzt, die dritte verbleibt bei dem Arzt, der den Notfalldienst oder eine Urlaubs- und Krankheitsvertretung ausübte. Soweit der Vordrucksatz für die Datenübermittlung genutzt wird – erste und zweite Seite – muß nun sorgsam unterschieden werden zwischen den Daten, die die Kassenärztliche Vereinigung für Abrechnungszwecke und den Daten, die der weiterbehandelnde Arzt für die ärztliche Behandlung benötigt. Letzterer benötigt auch die unter Verwendung des Vordrucks erhobenen Befunde, die Angaben zur Therapie und Angaben zur Dauer der Arbeitsunfähigkeit. Es besteht aber keine Notwendigkeit, diese Daten auch den Kassenärztlichen Vereinigungen und den Krankenkassen zu übermitteln, denn diese sind von Gesetzes wegen gehindert, diese Daten zu erheben und zu erfassen.

Da eine kurzfristigen Änderung des Vordrucksatzes technischen Schwierigkeiten begegnete, wurde von der Kassenärztlichen Bundesvereinigung und den Spitzenverbänden der Krankenkassen vorgeschlagen, daß vorübergehend nur die Seiten zwei und drei des Vordrucksatzes vollständig und die Seite eins ohne die vorbezeichneten, nicht übermittlungsfähigen Angaben ausgefüllt werden. Der LfD hat dies akzeptiert, jedoch eine baldige Änderung des Vordrucksatzes verlangt, weil gerade in der notfalldienstlichen ärztlichen Praxis vorstellbar ist, daß aufgrund des Zeitdrucks nicht in der empfohlenen Weise verfahren wird. Damit würden Ärzte jedoch die ärztliche Schweigepflicht verletzen und sich nach § 203 Strafgesetzbuch strafbar machen.

11.2.4 Wählbarkeit zum Personalrat unter Berücksichtigung der Datenschutzbestimmung in § 284 Abs. 4 SGB V

Eine AOK erbat die Stellungnahme des LfD zu der Frage, ob Mitarbeiterinnen und Mitarbeiter, denen die Prüfung ärztlicher Behandlungsscheine obliegt – und die dadurch auch Kenntnis über die Erkrankungen von Kolleginnen und Kollegen erlangen –, unter Berücksichtigung von § 284 Abs. 4 SGB V eine Funktion im Personalrat ausüben dürfen.

§ 284 Abs. 4 SGB V bestimmt, daß Versicherungs- und Leistungsdaten der Beschäftigten einer Krankenkasse einschließlich der Daten ihrer mitversicherten Angehörigen solchen Personen, die kasseninterne Personalentscheidungen treffen oder daran mitwirken können, nicht zugänglich sein oder diesen Personen von Zugriffsberechtigten offenbart werden dürfen.

Der LfD vertrat die Auffassung, daß Mitglieder des Personalrats bei der Wahrnehmung ihrer Aufgaben nach dem Personalvertretungsgesetz an kasseninternen Personalentscheidungen im Sinne des § 284 Abs. 4 SGB V mitwirken. Demzufolge treten die Rechtsfolgen der Vorschrift ein, d. h., Versicherungs- und Leistungsdaten der Beschäftigten usw. dürfen ihnen nicht zugänglich sein oder offenbart werden. Die Wählbarkeit zum Personalrat oder die Wahrnehmung von Aufgaben im Personalrat bleibt hierdurch unberührt.

11.2.5 Übermittlung von Abrechnungsdaten durch die Kassenärztlichen Vereinigungen an die Krankenkassen

Die Kassenärztlichen Vereinigungen des Landes und verschiedene Krankenkassen-Landesverbände fragten beim LfD an, ob es zulässig sei, die von den KV in maschinenlesbarer Form erfaßten Abrechnungsunterlagen der Ärzte (Krankenscheine) in dieser Form an die Krankenkassen zur weiteren Bearbeitung (Prüfung der Leistungspflicht usw.) zu übermitteln. Dieses Verfahren sei, so wurde argumentiert, rationeller als die Weitergabe der Krankenscheine und die Übermittlung von listenmäßig zusammengefaßten Daten, wie sie herkömmlich praktiziert werde, weil es den Krankenkassen eine direkte Weiterverarbeitung ohne nochmalige Erfassung ermögliche.

Der LfD vertrat die Auffassung, daß die Bestimmungen des SGB V einer Datenübermittlung in der beabsichtigten Weise entgegenstehen. Er verwies in seiner Stellungnahme auf die Regelungssystematik des SGB V, das die Datenübermittlung unter Verwendung von Datenbändern oder anderen maschinell verwertbaren Datenträgern in einer Reihe von Vorschriften ausdrücklich anspricht. Fehlt es an Regelungen über diese Form der Datenübermittlung – wie dies im Verhältnis zwischen den KV und den Krankenkassen der Fall war –, so könne eine Übermittlung auf maschinenlesbaren Datenträgern nicht in Betracht kommen.

Sicherlich ließe eine Datenübermittlung in der angestrebten Form gewisse Rationalisierungsvorteile erwarten. Es ist aber auch zu berücksichtigen, daß die maschinenlesbare Übermittlung oder Erfassung und Speicherung versichertenbezogener Angaben über ärztliche Leistungen durch die Krankenkasse die technische Grundlage des „Patientenkontos" bilden könnte, dessen Einführung bei der Neuordnung des Rechts der gesetzlichen Krankenversicherung durch das Gesundheitsreformgesetz zwar erörtert, vom Gesetzgeber aber als ein zu weitgehender Eingriff in die Persönlichkeitsrechte der Betroffenen abgelehnt wurde.

Unterdessen erfolgte eine Klarstellung durch den Gesetzgeber im Gesundheitsstrukturgesetz, das am 1. Januar 1993 in Kraft getreten ist (vgl. Tz. 11.2.1). Die Vorschrift über die Abrechnung ärztlicher Leistungen (§ 295 SGB V) wurde in Absatz 2 wie folgt gefaßt: „Für die Abrechnung der Vergütung übermitteln die Kassenärztlichen Vereinigungen den Krankenkassen, auf Verlangen auf Datenbändern oder anderen maschinell verwertbaren Datenträgern, für jedes Quartal die für die kassen- und vertragsärztliche Versorgung erforderlichen Angaben über die abgerechneten Leistungen fallbezogen, nicht versichertenbezogen."

11.2.6 Informationsübermittlung per Telefax

Nicht gering war das Erstaunen einer Firmeninhaberin, als ihr ein Telefax zuging, das die Methadonsubstitution eines namentlich genannten Drogenabhängigen betraf. Absender war die Geschäftsstelle einer Kommission, die bei der Kassenärztlichen Vereinigung angesiedelt ist.

Die nachfolgende Übersicht über den zeitlichen Ablauf der Sachbearbeitung zeigt, welche Mühe es gelegentlich bereitet, elementare Datenschutzforderungen durchzusetzen – im konkreten Falle die, auf die Übermittlung derart empfindlicher Daten per Telefax zu verzichten –.

- 22. Mai 1992 Anfrage des LfD an die KV, ob der Sachverhalt in der Eingabe zutreffend dargestellt sei;
- 16. Juni 1992 Erinnerung an die Beantwortung;
- 22. Juni 1992 Antwort der KV: Der Sachverhalt trifft zu;
- 7. August 1992 Anfrage an die KV, ob im Blick auf die Empfindlichkeit der Informationen über Drogenabhängige und die auch bei aller Sorgfalt nicht auszuschließende Gefahr von Fehlleitungen auf die Verwendung von Telefax vollständig verzichtet werden kann;
- 3. November 1992 Erinnerung an die Beantwortung;
- 2. Dezember 1992 zweite Erinnerung an die Beantwortung unter Fristsetzung bis zum 15. Dezember 1992;
- 28. Dezember 1992 Schreiben an das Ministerium für Arbeit, Soziales, Familie und Gesundheit als Aufsichtsbehörde der KV mit der Bitte, diese zur Beantwortung bis zum 20. Januar 1993 anzuhalten;
- 21. Januar 1993 Erinnerung an das Ministerium;
- 25. Januar 1993 Eingang einer Antwort der KV;
- 8. April 1993 nach Klärung des Verfahrens bei Anwendung der NUB-Richtlinien (vgl. Tz. 11.2.7) Mitteilung des LfD an die KV, daß völliger Verzicht auf die Telefaxübermittlung derart empfindlicher Daten empfohlen wird; die künftige Verfahrensweise solle mitgeteilt werden;
- 7. Juli 1993 Erinnerung und Fristsetzung für die Beantwortung bis zum 1. August 1993;
- 26. Juli 1993 Antwort der KV: „Die Problematik der Informationsübermittlung der Methadonkommission per Telefax hat sich insoweit erledigt, als keine personenbezogenen Daten mehr per Telefax durch die Methadonkommission übermittelt werden."

Sicherlich ein erfreuliches Ergebnis! Fände sich im Datum des Antwortschreibens die Jahreszahl 1992, so wäre es in einer durchaus angemessenen Zeit erzielt worden.

11.2.7 Verwaltungsverfahren aufgrund der Richtlinien des Bundesausschusses der Ärzte und Krankenkassen über die Einführung neuer Untersuchungs- und Behandlungsmethoden (NUB-Richtlinien)

Die Bearbeitung einer Eingabe führte zu einer näheren Befassung mit dem Verwaltungsverfahren aufgrund der NUB-Richtlinien. Nach den NUB-Richtlinien kann die Entscheidung zur Substitutionsbehandlung bei folgenden Indikationen durch den Arzt unter Wahrung berufsrechtlicher Regelungen getroffen werden:

- Drogenabhängigkeit mit lebensbedrohlichem Zustand im Entzug,
- Drogenabhängigkeit bei schweren konsumierenden Erkrankungen,
- Drogenabhängigkeit bei Aids-Kranken mit fortgeschrittener manifester Erkrankung,
- Drogenabhängigkeit bei Patienten, die sich einer unbedingt notwendigen stationären Behandlung wegen einer akuten oder schweren Erkrankung unterziehen müssen und denen gegen ihren Willen nicht gleichzeitig ein Drogenentzug zuzumuten ist (Überbrückungssituation),
- Drogenabhängigkeit in der Schwangerschaft und unter der Geburt.

Bei den genannten Indikationen hat der Arzt Beginn und Beendigung der Substitutionsbehandlung unverzüglich der zuständigen KV und der zuständigen Krankenkasse anzuzeigen. Besteht Drogenabhängigkeit bei einer vergleichbar schweren Erkrankung, so darf eine Substitution nur durchgeführt werden, wenn sie von der Kommission im Einzelfall als Teil der Krankenbehandlung genehmigt wird.

Die Durchbrechung der ärztlichen Schweigepflicht im Rahmen der Informationsübermittlung an die KV ist, da keine gesetzliche Offenbarungsbefugnis besteht, nur mit Zustimmung der Patienten zulässig. Auf die NUB-Richtlinien kann eine Offenbarungsbefugnis nicht gestützt werden.

Eine nähere Überprüfung durch den LfD ergab, daß die von den KV verwendeten Einwilligungserklärungen nicht den Bestimmtheitsanforderungen genügten; denn die Betroffenen wurden über den Inhalt und Zweck der Offenbarung sowie die Adressaten von Datenübermittlungen nicht ausreichend informiert. Eine KV beispielsweise ging sogar von der Notwendigkeit einer Offenbarung an den Amtsarzt des Wohnortes aus.

Im Blick auf die Strafrechtsrelevanz der Vorgänge und weil die vom Ministerium für Arbeit, Soziales, Familie und Gesundheit angemeldete wissenschaftliche Begleitforschung zur Substitutionsbehandlung sowohl inhaltlich wie auch verfahrensmäßig ein abgestimmtes Vorgehen aller KV voraussetzte, bemühte sich der LfD um eine schnelle, mit den KV abgestimmte Lösung. Aufgrund seiner Initiative fand am im März 1993 eine Besprechung statt, an der Vertreter aller KV beteiligt waren. Diese Besprechung erbrachte weitestgehende Übereinstimmung in der datenschutzrechtlichen Beurteilung des Melde- und Genehmigungsverfahrens nach NUB. Alle anwesenden KV erkannten an, daß die Einwilligung in die Offenbarung personenbezogener medizinischer Daten dem Bestimmtheitsgebot entsprechen muß, d.h. sich auf Informationsvorgänge beziehen muß, die dem Patienten zuvor im Detail dargelegt wurden. Zustimmung fanden insbesondere auch die in der Dienststelle des LfD ausgearbeiteten Entwürfe eines Merkblattes für Patienten und einer Schweigepflichtentbindungserklärung. Der LfD konnte also davon ausgehen, daß in angemessener Zeit bei den KV eine datenschutzkonforme Verfahrensweise realisiert sein wird. Nach den vorliegenden Informationen ist dies bei den KV Koblenz, Rheinhessen und Trier auch der Fall.

Die KV Pfalz hingegen teilte im Juli 1993 mit, daß sie ein Muster des neu einzuführenden Merkblattes für Patienten derzeit leider nicht vorlegen könne, da die Methadonkommission den vorgeschlagenen Entwurf nicht übernehmen konnte. Auch die Schweigepflichtentbindungserklärung entspricht nicht dem Beratungsergebnis vom März 1993.

In einem Schreiben an das Ministerium für Arbeit, Soziales, Familie und Gesundheit wies der LfD darauf hin, daß die KV Pfalz gegen ihre Pflicht verstößt, die Offenbarung von Patientendaten verfahrensmäßig so zu organisieren, daß die Verschwiegenheitspflichten der Ärzte nicht verletzt und die Patientengeheimnisse gewahrt werden. Er stellte die Entscheidungskompetenz der Methadon-Kommission in Frage und bat, die KV Pfalz von Aufsichts wegen zu veranlassen, den datenschutzrechtlichen Anforderungen zu entsprechen. Ein Ergebnis war zum Zeitpunkt der Berichtsvorlage noch nicht bekannt.

11.2.8 Herausgabe von Krankenhausentlassungsberichten an den Medizinischen Dienst

In einer Besprechung unter Beteiligung von Vertretern des Medizinischen Dienstes der Krankenversicherung Rheinland-Pfalz, einer Kassenärztlichen Vereinigung und einer AOK wurde die Frage erörtert, ob es zulässig ist, die von Krankenhäusern ihren Patienten erstellten Entlassungsberichte oder Arztbriefe an den Medizinischen Dienst zu übersenden.

Die an der kassen- und vertragsärztlichen Versorgung teilnehmenden Ärzte sind verpflichtet und befugt, die für die Erfüllung von Aufgaben der Krankenkassen sowie der Kassenärztlichen Vereinigungen notwendigen Angaben aufzuzeichnen und in den gesetzlich geregelten Fällen den Krankenkassen mitzuteilen (§ 294 SGB V). Für Krankenhausärzte gelten indessen spezielle Übermittlungsregelungen (§§ 301, 276 Abs. 4 SGB V), die eine Datenübermittlung an die Krankenkassen oder den Medizinischen Dienst nicht zulassen. Hieraus folgt, daß die Weitergabe von Krankenhausentlassungsberichten der Einwilligung des Patienten bedarf. Im übrigen gebietet es der Erforderlichkeitsgrundsatz, Entlassungsberichte dem Medizinischen Dienst unmittelbar und nicht über die zuständige Krankenkasse vorzulegen.

11.3 Sozialhilfe, Kinder- und Jugendhilfe

11.3.1 Mißbrauch von Asylrecht und Sozialhilfe

Der Innenausschuß des Landtags beschloß in seinen Sitzungen am 16. Februar 1993 und 11. März 1993, eine Anhörung zum Thema Mißbrauch von Asylrecht und Sozialhilfe durchzuführen. Der LfD kam der Bitte, aus datenschutzrechtlicher Sicht zu der Frage einer effektiven Kontrolle Stellung zu nehmen, durch Vorlage einer schriftlichen Äußerung (Vorlage 12/1358) und durch Sachvortrag in der Sitzung des Innenausschusses am 11. Mai 1993 nach.

Die Kernpunkte seiner Stellungnahme sind nachfolgend zusammengefaßt:

- Die routinemäßige erkennungsdienstliche Behandlung aller Asylbewerber nach § 16 Asylverfahrensgesetz ist, ungeachtet der damit verbundenen Eingriffe in das Recht auf informationelle Selbstbestimmung, geeignet, Asylmißbrauch und Sozialhilfemißbrauch zu verhindern. Die Prüfung der Tätigkeit einer vom Ministerium des Innern und für Sport gebildeten Arbeitsgruppe Asylbetrug der Polizei ergab keine Beanstandungen.
- Das Recht auf informationelle Selbstbestimmung gilt für Ausländer ebenso wie für deutsche Staatsangehörige.
- Die gesetzlichen Bestimmungen über den Sozialdatenschutz stehen der Durchführung und – soweit sich dies aufgrund gewonnener Erfahrungen als erforderlich erweist – der Intensivierung von Kontrollmaßnahmen zur Verhinderung von Leistungsmißbrauch grundsätzlich nicht entgegen.

- Die gesetzlichen Bestimmungen über den Sozialdatenschutz lassen es zu, in Einzelfällen zur Verhinderung von Leistungsmißbrauch Amtsermittlungen durchzuführen und in diesem Zusammenhang Sozialdaten in dem für die Aufgabenerfüllung erforderlichen Umfange zu offenbaren.
- Es ist ferner zugelassen, im Einzelfall auf Ersuchen anderer Sozialleistungsträger und für die Verfolgung von Delikten, die mit der Gewährung von Sozialleistungen zusammenhängen, im erforderlichen Umfange Sozialdaten zu offenbaren.
- Automatisierte Datenabgleiche, regelmäßige Datenübermittlungen in On-line-Verfahren und Zentraldateien zur Bekämpfung des Leistungsmißbrauchs können aufgrund der bestehenden Rechtslage nur in einem sehr engen Rahmen eingerichtet werden.
- Ob die Probleme des Leistungsmißbrauchs nur mit einer Erweiterung des Kontrollinstrumentariums durch Schaffung der gesetzlichen Voraussetzungen für neue Übermittlungsformen oder auch durch eine Intensivierung der Kontrollen auf der Grundlage vorhandener Übermittlungsregelungen gelöst werden können, läßt sich aufgrund der Erfahrungen aus der Prüfpraxis der Behörde des LfD nicht beurteilen.
- Bei einer Erweiterung des Instrumentariums zur Verbesserung der Mißbrauchskontrolle – durch Zulassung automatisierter Datenabgleiche usw. – muß an den verfassungsmäßigen Vorgaben für Eingriffe in das Recht auf informationelle Selbstbestimmung festgehalten werden. Es ist zu berücksichtigen, daß deartige Formen der automatisierten Datenverarbeitung zusätzliche Eingriffe in die Rechte der weit überwiegenden Zahl solcher Leistungsempfänger darstellen, die nicht mit Leistungsmißbrauch in Zusammenhang zu bringen sind.

Nach Vorlage der Stellungnahme an den Innenausschuß des Landtags ist aufgrund des Gesetzes zur Umsetzung des Föderalen Konsolidierungsprogramms – FKPG – mit Wirkung ab 27. Juni 1993 eine Änderung des BSHG in Kraft getreten, welche die Möglichkeiten der Mißbrauchskontrolle erweitert. Der in das Gesetz eingefügte § 117 läßt zu, daß Personen, die Leistungen nach dem BSHG beziehen, auch regelmäßig im Wege des automatisierten Datenabgleichs daraufhin überprüft werden dürfen, ob und in welcher Höhe und für welche Zeiträume von ihnen Leistungen der Bundesanstalt für Arbeit (Auskunftsstelle) oder der Träger der gesetzlichen Unfall- oder Rentenversicherung (Auskunftsstellen) bezogen werden oder wurden und in welchem Umfang Zeiten des Leistungsbezuges nach dem BSHG mit Zeiten einer Versicherungspflicht oder Zeiten einer geringfügigen Beschäftigung zusammentreffen. Ferner sind die Sozialhilfeträger befugt, durch automatisierten Datenabgleich mit anderen Trägern der Sozialhilfe festzustellen, ob und in welcher Höhe und für welche Zeiträume Leistungen bezogen wurden. Ferner dürfen die Träger der Sozialhilfe zur Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe die Richtigkeit von Leistungsdaten bei anderen Stellen ihrer Verwaltung, bei ihren wirtschaftlichen Unternehmen und bei den Kreisverwaltungsbehörden und Gemeinden überprüfen und zu diesem Zweck Daten übermitteln. Die übermittlungsfähigen Merkmale sind im Gesetz genau bezeichnet. Ergänzt werden diese Bestimmungen durch Zweckbindungsregelungen und durch Löschungsvorschriften.

11.3.2 Entbindung von der Schweigepflicht im Sozialleistungsverfahren

Die Vordruckgestaltung, insbesondere die im Sozialleistungsverfahren problematische Schweigepflichtsentbindung, ist immer wieder Gegenstand von Eingaben oder – wie im nachfolgend geschilderten Falle – von Anfragen an die Behörde des LfD (vgl. 13. Tb., Tz. 11.3.3).

Eine Kreisverwaltung wollte wissen, wie folgender Text einer Entbindungserklärung unter Datenschutzgesichtspunkten beurteilt werde: „Hiermit entbinde ich (Name, Geburtsdatum, Anschrift) die Stellen, die mit der Bearbeitung meines Antrages auf Gewährung von Pflegegeld nach dem Landespflegegeldgesetz, dem Bundesversorgungsgesetz oder dem Bundessozialhilfegesetz befaßt sind, von der Schweigepflicht. Dies gilt insbesondere für folgenden Personenkreis: Sachbearbeiter der Kreisverwaltung, Hausärzte bzw. Augenfachärzte, Mitarbeiter des Gesundheitsamtes, Gerichte, Kreisrechtsausschuß der Kreisverwaltung, Bedienstete der Verbandsgemeindeverwaltung."

Der LfD wies in seiner Stellungnahme darauf hin, daß eine Erklärung mit diesem Text nicht den Anforderungen genügt, die unter Datenschutzgesichtspunkten zu stellen sind. Soweit sich die Erklärung auf Hausärzte, Augenfachärzte oder Mitarbeiter des Gesundheitsamtes bezieht, ist sie zu unbestimmt. Die Person, die um Einwilligung ersucht wird, ist in geeigneter Weise über die Rechtsgrundlage der Datenerhebung (z. B. § 60 Abs. 1 Nr. 1 SGB I), über den Verwendungszweck der Daten und den möglichen Empfängerkreis aufzuklären. Es ist ferner erforderlich, in der Erklärung den Arzt zu benennen, der von der Schweigepflicht entbunden wird, und die Materialien zu bezeichnen, auf die sich die Schweigepflichtentbindung bezieht (z. B.: Gutachten vom . . . , ärztliche Feststellung einer Behinderung). Soweit sich die Entbindungserklärung auf Sachbearbeiter der Kreisverwaltung, Gerichte, den Kreisrechtsausschuß der Kreisverwaltung oder Bedienstete einer Verbandsgemeindeverwaltung bezieht, war auf folgendes hinzuweisen: Benötigt ein Sozialleistungsträger Sozialdaten, die bei anderen Leistungsträgern vorhanden sind, zur Erfüllung seiner gesetzlichen Aufgaben nach dem SGB, so ergibt sich die Zulässigkeit der Offenbarung regelmäßig aus § 69 Abs. 1 Nr. 1 SGB X. Der Weg zur Offenbarungsbefugnis nach § 67 Satz 1 Nr. 1 (Einwilligung) ist damit – grundsätzlich – versperrt, weil die Einwilligung des Betroffenen nicht eingeholt werden darf, soweit die Offenbarung

nach §§ 68 bis 77 ohnehin zulässig, vom Willen des Betroffenen also rechtlich gar nicht abhängig ist (vgl. Hase in GK-SGB X 2, Rz. 27 zu § 67). Aber auch soweit das Sozialgeheimnis nicht berührt ist, also eine Datenübermittlung durch Behörden, die nicht Sozialleistungsträger sind, in Rede steht, muß berücksichtigt werden, daß sich die Einwilligung des Betroffenen und gesetzliche Offenbarungsbefugnisse als Grundlagen von Datenübermittlungen wechselseitig ausschließen. M.a.W., soweit eine Behörde aufgrund gesetzlicher Bestimmungen zur Datenübermittlung befugt ist, kommt eine Datenübermittlung auf der Grundlage einer Einwilligung nicht in Betracht. Öffentlichen Stellen ist es verwehrt, Maßnahmen als zustimmungsbedürftig zu deklarieren, die sie ohnehin durchführen dürfen, die der Bürger also mit seinem Willen letztlich nicht verhindern kann (vgl. Hase a. a. O., Rz. 21 zu § 67). Angesichts der nach allgemeinem und bereichsspezifischem Datenschutzrecht sehr weitgehenden Übermittlungsbefugnisse, die den gesamten Bereich der für die Aufgabenerfüllung erforderlichen Datenübermittlungen abdecken, bleibt nach Auffassung des LfD für Datenübermittlungen durch die oben genannten Behörden aufgrund von Einwilligungserklärungen kein Raum.

Aus gegebener Veranlassung sind Sozialleistungsträger immer wieder darauf hinzuweisen, daß die Entbindung von der Verpflichtung zur Einhaltung des Bankgeheimnisses nur wirksam ist, wenn sie von einem Antragsteller oder Hilfeempfänger in Kenntnis eines konkreten Anlasses für einen Ermittlungsbedarf erteilt wurde und wenn sie den Adressaten (offenbarungsbefugtes Institut), den Umfang der zu offenbarenden Informationen und den Zeitraum, auf den sich die Offenbarungsbefugnis erstrecken soll, benennt.

Diese Forderung resultiert aus den Bestimmtheitsanforderungen, denen eine Willenserklärung entsprechen muß. Die Angabe einer Kontonummer ist selbstverständlich nicht Voraussetzung für ein Auskunftsersuchen, das darauf gerichtet ist, ob überhaupt ein Konto geführt wird.

Die Benennung mehrerer offenbarungsbefugter Institute in einem Vordruck deutet in aller Regel darauf hin, daß eine anlaßbezogene Prüfung der Erforderlichkeit gerade nicht vorgenommen wurde. Üblicherweise werden pauschale Ermächtigungen für alle örtlichen oder regionalen Kreditinstitute in dieser Weise erteilt. Problematisch ist die Vorlage einer solchen Ermächtigung bei einem Kreditinstitut deshalb, weil damit offenbart wird, daß und in welchem Umfang die Richtigkeit von Angaben der Betroffenen in Zweifel gezogen wird.

Gelegentlich beziehen sich Eingaben an den LfD auch auf Vordrucke, in denen Kreditinstitute beauftragt werden, Auskunft über das Vorhandensein und den Inhalt von Konten des Ehegatten oder der Eltern zu erteilen. Mit einer solchen Ermächtigung und Beauftragung zur Auskunftserteilung dürfte der Antragsteller indessen in aller Regel seine Befugnisse überschreiten.

Der Hinweis auf die Mitwirkungspflichten nach §§ 60 ff. SGB I ist nur dann korrekt, wenn ein Antragsteller oder Empfänger von Sozialleistungen Adressat des Hinweises ist. Ehegatten oder Eltern als Unterhaltspflichtige sind nicht Normadressaten der genannten Vorschriften. Im Bereich der Sozialhilfegewährung ergibt sich die Auskunftspflicht Unterhalts- und Kostenersatzpflichtiger aus § 116 BSHG.

11.3.3 Offenbarung von Sozialdaten im Rahmen der strafrechtlichen Verfolgung von Mietwucher

Sozialhilfeträger klagen über eine Zunahme von Fällen, in denen Sozialhilfeempfängern Wohnungen zu überhöhten Preisen vermietet werden. Es wird berichtet, daß die Vermieter bisweilen Mieten forderten, die um mehr als das Doppelte über der ortsüblichen Vergleichsmiete liegen. Verbreitete Unsicherheit bestand hinsichtlich der Frage, ob und in welchem Umfange die Sozialhilfeträger befugt sind, im Rahmen der Verfolgung als Straftat oder Ordnungswidrigkeit Sozialdaten zu offenbaren.

Das Sozialgeheimnis schützt Einzelangaben über die persönlichen und sachlichen Verhältnisse der Hilfeempfänger (§ 35 SGB I). Dies sind auch Angaben über die Wohnung und die Miethöhe. Derartige Angaben wären in einem Strafverfahren oder einem Ordnungswidrigkeitsverfahren nach § 5 Wirtschaftsstrafgesetzbuch vom Leistungsträger spätestens dann zu offenbaren, wenn die Behauptung der Mietpreisüberhöhung substantiiert und möglicherweise bewiesen werden müßte. Sowohl dem Vermieter – sofern er die Tatsache des Sozialhilfebezugs noch nicht kennt – wie auch der Strafverfolgungs- oder Bußgeldbehörde wird offenbart, daß der Mieter einer Wohnung Sozialhilfeempfänger ist.

Eine Offenbarung der Sozialdaten für die genannten Zwecke käme in Betracht, wenn die betroffenen Hilfeempfänger hierzu ihr schriftliches Einverständnis erteilen würden (§ 67 Satz 1 Nr. 1, Satz 2 SGB X). Auch wenn die Mieter aus Angst vor Repressalien von Anzeigen gegen ihre Vermieter absehen, so ist es doch nicht ausgeschlossen, daß sie der Verfahrenseinleitung durch das Sozialamt zustimmen. Hierzu sollten sie unter Hinweis auf § 2 Abs. 1 i. V. m. § 1 Abs. 2 Satz 2, 2. Halbsatz BSHG angehalten werden. Nach diesen Vorschriften erhält derjenige keine Sozialhilfe, der sich selbst helfen kann, und der Hilfeempfänger muß nach seinen Kräften daran mitwirken, soweit wie möglich unabhängig von Sozialhilfe zu leben. Wenn Mieten überhöht und damit rechtswidrig sind, kann der Mieter durch geeignete rechtliche Schritte dagegen vorgehen und damit seine Mietverbindlichkeiten reduzieren. Durch seine Zustimmung zur Offenbarung von Daten im Rahmen der Einleitung von Verfahren durch das Sozialamt erfüllt er seine Verpflichtung zur Mitwirkung bei der Verringerung seines Sozialhilfebedarfs.

Es erscheint aber auch vertretbar, eine Offenbarungsbefugnis unmittelbar aus § 69 Abs. 1 Nr. 1 SGB X zu folgern, denn es ist eine Aufgabe des Sozialamtes, im Rahmen einer wirtschaftlichen und sparsamen Mittelverwendung dafür zu sorgen, daß die Mietzahlungsverpflichtungen der Hilfeempfänger minimiert werden. Die Befugnis des Sozialamtes, sich mit dem Vermieter in Verbindung zu setzen und auf eine Herabsetzung der Miete hinzuwirken – und dabei ggf. Sozialdaten zu offenbaren – steht außer Frage. Führt diese Vorgehensweise nicht zum Erfolg, so hat das Sozialamt auch die Befugnis, ein Straf- oder Ordnungswidrigkeitsverfahren einzuleiten, denn auf das Ergebnis eines solchen Verfahrens kann unmittelbar eine Herabsetzung der Miete gestützt werden. Das Sozialamt erfüllt damit eine Aufgabe im Sinne der obigen Vorschrift.

Die Abwägung, welches Verfahren (Einwilligung oder Anwendung der gesetzlichen Offenbarungsbefugnis) in Betracht kommt, hat das Sozialamt nach pflichtgemäßem Ermessen unter Beachtung des Verhältnismäßigkeitsgrundsatzes zu treffen. Handelt es sich um Fälle von geringerer Bedeutung, wird das Sozialamt nur auf der Grundlage der Einwilligung offenbaren dürfen, denn in solchen Fällen überwiegt die Pflicht zur Beachtung des informationellen Selbstbestimmungsrechts der Betroffenen. In schwerwiegenden Fällen müssen die schutzwürdigen Belange der Betroffenen hinter der Pflicht des Sozialamtes zur wirtschaftlichen und sparsamen Mittelverwendung zurückstehen.

11.3.4 Offenbarung von Vermieteradressen an die Steuerfahndung

Mit inhaltlich weitgehend identischen Schreiben wandten sich Steuerfahndungsstellen der Finanzämter mit der Bitte an Städte und Verbandsgemeinden, Sammelauskünfte über die Namen und Anschriften von Vermietern zu erteilen, an die das Sozialamt im Auftrag von Mietern (Asylbegehrenden) oder als Mieter (von Sammelunterkünften u. a.) unmittelbar Mietzahlungen leistet. Ferner wurden Auskünfte über die Namen der Mieter erbeten.

Sie wiesen darauf hin, daß die Steuerfahndungsstellen im Bundesland Baden-Württemberg bei der steuerlichen Überprüfung von Vermietungsverhältnissen mit Asylbegehrenden festgestellt hätten, daß eine Vielzahl von Vermietern ihre Mieteinnahmen nicht bzw. nicht vollständig deklarierten mit der Folge, daß Ertragsteuern (Einkommen-/Körperschaftsteuer) in beträchtlichem Umfang zu niedrig festgesetzt und erhoben worden seien. Daneben gebe es auch die allgemeine Steuerfahndungserfahrung, daß eine unbekannte Anzahl von Vermietern – insbesondere bei befristeten Mietverhältnissen – ihre Einkünfte ganz oder teilweise der Besteuerung entzögen.

Die anfragenden Gebietskörperschaften wollten vom LfD wissen, ob die Erteilung der Sammelauskünfte zulässig sei oder ob die Vorschriften zum Schutze des Sozialgeheimnisses entgegenstünden.

Zutreffend gingen die Städte und Gemeinden davon aus, daß es sich bei den Daten, um deren Übermittlung gebeten wurde, um Sozialdaten handelt, die durch das Sozialgeheimnis (§ 35 SGB I) besonders geschützt sind. Dies gilt nicht nur für die Namen der Mieter (Leistungsempfänger), sondern auch für die Namen und Anschriften der Vermieter, die Höhe der Zahlungen usw. Die Offenbarung dieser Daten ist nur beim Vorliegen der Voraussetzungen der §§ 67 ff. SGB X, konkret des § 71 Abs. 1 Nr. 3 SGB X, zulässig. Voraussetzung der Offenbarung nach dieser Vorschrift ist die Erforderlichkeit zur Erfüllung der gesetzlichen Mitteilungspflichten zur Sicherung des Steueraufkommens nach den im einzelnen genannten Bestimmungen der Abgabenordnung (AO).

Die Steuerfahndung hat nach den Vorschriften der AO umfassende Ermittlungsbefugnisse. Mit diesen Ermittlungsbefugnissen korrespondieren Auskunftspflichten, beispielsweise nach § 93 AO. Danach haben der Finanzbehörde auch Behörden die zur Feststellung eines für die Besteuerung erheblichen Sachverhaltes erforderlichen Auskünfte zu erteilen. Im Rahmen der Erfüllung dieser Auskunftspflicht gegenüber der Steuerfahndung findet indessen § 93 Abs. 1 Satz 3 keine Anwendung, d. h. die Steuerfahndung ist nicht verpflichtet, den Sachverhalt zunächst unter Inanspruchnahme der Beteiligten aufzuklären (§ 208 Abs. 1 AO).

Der Bundesfinanzhof (BFH) hat in seinem Urteil vom 24. März 1987 die Rechtmäßigkeit eines Sammelauskunftsersuchens bestätigt. Er hält derartige Auskunftsersuchen dann für zulässig, wenn dazu ein hinreichender Anlaß besteht, wobei die objektive Steuerverkürzung einer verhältnismäßig großen Zahl von Gewerbeausübenden – im konkreten Falle Kreditvermittler – ausreicht. Bereits in seiner Entscheidung vom 29. Oktober 1986 – VII R 82/85 – hatte der BFH klargestellt, daß für die Einholung einer Auskunft nach § 93 Abs. 1 Satz 1 AO im Rahmen der Steuerfahndung keine höheren Anforderungen als für das Tätigwerden nach § 208 Abs. 1 Nr. 3 AO – Aufdeckung und Ermittlung unbekannter Steuerfälle – bestehen. Das Finanzgericht Hamburg wies in seinem Urteil vom 4. Dezember 1986 – V 66/86 – auf folgendes hin: Im Gegensatz zu Ermittlungen im Steuerstrafverfahren setzt das Tätigwerden im Falle des § 208 Abs. 1 Satz 1 Nr. 3 AO keinen Anfangsverdacht, also das Vorliegen zureichender tatsächlicher Anhaltspunkte für eine Steuerstraftat oder eine Steuerordnungswidrigkeit voraus. Ausreichend – aber auch erforderlich – ist vielmehr die Möglichkeit einer Steuerstraftat bzw. Steuerordnungswidrigkeit oder einer objektiven Steuerverkürzung. Für die Ermittlungen nach § 208 Abs. 1 Satz 1 Nr. 3 AO genügt bereits eine sich auf die bloße Möglichkeit einer Tatbestandsverwirklichung stützende Vermutung. Die herrschende Ansicht in Literatur und Rechtsprechung läßt hierfür abstrakte Anhaltspunkte, also auch eine allgemeine Erfahrung, nach der die Möglichkeit einer Tatbestandsverwirklichung in Betracht kommt, genügen (vgl. RDV 1992, S. 90 f).

Zusammenfassend vertrat der LfD die Auffassung, daß die verfassungsrechtliche Verhältnismäßigkeit des Anliegens der Steuerfahndung durchaus diskussionswürdig erscheint; angesichts der höchstrichterlichen Rechtsprechung dürfte es aber nicht durchsetzbar sein, daß Auskünfte über die Vermieter unter Berufung auf Datenschutzgründe verweigert werden. Dies gilt indessen nicht für die gleichfalls erbetene Auskunft über die Anschriften der Leistungsempfänger (Mieter), denn die Erforderlichkeit dieser Daten für die Aufgabenerfüllung wurde von den Steuerfahndungsstellen nicht dargelegt und auch auf Anfrage nicht begründet.

11.3.5 Übermittlung von Kfz-Zulassungsdaten an Sozialämter

Ein Sozialhilfeempfänger wird kaum in der Lage sein, einen Teil der ihm zur Verfügung stehenden Mittel zum Kauf und zur Unterhaltung eines Pkw zu verwenden. In der einschlägigen Literatur wird folgerichtig die Auffassung vertreten, daß eine grundsätzliche Unvereinbarkeit zwischen Sozialhilfebezug und dem Halten eines Kraftfahrzeugs besteht. Dementsprechend sind die Sozialämter daran interessiert, von Amts wegen zu ermitteln, ob der Besitzer eines Kraftfahrzeugs etwa dadurch gegen das Gebot zum wirtschaftlichen Mitteleinsatz verstößt, daß er die Sozialhilfe nicht zunächst für die Sicherstellung des Lebensunterhalts, insbesondere den Lebensmittelbedarf und vor allem die Wohnungsmiete, sondern für Ausgaben wie Autokauf einsetzt oder ob die Sozialhilfe mit falschen Angaben erschlichen wurde (Sozialhilfebetrug). Außerdem ist zu prüfen, ob ein im Eigentum des Hilfeempfängers befindliches Kraftfahrzeug verwertbares Vermögen darstellt. Dieses Ermittlungsinteresse der Sozialämter besteht unabhängig davon, ob es sich bei dem Hilfeempfänger um einen Deutschen oder um einen Ausländer handelt. Gerade bei Asylbewerbern wurde indessen mehrfach beobachtet, daß sie, obwohl Sozialhilfeempfänger, ein Kraftfahrzeug hielten. Eine Verbandsgemeinde wollte wissen, ob es zulässig sei, den Vor- und Familiennamen, die Anschrift, das Geburtsdatum und Geburtsort von Asylbewerbern – die Sozialhilfeempfänger sind – an die Kfz-Zulassungsstelle mit dem Ersuchen zu übermitteln, durch Abgleich der übermittelten Daten mit den Zulassungsdaten solche Fälle zu ermitteln und mitzuteilen, in denen die Zulassung eines Pkw durch einen Asylbewerber (Sozialhilfeempfänger) beantragt wurde. Sie war der Meinung, daß die Offenbarung von Sozialdaten durch Weitergabe von Daten in Listenform auf § 68 SGB X – Offenbarung im Rahmen der Amtshilfe – gestützt werden könne.

Diese Rechtsauffassung ließ indessen unberücksichtigt, daß Amtshilfe ihrem Wesen nach nur dann vorliegt, wenn ein Ersuchen gestellt worden ist (vgl. § 4 Abs. 1 VwVfG, § 3 Abs. 1 SGB X). Sozialleistungsträger können also nicht von sich aus Daten unter Berufung auf § 68 SGB X an andere Stellen weitergeben (vgl. Walz in GK SGB X 2, RdNr. 17 zu § 68).

Der Sozialleistungsträger ist aber nicht gehindert, den Sachverhalt in konkreten Verdachtsfällen zu ermitteln (§ 20 SGB X). Im Rahmen dieser Ermittlungen ist er nach § 69 Abs. 1 Nr. 1 SGB X auch befugt, Einzelanfragen an die Kfz-Zulassungsstelle zu richten und damit die Tatsache des Sozialhilfebezugs zu offenbaren, denn es gehört zu den „Aufgaben nach diesem Gesetzbuch", Fälle unberechtigten Sozialhilfebezugs aufzuklären.

Die vom Sozialamt begehrten Auskünfte könnten durch die Kfz-Zulassungsstelle erteilt werden, wenn dies zur Verfolgung von Straftaten oder zur Verfolgung von Ordnungswidrigkeiten erforderlich wäre (§ 35 Abs. 1 Nr. 2 und 3 StVG).

§ 39 StVG kommt als Rechtsgrundlage für die Datenübermittlung nur dann in Betracht, wenn das Sozialamt Auskünfte „unter Angabe der Personalien des Halters oder des Kfz-Kennzeichens" erfragt und die Rückforderung von Sozialleistungen in Höhe von mehr als 1 000,– DM beabsichtigt ist."

Die Datenübermittlung nach § 35 Abs. 1 Nr. 2 StVG durch die Zulassungsstelle könnte indessen auch dann erfolgen, wenn der Verdacht eines Sozialhilfebetrugs in jedem Fall vorläge, in dem ein Asylbewerber ein Kraftfahrzeug anmeldet, denn es gehört zu den Aufgaben der Sozialämter, die Strafverfolgung wegen Sozialhilfebetrugs einzuleiten.

§ 69 Abs. 1 Nr. 1 SGB X bietet im übrigen auch eine Rechtsgrundlage bezüglich der Offenbarung sonstiger Einzelheiten vom Sozialamt an die Strafverfolgungsbehörde, etwa der Höhe des beim Sozialamt eingetretenen Schadens.

Unterdessen erfolgte eine Klarstellung durch die Änderung des Bundessozialhilfegesetzes im Rahmen des Gesetzes zur Umsetzung des Föderalen Konsolidierungsprogramms. In § 117 Abs. 3 BSHG wurde eine spezielle Rechtsgrundlage für die Überprüfung der Eigenschaft als Kraftfahrzeughalter geschaffen.

11.3.6 Öffentliche Verbreitung von Sozialhilfebescheiden

Aufgrund von Eingaben und der öffentlichen Berichterstattung wurden zwei Fälle ausländerfeindlicher Betätigung bekannt, die auch Datenschutzrelevanz hatten: Mit dem Ziel, Ressentiments in der Bevölkerung gegen Ausländer zu schüren, wurden Ablichtungen von Sozialhilfebescheiden in Umlauf gesetzt. Da es sich in beiden Fällen um sehr kinderreiche Familien handelte und die Sozialhilfe einen hohen Mietanteil umfaßte, waren in beiden Fällen erhebliche Geldleistungen zu erbringen, die – so der Kommentar der Initiatoren der Aktionen – belegten, wie „das Deutsche Volk von den Ausländern ausgenommen" werde.

Die ausländerfeindlichen Aktionen waren keineswegs auf den Zuständigkeitsbereich der Sozialleistungsträger beschränkt, sondern erstreckten sich auf das gesamte Bundesgebiet. Dies kann jedenfalls aus einer Vielzahl von Hinweisen gefolgert werden, die bei den zuständigen Sozialämtern eingingen.

Die Recherchen des LfD zielten auf die Klärung des Sachverhalts, soweit die Verletzung des Sozialgeheimnisses durch die beteiligten Behörden in Rede stand.

In einem der Fälle konnte dies von vornherein ausgeschlossen werden. Der Sozialhilfeempfänger räumte eigene Unachtsamkeit ein, die dazu führte, daß der Sozialhilfebescheid in fremde Hände gelangte und veröffentlicht werden konnte.

In dem zweiten bekanntgewordenen Fall lagen die Dinge anders: Es war nicht nachweisbar, daß das Verhalten des Hilfeempfängers selbst ursächlich war für die Herstellung der Kopien. Demzufolge konnte nicht ausgeschlossen werden, daß das Sozialgeheimnis durch eine Person oder Stelle im öffentlichen Bereich verletzt wurde.

Eine vom LfD durchgeführte örtliche Prüfung ergab hierfür aber keine konkreten Anhaltspunkte. Auch die staatsanwaltschaftlichen Ermittlungen führten nicht weiter. Es konnte nicht festgestellt werden, ob es sich bei dem in die Öffentlichkeit gelangten Sozialhilfebescheid um das dem Leistungsempfänger zugegangene Original oder um eine Ablichtung der bei der Verbandsgemeinde verbliebenen Zweitschrift handelte. Die Feststellungen wurden dadurch erschwert, daß die Zweitschrift nicht als Durchschrift erstellt wurde, sondern daß sie wie die Erstschrift im automatisierten Verfahren gesondert ausgedruckt worden war.

Der LfD mußte deshalb darauf hinweisen, daß er keine Möglichkeit sieht, die Verbreitung der Bescheidkopien, soweit hieran Personen und Stellen außerhalb des öffentlichen Bereichs beteiligt sind, zu verhindern.

11.3.7 Öffentliche Zustellung eines Rückzahlungsbescheids

Nach § 15 Abs. 1 Buchst. a des Bundesverwaltungszustellungsgesetzes (VwZG) – anzuwenden nach § 1 des Landesgesetzes über die Zustellung in der Verwaltung – kann durch öffentliche Bekanntmachung zugestellt werden, wenn der Aufenthaltsort des Empfängers unbekannt ist.

Ein Sozialhilfeträger fragte beim LfD an, ob diese gesetzliche Bestimmung auch im Sozialleistungsbereich, konkret bei der Zustellung eines Bescheids über die Rückzahlung von zu Unrecht gewährter Sozialhilfe an einen Adressaten unbekannten Aufenthalts, anzuwenden ist. Er wies darauf hin, daß mit der Zustellung durch öffentliche Bekanntmachung eine Fülle von Sozialdaten des Betroffenen offenbart werde und verwies auf die Kollission der Zustellungsregelung mit den gesetzlichen Vorschriften zum Schutze des Sozialgeheimnisses.

Der LfD vertrat die Auffassung, daß beim Vorliegen der Voraussetzungen des § 15 Abs. 1 Buchst. a VwZG unter sorgfältiger Beachtung des Verhältnismäßigkeitsgrundsatzes auch ein Bescheid über die Rückzahlung von zu Unrecht gewährter Sozialhilfe öffentlich zugestellt werden kann. Im Rahmen der Verhältnismäßigkeitsprüfung ist abzuwägen zwischen der Bedeutung der Sache (Höhe der Forderung) und dem Geheimhaltungsinteresse des Betroffenen. Der Grundsatz des geringstmöglichen Eingriffs fordert im Sozialleistungsbereich darüber hinaus in aller Regel die Zustellung unter Berücksichtigung des § 15 Abs. 2 Satz 2 VwZG, d. h. die Aushängung einer Benachrichtigung, in der allgemein anzugeben ist, daß und wo das Schriftstück eingesehen werden kann.

11.3.8 Der zulässige Inhalt von Überleitungsanzeigen

Ein Sozialhilfeempfänger beklagte sich, daß einem Drittschuldner mit einer Überleitungsanzeige nach § 90 BSHG die Höhe der monatlichen Sozialhilfeaufwendungen sowie die Anschrift des Pflegeheims mitgeteilt wurden, in dem er sich befindet.

Eine Überleitungsanzeige muß als Verwaltungsakt inhaltlich hinreichend bestimmt (§ 33 SGB X) und begründet (§ 35 SGB X) sein. Im konkreten Falle wäre dem Bestimmtheitsgebot und der Begründungspflicht aber auch dann entsprochen worden, wenn lediglich mitgeteilt worden wäre, daß Sozialhilfe geleistet wird und daß die monatlichen Aufwendungen die übergeleiteten Forderungen übersteigen.

Ferner ist der Sozialleistungsträger grundsätzlich verpflichtet, bei einer Offenbarung von Sozialdaten an Private – wie sie im Rahmen einer Überleitungsanzeige erfolgt – auf die Geheimhaltungspflichten hinzuweisen, die sich aus § 78 SGB X ergeben.

11.3.9 Wahrung des Sozialgeheimnisses bei der Geltendmachung eines Anspruches gegenüber einer Eigenschadenversicherung

Nach § 86 des Landesbeamtengesetzes Rheinland-Pfalz hat der Dienstherr den Vermögensschaden bei einfacher Fahrlässigkeit zu tragen. Dieses Schadensrisiko wird gelegentlich durch sog. Eigenschadenversicherungen abgedeckt. Ob eine solche Versicherung abgeschlossen wird, liegt in der Entscheidung der jeweiligen Behörde.

Der LfD vertritt – jedenfalls für den Sozialleistungsbereich – die Auffassung, daß im Rahmen der Geltendmachung von Ansprüchen gegen die Versicherung keine Befugnis zur Offenbarung der Identität von Hilfeempfängern besteht, es sei denn, die Betroffenen erklärten ihre Einwilligung nach § 67 SGB X. § 69 Abs. 1 Nr. 1 SGB X kommt als gesetzliche Offenbarungsbefugnis deshalb nicht in Betracht, weil der Abschluß und die Inanspruchnahme der Versicherung nicht zu den gesetzlichen Aufgaben nach dem Sozialgesetzbuch zählt.

In mehreren bekanntgewordenen Fällen haben die Versicherungen diese Rechtsauffassung anerkannt und auf die Bekanntgabe von Namen der Sozialleistungsempfänger – die im übrigen für die Schadensbearbeitung relativ belanglos sind – verzichtet. Das Rechtsamt einer größeren Stadt teilte mit, daß die Versicherung gegen die Anonymisierung von Vorgängen, die dem Sozialdatenschutz unterliegen, keine Bedenken erhebe. In der Praxis werde so verfahren, daß die kompletten Akten fotokopiert und in den Fotokopien die Namen der Hilfeempfänger und anderer Personen unkenntlich gemacht würden.

Falls eine Versicherung dieses Anonymisierungsverfahren nicht akzeptiert, verbleibt nur die Möglichkeit, Sozialleistungsfälle aus der Versicherung herauszunehmen.

11.3.10 Offenbarung von Daten Unterhaltspflichtiger

Die Beschwerde eines Bürgers richtete sich gegen die Offenbarung seines Erwerbseinkommens und anderer seine Fähigkeit zur Leistung von Unterhalt kennzeichnender Informationen durch ein Jugendamt gegenüber der geschiedenen Ehefrau im Rahmen der Beratung und Unterstützung bei der Ausübung der Personensorge nach § 18 SGB VIII. Durch die Offenbarung sollte der Ehefrau ermöglicht werden, ihre Unterhaltsansprüche gegen den geschiedenen Ehemann geltend zu machen.

Bei der rechtlichen Bewertung des Vorganges war zu berücksichtigen, daß keine Ansprüche übergeleitet waren. Die Mutter war Inhaberin des vollen elterlichen Sorgerechts und sie konnte ihr Kind unterhaltsrechtlich selbst vertreten. Damit war sie auch auskunftsberechtigt im Sinne des § 1605 BGB. Die Inanspruchnahme des Jugendamtes zur Beratung und Unterstützung im Rahmen der Geltendmachung des Auskunftsanspruchs begründet zwischen diesem und der Mutter als der nach dem Gesetz Auskunftsberechtigten keine Verschwiegenheitspflichten.

11.3.11 Archivierung von Jugendamtsakten

Die Anwendung des Landesarchivgesetzes (LArchG) bereitet in der Praxis noch Schwierigkeiten. Unklar ist insbesondere seine Geltung im Sozialleistungsbereich und das Verhältnis zwischen Löschungs- und Anbietungspflicht.

Nach § 2 Abs. 2 LArchG gewährleisten die kommunalen Gebietskörperschaften für ihre eigenen Archive, daß in ihnen hinsichtlich der Sicherung, Erhaltung und Nutzung des Archivgutes die für die staatlichen Archive geltenden Grundsätze beachtet werden. Hieraus folgt, daß die Bestimmungen über die Anbietungspflicht (§ 7 LArchG) entsprechend anzuwenden sind. Nach § 7 Abs. 2 Nr. 1 LArchG sind auch solche Unterlagen anzubieten, die nach datenschutzrechtlichen Vorschriften vernichtet oder gelöscht werden müßten. Aufgrund der Verweisung auf § 1 Abs. 4 LArchG soll dies zwar nur für solche Unterlagen gelten, bezüglich deren eine durch landesrechtliche Vorschrift begründete Pflicht zur Vernichtung oder Löschung besteht. Dieser Gesetzeswortlaut, der im Verlauf der Ausschußberatungen im Blick auf einen konkreten Vorgang aus dem Anwendungsbereich des Landeskrankenhausgesetzes entstand, gibt indessen den gesetzgeberischen Willen nur unvollständig wieder. Gewollt war eine Ausnahme von der Löschungs- bzw. Vernichtungspflicht und eine Erstreckung der Anbietungspflicht auf alle Unterlagen, für die der Landesgesetzgeber regelungsbefugt ist, also auch auf solche Unterlagen, die durch das Sozialgeheimnis geschützt sind (entsprechend § 2 Abs. 4 Nr. 1 BArchG). Daß der Landesgesetzgeber befugt ist, derartige Regelungen zu treffen, steht außer Frage. § 71 Abs. 1 Satz 2 SGB X statuiert ausdrücklich eine Offenbarungsbefugnis für die Erfüllung der gesetzlichen Pflichten zur Sicherung und Nutzung von Archivgut aufgrund gesetzlicher Vorschriften der Länder. Auch § 3 Abs. 3 Satz 4 LArchG, der eine Nutzung in Übereinstimmung mit § 5 Abs. 3 BArchG erst 80 Jahre nach der Entstehung zuläßt, deutet darauf hin, daß der Landesgesetzgeber eine Ausnahmeregelung – bezüglich der Löschung oder Vernichtung – auch für den Anwendungsbereich des § 35 SGB I treffen wollte.

Das Archiv hat binnen sechs Monaten im Benehmen mit der anbietenden Stelle zu entscheiden, welche der angebotenen Unterlagen bleibenden Wert haben und deshalb zu übernehmen sind (§ 8 Abs. 1 LArchG). § 66 SGB VIII ist auf solche Unterlagen anzuwenden, die vom Archiv nicht übernommen werden, weil die Übernahmevoraussetzung nicht vorliegt. Aufgrund seiner Prüfungserfahrung geht der LfD davon aus, daß nur ein sehr geringer Teil der bei Jugendämtern entstehenden Vorgänge archivwürdig ist.

In der Praxis wird so vorzugehen sein, daß die Unterlagen des Jugendamtes daraufhin überprüft werden, ob die Löschungsvoraussetzungen des § 66 SGB VIII i. V. mit § 84 SGB X vorliegen. Wenn dies der Fall ist, sind die Unterlagen dem Archiv anzubieten. Die Unterlagen sind zu löschen – bzw. nach § 66 Abs. 2 SGB VIII zu sperren –, wenn das Archiv nicht innerhalb einer Frist von sechs Monaten erklärt, daß sie bleibenden Wert haben und deshalb übernommen werden (§ 8 Abs. 1 LArchG).

Die Nutzung von Archivgut durch Sozialarbeiter bestimmt sich nach § 3 Abs. 5 i. V. m. Abs. 2 Nr. 4 LArchG. § 203 Abs. 1 StGB, der die unbefugte Geheimnisoffenbarung durch Sozialarbeiter unter Strafe stellt, zwingt die Archivverwaltung, bei der Herausgabe von Unterlagen sorgfältig darauf zu achten, daß sie nur dem Mitarbeiter ausgehändigt werden, der im Sinne dieser Vorschrift befugt ist.

Es besteht für die Jugendämter kein Hinderungsgrund, die endgültig an das Archiv abgegebenen Unterlagen sowie die nach § 66 SGB VIII gesperrten Unterlagen in einer Kartei nachzuweisen. Für den Nachweis gelöschter Daten oder vernichteter Akten in einer Kartei existiert hingegen keine Rechtsgrundlage.

Eine Kartei zum Nachweis archivierter oder gesperrter Unterlagen darf nur die zum Auffinden dieser Unterlagen erforderlichen Angaben enthalten. Die Angabe des Grundes der Aktenführung ist nicht erforderlich und daher unzulässig.

Gesperrte Daten dürfen – auch von Sozialarbeitern – nur mit Einwilligung des Betroffenen oder beim Vorliegen der Voraussetzungen des § 20 Abs. 6 Nr. 1 und 2 BDSG (neue Fassung) genutzt werden.

11.4 Sonstiges

11.4.1 SGB-Auslegungsfragen

Die Behörde des LfD wird häufig um Beratung in datenschutzbezogenen Fragen zur Auslegung des Sozialgesetzbuchs gebeten. Wegen ihrer grundsätzlichen Bedeutung ist nachfolgend seine Stellungnahme zur Anfrage einer Kreisverwaltung abgedruckt, die folgende Sachverhalte betraf:

a) Ein Antragsteller macht in verschiedenen Leistungsbereichen, die einer Abteilung angehören (z. B. Wohngeld, Ausbildungsförderung) Angaben zum Einkommen, Familienstand usw. Stellt die Nutzung der Daten für unterschiedliche Zwecke eine Offenbarung dar und unter welchen Bedingungen ist diese ggf. zulässig?

   Der LfD äußerte sich wie folgt:

   Offenbaren personenbezogener Daten ist das Bekanntgeben der Daten an einen Dritten – andere Stelle oder Person, jedoch nicht der Betroffene – oder an die Öffentlichkeit in der Weise, daß die Daten weitergegeben oder zum Abruf oder zur Einsichtnahme bereitgehalten werden. Für die Bestimmung des Begriffs des „Dritten" kommt es maßgeblich darauf an, wie die „SGB-Stelle", die Normadressat der Vorschriften zum Schutze des Sozialgeheimnisses ist, definiert wird, denn „Datenweitergabe innerhalb der SGB-Stelle ist kein Offenbaren, Datenweitergabe nach außen ist offenbaren" (vgl. Borchert in Borchert/Haase/Walz, GK zum SGB – Schutz der Sozialdaten, RdNr. 54 zu § 35 SGB I).

   Zur Abgrenzung des Stellenbegriffs werden in der Literatur unterschiedliche Auffassungen vertreten; vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts – Volkszählungsurteil und insbes. Kammerbeschluß vom 18. Dezember 1987 – 1 BvR 962/87 – ist es geboten, den Stellenbegriff im Grundsatz nach funktionalen Gesichtspunkten zu bestimmen. Danach ist eine „SGB-Stelle" jede Verwaltungseinheit, die eine Aufgabe nach dem SGB zu erfüllen hat. Organisationsrechtliche Grundsätze spielen freilich insoweit eine Rolle, als innerhalb des kleinsten organisationsrechtlich bestimmten Bereichs eine weitere Untergliederung – in mehrere SGB-Stellen – nicht in Betracht kommt. Auf die obige Anfrage bezogen bedeutet dies, daß innerhalb eines Dezernats, eines Amtes oder einer Abteilung gebildete Referate oder Sachgebiete für Wohngeld als selbständige SGB-Stellen anzusehen sind, die im Rechtssinne Sozialdaten offenbaren, wenn sie Informationen an ein innerhalb des gleichen Dezernats usw. gebildetes Referat für Ausbildungsförderung weitergeben. Werden beide Aufgaben indessen innerhalb der gleichen nicht weiter untergliederten Organisationseinheit wahrgenommen, handelt es sich um eine SGB-Stelle, innerhalb deren keine Offenbarung stattfindet. Wenn also im Extremfall ein Sachbearbeiter mit Schreibkraft das Referat „Wohngeld und Ausbildungsförderung" bildet, so findet keine Offenbarung statt, wenn er sich bei der Bearbeitung des Wohngeldantrages erinnert, daß die Einkommensverhältnisse bei der Beantragung von Ausbildungsförderung anders dargestellt wurden und aufgrund der ihm unmittelbar zugänglichen Informationen nähere Feststellungen trifft.

   Bei sachgemäßer Behördenorganisation wird die sich daraus ergebende funktionale Gliederung weitgehend mit der Aufbauorganisation korrespondieren. Die Verwaltung ist verpflichtet – so das Bundesverfassungsgericht im Volkszählungsurteil –, dem Grundsatz der informatorischen Gewaltenteilung durch organisatorische und verfahrenssichernde Maßnahmen Geltung zu verschaffen. In aller Regel wird – abgesehen von sehr kleinen Verwaltungen – eine Zweckänderung von Daten stets auch mit einer Offenbarung verbunden sein.

   Auch wenn danach die Zulässigkeit von Informationsweitergaben weitestgehend unter Anwendung der Offenbarungsbestimmungen des Sozialgesetzbuchs zu beurteilen ist, so bedeutet dies keineswegs, daß die für die Erfüllung von Aufgaben nach dem SGB zuständigen Stellen grundsätzlich gehindert wären, Angaben der Antragsteller auf ihre Richtigkeit hin zu überprüfen und zu diesem Zweck Daten zu offenbaren oder bei anderen Stellen, die ihrerseits die Offenbarungsbestimmungen anzuwenden haben, zu erfragen. Zwar gilt der „Vorrang der Datenerhebung beim Betroffenen", d. h., eine für die

Gewährung einer Sozialleistung zuständige Stelle darf nicht etwa deshalb auf die Erhebung von Angaben beim Betroffenen verzichten, weil diese Angaben bei einer anderen Stelle, die für einen anderen Leistungsbereich zuständig ist, bereits vorliegen. Eine Nutzung von Informationen auf der Basis einer Einwilligung (§ 67 Satz 1 Nummer 1 SGB X) ist dadurch selbstverständlich nicht ausgeschlossen. Besteht Grund zu der Annahme, daß der Antragsteller oder Leistungsempfänger seinen Mitwirkungspflichten nicht vollständig nachgekommen ist oder unzutreffende Angaben gemacht hat, so lassen es die §§ 20 (Untersuchungsgrundsatz) und 21 SGB X (Beweismittel) zu, Informationen zum Zwecke der Überprüfung im Einzelfall auch bei anderen Sozialleistungsträgern zu erfragen, die ihrerseits, weil die Offenbarung „für die Erfüllung einer gesetzlichen Aufgabe nach diesem Gesetzbuch durch eine in § 35 des Ersten Buches genannte Stelle" erforderlich ist (§ 69 Abs. 1 Nr. 1, erste Alternative), auch offenbarungsbefugt sind. Die Aufgabenwahrnehmung im Rahmen der §§ 20 und 21 SGB X muß verhältnismäßig sein. Mit dem Verhältnismäßigkeitsgrundsatz wäre es nicht vereinbar, nicht erforderliche Prüfungen vorzunehmen – etwa wenn die Einkommensnachweise lückenlos erbracht sind – oder routinemäßig jeden Fall dadurch zu überprüfen, daß eine andere Stelle um Offenbarung von Informationen, die bei dieser vorliegen, ersucht wird.

b) Ein Antragsteller erteilt der Wohngeldstelle – Sozialamt – und der Veranlagungsstelle der Abfallbeseitigung – Abt. Umweltschutz – Auskünfte zu seinen Familien- und Wohnverhältnissen. Ist eine Offenbarung zum Zwecke der Überprüfung der Angaben zulässig?

Hierzu nahm der LfD wie folgt Stellung:

Es steht außer Frage, daß Informationen, sofern sie von SGB-Stellen an Nicht-SGB-Stellen weitergegeben werden, im Rechtssinne offenbart werden. Anzuwenden sind selbstverständlich auch insoweit die Offenbarungsbestimmungen des SGB. Wird eine SGB-Stelle im Rahmen der §§ 20 f. SGB X, also „bei der Erfüllung einer gesetzlichen Aufgabe nach diesem Gesetzbuch" tätig, so darf sie unter Beachtung des Verhältnismäßigkeitsprinzips bei Kontrollrückfragen die Tatsache der Antragstellung oder des Leistungsbezugs offenbaren. Die Veranlagungsstelle der Abfallbeseitigung ist eine Finanzbehörde im Sinne des § 21 Abs. 4 SGB X. Sie hat in dem in dieser Vorschrift genannten Umfange Auskünfte zu erteilen.

11.4.2 Weiterleitung von Anfragen an die zuständige Behörde

Ist eine Behörde als Adressat einer Anfrage für die Beantwortung sachlich oder örtlich unzuständig, so wird der Vorgang oft routinemäßig mit der Bitte um Übernahme der Bearbeitung an die zuständige Behörde weitergeleitet. Der Anfrager erhält eine Abgabenachricht; seine Zustimmung zur Weiterleitung wird in aller Regel nicht eingeholt. Diese Zustimmung ist aber erforderlich, wenn aus dem Inhalt der Anfrage gefolgert werden kann, daß er eine Anfrage ganz bewußt an eine bestimmte Behörde richten wollte oder wenn die Behörde besondere Geheimhaltungsbestimmungen – z. B. Sozialgeheimnis, Statistikgeheimnis oder Steuergeheimnis – zu beachten hat.

Wenig Sensibilität ließ das Versicherungsamt einer Kreisverwaltung erkennen, als es die Anfrage eines Rentenbeziehers nach dem steuerlichen Ertragsanteil einer BfA-Rente ohne dessen Zustimmung zur Beantwortung an das zuständige Finanzamt weiterleitete. Die direkte Folge war eine Steuernachforderung des Finanzamtes.

Man wird sicherlich argumentieren können, daß doch damit alles in bester Ordnung sei. Die Steuer hätte ohnehin gezahlt werden müssen; die Vorgehensweise des Versicherungsamtes habe das Verfahren nur etwas abgekürzt.

Diese Argumentation läßt aber unberücksichtigt, daß das Versicherungsamt als aufsichtsberechtigte Behörde i. S. des § 35 Abs. 1 Satz 3 SGB I die Vorschriften zum Schutze des Sozialgeheimnisses zu beachten hat. Das Sozialgeheimnis umfaßt den gesamten Aufgabenbereich des Versicherungsamtes, also auch die Auskunftserteilung nach § 92 Abs. 1 SGB IV. Wer sich mit der Bitte um Auskunft an ein Versicherungsamt wendet, soll darauf vertrauen dürfen, daß die Anfrage selbst wie auch Informationen über ihren Inhalt nur beim Vorliegen bestimmter gesetzlicher Voraussetzungen offenbart werden. Eine der gesetzlichen Voraussetzungen bildet nach § 71 Abs. 1 Satz 1 Nr. 3 SGB X zwar auch die Offenbarung zur Sicherung des Steueraufkommens. Die korrespondierende Vorschrift (§ 116 AO) begründet eine Offenbarungsverpflichtung aber nur dann, wenn der Verdacht einer Steuerstraftat begründet ist. Diese Voraussetzung lag eindeutig nicht vor, so daß die Vorgehensweise des Versicherungsamtes als Verstoß gegen die Vorschriften zum Schutze des Sozialgeheimnisses zu rügen war.

11.4.3 Sozialdatenschutz bei der Einschaltung eines Gegengutachters durch das Versorgungsamt

In einer Eingabe an den LfD wandte sich ein Empfänger von Leistungen nach dem Bundesversorgungsgesetz dagegen, daß ein aufgrund eines Beweisbeschlusses des Landessozialgerichts erstelltes medizinisches Gutachten, das dem Landesversorgungsamt zur Stellungnahme zugeleitet worden war, ohne seine Zustimmung einem Gegengutachter zugänglich gemacht wurde. Er sah hierin eine Verletzung der gesetzlichen Bestimmungen zum Schutze des Sozialgeheimnisses.

Im Rahmen der Beurteilung des Sachverhalts unter datenschutzrechlichen Gesichtspunkten kann dahingestellt bleiben, ob das Landesversorgungsamt nach § 35 SGB I i. V. m. § 67 ff. SGB X Sozialdaten offenbart hat oder ob die Daten innerhalb der

speichernden Stelle genutzt wurden, denn selbst wenn die Weitergabe als Offenbarung zu qualifizieren wäre, stünden ihr diese Bestimmungen nicht entgegen. § 69 Abs. 1 Nr. 1 SGB X läßt die Offenbarung von Sozialdaten zu, soweit sie für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch durch einen Sozialleistungsträger oder für die Durchführung eines damit zusammenhängenden gerichtlichen Verfahrens erforderlich ist. Die zweite Offenbarungsalternative liegt vor, denn es gehört zu den gesetzlichen Aufgaben des Landesversorgungsamtes, die Leistungsvoraussetzungen zu klären bzw. die auf die Klärung der Leistungsvoraussetzungen zielenden Beweisfragen des Gerichts zu beantworten. Sofern es zur Beantwortung einen externen Sachverständigen heranzieht – der im übrigen wie das Landesversorgungsamt das Sozialgeheimnis zu beachten hat und der Strafandrohung des § 203 StGB unterliegt –, ist die Weitergabe des Gutachtens zur Aufgabenerfüllung erforderlich und damit zulässig.

§ 76 SGB X, der strenge Offenbarungsrestriktionen für besonders schutzwürdige personenbezogene Daten statuiert, findet keine Anwendung, denn die Daten wurden nicht – wie Absatz 1 dieser Vorschrift voraussetzt – von einem Arzt oder einer anderen in § 203 Abs. 1 und 3 StGB genannten Person, sondern vom Landessozialgericht zugänglich gemacht. Eine Zweckänderung i. S. des § 78 SGB X liegt nicht vor, so daß auch bei Anwendung dieser Vorschrift die Vorgehensweise des Landesversorgungsamtes nicht zu beanstanden war.

11.4.4 Adoptions- und Pflegekinderwesen Verwendung eines Motivationserfassungsbogens

Das Landesamt für Jugend und Soziales bemüht sich seit langem, in Zusammenarbeit mit den Jugendämtern in Rheinland-Pfalz einen Motivationserfassungsbogen für Adoptionsbewerber und künftige Pflegeeltern zu entwickeln und einzuführen. Die standardisierte Datenerhebung unter Verwendung dieses Bogens soll eine Eignungsprüfung nach einheitlichen Kriterien fördern. Der Bogen soll Bestandteil der Jugendhilfeakten werden und die Grundlage für die Erstellung des Adoptionseignungsberichts bilden. Die Datenerhebung wie auch die Weiterleitung des Erfassungsbogens an andere Adoptionsvermittlungsstellen soll nur mit dem Einverständnis der Bewerber erfolgen dürfen. Ein Muster des Motivationserfassungsbogens wurde dem LfD zur Stellungnahme unter datenschutzrechtlichen Gesichtspunkten vorgelegt.

Das Landesamt wurde darauf hingewiesen, daß aus dem sehr allgemein gehaltenen Text der Einverständniserklärung keine Befugnis für eine umfassende Nutzung des Erfassungsbogens in der beschriebenen Weise hergeleitet werden kann. Grundsätzlich muß jede Einwilligung dem Bestimmtheitserfordernis genügen, d. h., der Betroffene muß über Anlaß und Zweck des Vorganges informiert werden. Außerdem kann eine Einwilligung in die Offenbarung von Daten nach § 67 Nr. 1 SGB X nur für den Einzelfall erteilt werden, m. a. W., sofern sich ein Erfordernis für die Weitergabe der Adoptionseignungsberichte ergibt, sind die Bewerber hierüber zu unterrichten – sofern die Bitte um Weiterleitung nicht von ihnen selbst ausgeht – und um ihr Einverständnis in Schriftform zu bitten. Von dieser gesetzlichen Anforderung kann auch dann nicht abgegangen werden, wenn die Einholung der Einwilligung im Einzelfall mit einem erheblichen Verwaltungsaufwand verbunden sein sollte. Die – ebenfalls beabsichtigte – Ermöglichung des Zugangs anderer Adoptionsvermittlungsstellen zu den kompletten Akten hielt der LfD grundsätzlich nicht für einwilligungsfähig, weil der Gewährung des Zuganges die Prüfung vorausgehen muß, welche der in den Akten enthaltenen Informationen für den Übermittlungsempfänger erforderlich sind.

Weitere Anmerkungen des LfD bezogen sich auf die Sensitivität einzelner Fragen, die beispielsweise prägende Begegnungen und Erlebnisse, angenehme und unangenehme Erinnerungen an Kindheit und Jugend und die Religionsausübung betrafen. Er wies in seiner Stellungnahme darauf hin, daß die routinemäßige Erfassung solcher Informationen in einem Fragebogen – mit anschließender automatisierter Verarbeitung – auch mit der Zustimmung der Betroffenen als unverhältnismäßiger Eingriff in das Recht auf informationelle Selbststimmung anzusehen ist. Dabei hat er berücksichtigt, daß die Beantwortung oder Nichtbeantwortung angesichts der besonderen Situation, in der sich Adoptionsbewerber und künftige Pflegeeltern befinden, nicht als freiwillig angesehen werden kann. Die Betroffenen müssen davon ausgehen, daß eine Nichtbeantwortung oder ausweichende Beantwortung für sie nachteilig ist und werden deshalb die Fragen möglichst gewissenhaft und sorgfältig beantworten, auch wenn sie diese als zu weitgehend empfinden. Die Frage nach der Religionsausübung ist überdies im Blick auf den Schutz der Bekenntnisfreiheit (Art. 140 GG i. V. m. Art. 136 Sätze 3 und 5 Weimarer Reichsverfassung) problematisch. Danach haben Behörden nur insoweit ein Fragerecht, als von der Antwort Rechte und Pflichten abhängen oder eine gesetzlich angeordnete statistische Erhebung dies erfordert.

In der Stellungnahme wurde ausdrücklich darauf hingewiesen, daß keine Bedenken bestünden, wenn für die Adoptionsvermittlung notwendige Informationen, auch soweit sie sehr sensitiver Natur sind, in einem Gespräch mit den Adoptionsbewerbern erhoben und die Folgerungen für die Antragsbearbeitung in einer Zusammenfassung aktenkundig gemacht würden. Die routinemäßige Erfragung, Erfassung, Aufbewahrung (Speicherung) und sonstige Verarbeitung ist indessen auch mit Zustimmung der Betroffenen nicht vertretbar.

Es war ferner anzumerken, daß Fragen zum Gesundheitszustand und zu den Vorstrafen aller Familienmitglieder und sonstiger im Haushalt lebender Personen nur mit Zustimmung der im einzelnen betroffenen Personen zulässig sind. Weitere Empfehlungen des LfD bezogen sich auf den Löschungszeitpunkt gespeicherter Daten.

12 Ausländer

12.1 Datei „Asylbewerbererfassung"

Die Prüfung der von der Zentralen Anlaufstelle für Asylbewerber Rheinland-Pfalz in Ingelheim (ZAST) angemeldeten Datei zeigte erneut die Defizite bei der Regelung des Datenschutzes im Ausländer- und im Asylverfahrensrecht.

Die ZAST war nach dem Landesaufnahmegesetz und nach § 1 der Landesverordnung über die zentrale Anlaufstelle für Asylbewerber vom 2. Juli 1984 für die Aufnahme, die vorübergehende Unterbringung und die weitere Verteilung von Asylbewerbern und Kontingentflüchtlingen zuständig. Sie arbeitete auf ihrem Gelände in Ingelheim mit der Ausländerbehörde der Kreisverwaltung Mainz-Bingen, die dort eine Außenstelle unterhält, zusammen. Bei dieser waren gemäß Artikel 5 a Ziff. 1 des Gesetzes zur Neuregelung des Asylverfahrens vom 26. Juni 1992, BGBl. I S. 1126 die Asylanträge noch bis zum 31. März 1993 zu stellen.

Im April 1992 meldete die ZAST eine Datei „Asylbewerbererfassung" zur Eintragung in das Datenschutzregister an. Die Datei diente sowohl den Zwecken der ZAST als auch denen der Ausländerbehörde im Rahmen ihrer Zuständigkeit. Die Ausländerbehörde erhob und speicherte insoweit alle erforderlichen Daten einschließlich derjenigen, die ausschließlich von der ZAST benötigt wurden, für diese mit.

Nach der Systembeschreibung wurden Eingabeberechtigung, Änderungsberechtigung und Leseberechtigung zu jedem Datum getrennt für die ZAST und die Ausländerbehörde der Kreisverwaltung je nach Art und Aufgabenstellung zugeteilt. Überschreitungen dieser Berechtigungen wurden technisch ausgeschlossen. Damit handelte es sich faktisch um zwei Dateien.

Rechtlich fand auf die Nutzung der Daten durch die ZAST ausschließlich das Landesdatenschutzgesetz Anwendung. Für die Speicherung und Löschung personenbezogener Daten durch die Ausländerbehörden enthält § 80 Abs. 1 des Ausländergesetzes eine Verordnungsermächtigung. In Satz 2 wird der Umfang der Ermächtigung eingeschränkt auf die Personalien einschließlich Staatsangehörigkeit, Anschrift, Angaben zum Paß, über ausländerrechtliche Maßnahmen und über die Erfassung im AZR sowie über frühere Anschriften, die zuständige Ausländerbehörde und über die Abgabe von Akten an eine andere Ausländerbehörde. Die hierauf erlassene Ausländerdateienverordnung (AuslDatVO) bestimmt in § 2 Abs. 1 Ziff. 1b, daß in die Ausländerdatei A die Daten von jedem Ausländer aufgenommen werden, der bei der Ausländerbehörde einen Asylantrag stellt. In § 4 – erweiterter Datensatz – waren unter Ziff. 6 verschiedene asylverfahrensrechtliche Maßnahmen aufgeführt, die in dieser Datei gespeichert sein durften. Insgesamt reichte der Katalog jedoch – wie die Praxis zeigte – bei weitem nicht aus, die auch für das Asylverfahren notwendigen Speicherungen vorzunehmen. Bereits verschiedene in der vorliegenden Anmeldung beschriebene Speicherungen wie Religion, bestimmte Gesundheitsdaten und Angaben über persönliche Beziehungen im Bundesgebiet, wurden von dem Katalog nicht umfaßt. Da dieser einen offensichtlich abschließenden Charakter aufwies, wäre nach herkömmlichen juristischen Auslegungsregeln die Speicherung der nicht umfaßten Arten von Daten unzulässig gewesen. Demgegenüber war jedoch weithin davon ausgegangen worden, daß – unter Berufung auf die Organisationshoheit der Länder – „hilfsweise" die jeweiligen Landesdatenschutzgesetze anzuwenden seien, soweit der Katalog in dem Spezialgesetz nicht greift.

Auch für das Asylverfahren, das bis März 1993 die Antragstellung bei Landesbehörden vorsah, stellt sich die Situation nicht viel anders dar. Das Asylverfahrensgesetz enthält zwar datenschutzrechtliche Regelungen über die Erhebung in § 7 und über die Übermittlung in § 8. Zur Speicherung ist jedoch nichts gesagt. Im Laufe des Gesetzgebungsverfahrens war zeitweise eine Speicherungsbestimmung vorgesehen, wobei das Bundesinnenministerium an eine bestimmte Datei „ASYLON" dachte, dann aber wohl zu dem Ergebnis gekommen sein muß, § 14 BDSG könne hierfür ausreichen. Trotz eindringlicher Forderungen seitens der Datenschutzbeauftragten dieses und anderer Länder nach einer bereichsspezifischen Speicherungsregel ist nichts geschehen. Damit ist die allgemein unter „Schnittstellenproblematik" bekannte Frage auch weiterhin nicht zufriedenstellend gelöst.

Für die genannte Datei war daher, soweit die Ausländerbehörde tätig wurde und das Asylverfahrensgesetz keine Regelung enthielt, das LDatG, für Speicherungen also der Grundsatz der Erforderlichkeit anzuwenden. Da für die Tätigkeit der ZAST ohnehin das allgemeine Datenschutzrecht gilt, kam – jedenfalls für die Erforderlichkeit von Speicherungen – für die Datei insgeamt das Landesdatenschutzgesetz zur Anwendung. Vor diesem Hintergrund ergaben sich allerdings für die Erforderlichkeit der zu speichernden Daten keine Zweifel.

Die Kenntnis der Religion war im Blick auf Unterbringung und Verpflegung erforderlich. Die Kenntnis von Angehörigen und von anderen persönlichen Bindungen innerhalb Deutschlands wurde für die Verteilung benötigt. Die Notwendigkeit der Speicherung bestimmter Gesundheitsdaten folgte aus der Untersuchungspflicht nach dem neuen § 62 Abs. 2 AsylVerfG. Sie waren von der hier verwendeten Art her ohnehin wenig sensibel. Die erste Speicherung unterschied nur nach einem Schlüssel zwischen „unbedenklich", „Verteilung nur nach Rücksprache" und „z. Z. keine Verteilung möglich". Zusätzsätzliche Gesundheitsdaten wurden nicht gespeichert. Das Ergebnis der Untersuchung sollte sich in einem verschlossenen Umschlag bei den personenbezogenen Akten befinden.

Die Speicherungsdauer der erfaßten Daten wurde auf die Empfehlung des LfD hin vom Ministerium für Arbeit, Soziales, Familie und Gesundheit in Anlehnung an die bestehenden Bestimmungen im Ausländerrecht von 30 auf zehn Jahre herabgesetzt. Eine kürzere Löschungsfrist für Gesundheitsdaten erwies sich als nicht erforderlich, da Ergebnisse der Gesundheitsuntersuchung nicht an die ZAST mitgeteilt und somit nicht erfaßt werden.

Ab dem 1. April 1993 ist die ZAST Ingelheim aufgelöst worden. An ihre Stelle sind nach den Vorschriften des Asylverfahrensgesetzes (§§ 44 ff.) drei Aufnahmeeinrichtungen (AfA) in Ingelheim, Trier und Neustadt getreten. Deren Aufgabe ist es, die Asylbegehrenden im Rahmen ihrer Zuständigkeit aufzunehmen und bis zur Entscheidung über den Asylantrag durch die Außenstelle des Bundesamtes zur Anerkennung ausländischer Flüchtlinge (BAFl) unterzubringen. Nach der Entscheidung durch das BAFl erläßt die jeweilige AfA die Zuweisungsentscheidung im Rahmen der landesinternen Verteilung (§ 50 AsylVfg). Zur Vereinfachung des Verfahrens haben die AfA Trier und AfA Neustadt ein Programm zur Erfassung, Aktualisierung und Auswertung der Daten von Asylbegehrenden erstellen lassen.

Zur Klärung des Verbleibs von Asylbegehrenden bei Anfragen berechtigter Dritter wird eine DV-Anbindung der einzelnen AfAs untereinander mit der Möglichkeit des lesenden Zugriffs für erforderlich gehalten. Über die Art der technischen Realisierung der DV-Anbindung ist derzeit noch nicht entschieden. Nach endgültiger Klärung wird der Landesbeauftragte eingeschaltet.

Die Ausländerbehörde muß im Rahmen des Asylverfahrens ab dem 1. April 1993 nur noch die aufenthaltsbeendenden Maßnahmen durchführen. Die Zugriffsmöglichkeit der Kreisverwaltung als Ausländerbehörde bei der AfA Ingelheim ist für die Bearbeitung von Altfällen vorübergehend noch erforderlich. Derzeit wird vom Ministerium für Arbeit, Soziales, Familie und Gesundheit noch geprüft, inwieweit der Zugriff auf die gespeicherten Daten im Rahmen des Asylverfahrens ab dem 1. April 1993 im bisherigen Umfang weiterhin erforderlich ist.

Nach § 2 Landesaufnahmegesetz i. V. m. Nr. 4 ff. der VV zur Durchführung des Landesaufnahmegesetzes erstattet das Landesamt für Jugend und Soziales den kommunalen Gebietskörperschaften nach Überprüfung der Ordnungsmäßigkeit die Kosten, die aus Leistungen des BSHG und dem Gesetz über Jugendwohlfahrt für Asylberwerber und Kontingentflüchtlinge entstehen. Hierfür werden dem Landesamt die Zuweisungsverfügung und jede Statusveränderung mitgeteilt. Dies erfolgt derzeit in Form von formularmäßigen Mitteilungen. Alle Erstattungsanträge der kommunalen Gebietskörperschaften werden vom Landesamt für Jugend und Soziales überprüft. Zur Vermeidung von Differenzen ist beabsichtigt, die Überprüfung der Abrechnungen mit Hilfe eines Online-Zugriffs (nur lesend) auf die bei der AfA Ingelheim gespeicherten Daten zu erleichtern und zu beschleunigen. Ein Zugriff wird ausschließlich auf die bereits verteilten Asylbewerber ermöglicht werden. Der dafür erforderliche Datenumfang beschränkt sich auf die Daten, die in der Verteilungsverfügung ohnehin bereits enthalten sind.

Eine abschließende Beurteilung kann erst nach Kenntnis des genauen Konzepts erfolgen.

12.2 Ausländerzentralregistergesetz ad calendas graecas?

Im 13. Tb. wurde unter Tz. 12.1 zu einem Referentenentwurf des Bundesinnenministeriums für ein Ausländerzentralregistergesetz ausführlich Stellung genommen. Der Entwurfsstand ist auch heute noch der gleiche. Wann mit einer überarbeiteten Fassung oder gar mit einem Regierungsentwurf zu rechnen ist, ist nicht bekannt.

Angesichts der Zahl der in der Bundesrepublik lebenden Ausländer und der Verarbeitung sensibler Daten durch das Ausländerzentralregister ist es nicht mehr hinnehmbar, hierfür als einzige Rechtsgrundlage das Gesetz über die Errichtung des Bundesverwaltungsamtes aus dem Jahre 1959 anzuwenden.

Abgesehen von der Unzumutbarkeit für die Ausländerverwaltungen ist es auch gegenüber den in Deutschland lebenden Ausländern kaum noch zu vertreten, daß sie ständig die mit dem Betrieb des Registers verbundenen Eingriffe in das auch ihnen zustehende Recht auf informationelle Selbstbestimmung ohne eine transparente Rechtsgrundlage hinnehmen müssen, aus der sie ersehen könnten, was, wann und von wem über sie gespeichert wird und ggf. welche Rechte sie hierbei haben.

Der LfD hat das Gesetz mehrfach an den verschiedensten Stellen angemahnt.

12.3 Ausländerdaten an Ausländerbeauftragte?

Eine Stadtverwaltung fragte, ob der dortige Ausländerbeauftragte Namen und Anschriften der in seinem Bereich ansässigen Ausländer erhalten könne, um durch Kontaktaufnahme die im Gesetzentwurf der Landesregierung zur Änderung kommunalrechtlicher Vorschriften vorgesehene Wahl des Ausländerbeirates vorbereiten zu können. Dabei geht es nicht um die verwaltungsmäßige Durchführung der Wahl selbst, sondern um vielfältige Formen der Ansprache bis hin zur Einladung zu Veranstaltungen. Die im Melderegister enthaltenen Daten eignen sich hierfür weniger, da dort beispielsweise Einbürgerungen

mitunter zu keiner Berichtigung führen, was zur Folge haben könnte, daß inzwischen eingebürgerte deutsche Staatsangehörige unzutreffend als Ausländer angeschrieben werden. Überflüssiger Verwaltungsaufwand, Portokosten und die Beantwortung von Rückfragen wären unvermeidbar. Die Adressen könnten praktisch nur dem bei der zuständigen Ausländerbehörde geführten Register entnommen werden.

Personenbezogene Daten von Ausländern sind durch das Recht auf informationelle Selbstbestimmung ebenso geschützt wie die von Deutschen; ihre Übermittlung durch öffentliche Stellen setzt nach dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 eine ausreichende, bestimmte und normenklare Rechtsgrundlage voraus.

Das Ausländergesetz sieht in § 79 Übermittlungen durch Ausländerbehörden im wesentlichen nur bei Verstößen gegen arbeits- und sozialrechtliche Bestimmungen vor. Soweit ergänzend das allgemeine Datenschutzrecht, hier das LDatG, heranzuziehen ist, wäre dessen § 6 Abs. 1 zu prüfen, der die Übermittlung an Behörden und sonstige öffentliche Stellen zuläßt, wenn dies zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist. Da die Übermittlung durch die Ausländerbehörde zu deren Aufgabenerfüllung nicht erforderlich ist, käme es auf den Aufgabenbereich der oder des Ausländerbeauftragten an. Dieser ist bislang jedoch nicht normativ definiert. In diesem Zusammenhang würde sich jedoch dann die weitere Frage stellen, ob für die Erfüllung bestimmter Aufgaben die Übermittlung von Anschriften aus dem Ausländerregister überhaupt erforderlich ist. Soweit bisher von Ausländerbeauftragten der Kontakt zu Ausländern gesucht wurde, beispielsweise im Wege der Einladung zu Veranstaltungen, wurden in den dem LfD bekannten Fällen die fertigen Einladungen der Ausländerbehörde übergeben und von dieser anhand der dort vorhandenen Adressen versandt. Die Übermittlung an Ausländerbeauftragte war insoweit nicht erforderlich. Dieser schon in der Vergangenheit von der DSK für zulässig erachtete Weg erscheint auch heute noch als geeignet.

12.4 Ausländische Botschaft ersucht um Listen mit den Adressen ihrer in Deutschland lebenden Staatsbürger

Die Botschaft eines nordafrikanischen Staates ersuchte im Berichtszeitraum mehrere Innenministerien, darunter das Ministerium des Innern und für Sport Rheinland-Pfalz, um eine listenmäßige Zusammenstellung ihrer in dem jeweiligen Bundesland lebenden Staatsangehörigen, einschließlich der vollständigen Anschrift. Praktisch könnte eine solche Gruppenauskunft nur vom Ausländerzentralregister (AZR), zumindest aber mit dessen Unterstützung erteilt werden, wobei es noch schwierig sein könnte, die Auskunft mit den gegenwärtigen Anschriften der Betroffenen zu versehen. Die derzeit für das AZR geltenden Verfahrensregeln lassen eine derartige Gruppenauskunft nicht zu. Der immer noch nicht verabschiedete Entwurf eines AZR-Gesetzes schließt nach gegenwärtigem Stand Gruppenauskünfte an Behörden anderer Staaten ausdrücklich aus. Das Landesmeldegesetz fordert für Gruppenauskünfte das Vorliegen eines öffentlichen Interesses (§ 34 Abs. 3 Satz 1), das hier wohl ausscheiden dürfte. Außerdem wäre vor einer möglichen Übermittlung an ausländische Stellen zu prüfen, ob die vorgeschriebene Zweckbindung (§ 34 Abs.4) sichergestellt ist.

Schließlich wären die Betroffenen zuvor im Rahmen der nach § 7 Landesmeldegesetz vorgesehenen Prüfung, ob ihre schutzwürdigen Interessen beeinträchtigt werden, anzuhören. In die Prüfung wäre einzubeziehen gewesen, ob in jedem einzelnen Fall eine Auskunftssperre nach § 34 Abs. 5 LMG zu beachten war.

Das Ministerium des Innern und für Sport hatte das Ersuchen bereits vor der Anfrage des LfD abgelehnt. Der Vorgang zeigt erneut die Dringlichkeit, das Gesetz über das Ausländerzentralregister nun endlich zu verabschieden.

12.5 Zwangsweise ärztliche Untersuchung von Asylsuchenden

Die Zulässigkeit einer zwangsweisen ärztlichen Untersuchung von Asylsuchenden wurde in der Vergangenheit kontrovers diskutiert. Die DSK forderte wegen des Eingriffscharakters derartiger Untersuchungsmaßnahmen die Schaffung einer bundesrechtlichen Grundlage und wurde mit dieser Forderung durch den Bundesbeauftragten für den Datenschutz und später auch durch das Ministerium für Umwelt und Gesundheit unterstützt (vgl. 13. Tb., Tz. 12.4). Im Berichtszeitraum hat sich die rechtliche Situation aufgrund des Gesetzes zur Neuregelung des Asylverfahrens vom 26. Juni 1992 (BGBl. I S. 1126) geändert. Das Asylverfahrensgesetz enthält nunmehr einen die Gesundheitsuntersuchung regelnden § 62:

„(1) Ausländer, die in einer Aufnahmeeinrichtung oder Gemeinschaftsunterkunft zu wohnen haben, sind verpflichtet, eine ärztliche Untersuchung auf übertragbare Krankheiten einschließlich einer Röntgenaufnahme der Atmungsorgane zu dulden. Die oberste Landesgesundheitsbehörde oder die von ihr bestimmte Stelle bestimmt den Umfang der Untersuchung und den Arzt, der die Untersuchung durchführt.

(2) Das Ergebnis der Untersuchung ist der für die Unterbringung zuständigen Behörde mitzuteilen."

Das Ministerium für Arbeit, Soziales, Familie und Gesundheit ließ für Zwecke der Datenerhebung und -übermittlung einen Formularsatz entwickeln, gegen den datenschutzrechtliche Einwendungen nicht zu erheben waren.

13 Finanzverwaltung

13.1 Abgabenordnung (AO)

Im letzten Tätigkeitsbericht wurde detailliert dargestellt, welche datenschutzrechtliche Ergänzung der AO geplant war.

Nunmehr hat sich ergeben, daß der Bundesminister der Finanzen kein Interesse mehr an der Einfügung datenschutzrechtlicher Regelungen in die AO hat.

Hintergrund dieser Meinungsänderung dürfte der im letzten Tätigkeitsbericht dargestellte Diskussionsstand sein: Ursprünglich hatte das Bundesfinanzministerium beabsichtigt, in der AO den Datenschutzstandard gegenüber dem allgemeinen Datenschutzrecht zurückzuschrauben und ergänzend für die Landesfinanzverwaltungen die Anwendung des seinerzeit datenschutzrechtlich noch unzureichenden Bundesdatenschutzgesetzes vorzuschreiben.

Nachdem dieses Ziel nach der Novellierung des Bundesdatenschutzgesetzes und aufgrund des Widerstandes der Datenschutzbeauftragten nicht erreicht werden konnte, ist für das Bundesfinanzministerium der Grund einer datenschutzrechtlichen Ergänzung der AO entfallen.

Die Anliegen der Datenschutzbeauftragten waren und sind demgegenüber, in die AO bereichsspezifische Datenschutznormen einzufügen, die den Datenschutz im Besteuerungsverfahren im Vergleich zum allgemeinen Datenschutzrecht genauer und angemessener regeln, oder vorhandene Regelungen in der AO datenschutzfreundlicher auszugestalten.

Der LfD ist allerdings der Auffassung, daß auch auf der Basis des allgemeinen Datenschutzrechtes (insbesondere dann, wenn auch das Landesdatenschutzgesetz dem Standard des Volkszählungsurteils des Bundesverfassungsgerichts angepaßt sein wird) die Regelungen im Grundsatz ausreichen, um die bei der Finanzverwaltung bestehenden datenschutzrechtlichen Fragen zufriedenstellend zu lösen. Die im 13. Tb. genannten Änderungen einzelner Regelungen der AO bleiben jedoch ein Anliegen, das der LfD nach wie vor mit Nachdruck unterstützt.

13.2 Darf es in den Finanzämtern Personen geben, die auf Knopfdruck alles über jeden Steuerbürger erfahren können?

Anläßlich örtlicher Feststellungen im Bereich der Finanzämter des Landes Rheinland-Pfalz ist der LfD auf die Frage des Umfangs der finanzamtsinternen Zugriffsbefugnisse der Bediensteten auf Daten der Steuerpflichtigen aufmerksam geworden. Im Bereich des integrierten automatisierten Besteuerungsverfahrens (IABV), das bundeseinheitlich entwickelt und in vielen (allerdings nicht in allen) Bundesländern eingesetzt wird, hat sich ergeben, daß folgende Zugriffsbefugnisse bestehen, deren Erforderlichkeit unter datenschutzrechtlichen Gesichtspunkten zunächst zweifelhaft erscheint:

Für jeden Steuerpflichtigen werden bestimmte Stammdaten gespeichert, wie Name, Anschrift, Religionszugehörigkeit, Familienstand, Kontoverbindung. Unter den Suchbegriffen des Namens bzw. der Steuernummer können außer den genannten Stammdaten auch die zuletzt festgesetzten Steuerbeträge, aufgegliedert nach einzelnen Steuerarten, die derzeit offenen Steuerbeträge und die demnächst fällig werdenden Steuerbeträge abgerufen werden. Soweit diese Informationen nur den Sachbearbeitern zur Verfügung stehen, die – etwa im Veranlagungsbereich – für die jeweiligen Steuerpflichtigen auch zuständig sind, ergeben sich hiergegen keine Bedenken. Problematisch erscheint dem LfD allerdings, daß für Arbeitsbereiche, die zentrale Funktionen für das gesamte Finanzamt wahrnehmen, Zugriffsbefugnisse auf die Daten aller Steuerpflichtigen, die dem jeweiligen Finanzamt zugeordnet werden, bestehen. So besitzt z. B. jeder Sachbearbeiter der Vollstreckungsstelle die technische (Lese-)Zugriffsbefugnis auf die Daten aller Steuerpflichtigen (im o. g. Umfang), unabhängig davon, ob ein konkreter Vorgang im Rahmen der Vollstreckung zu bearbeiten ist oder nicht. Eine am Erforderlichkeitsgrundsatz orientierte Zugriffsbefugnis müßte wohl auf diejenigen Steuerpflichtigen beschränkt sein, bei denen Steuerbeträge nach dem Fälligkeitsdatum noch offen sind.

In verstärktem Ausmaß betreffen ähnliche Bedenken die Steuerfahndungsstellen sowie die Bußgeld- und Strafsachenstellen. Die Bedenken sind hier deshalb noch gewichtiger, weil diese Stellen jedenfalls in Rheinland-Pfalz grundsätzlich nicht nur jeweils für ein einziges Finanzamt zuständig sind, sondern ihre Aufgaben konzentriert jeweils für ca. drei bis vier Finanzämter wahrnehmen. Ihrem räumlich ausgedehnten Zuständigkeitsbereich entspricht dann auch die genannte Zugriffsbefugnis auf die Steuerpflichtigen aller Finanzämter, für die diese Stellen jeweils zuständig sind. Auch diese Stellen haben zwar nur einen Lesezugriff in dem genannten Umfang. Aber auch daraus ergibt sich eine weit über das Erforderliche hinausgehende Zugriffsmöglichkeit, da nur ein geringer Prozentsatz der Steuerpflichtigen mit der Strafsachenstelle oder mit der Steuerfahndungsstelle in Kontakt kommen wird. Fraglich ist, ob die bestehenden Protokollierungen von Abfragen als ausreichende Korrektur des grundsätzlich über das Erforderliche hinausgehenden Zugriffsprofils anzusehen sind.

Der LfD hat zunächst das Ministerium um Stellungnahme gebeten. Änderungen an diesem geschilderten Verfahren ließen sich aber wohl – schon wegen des Programmierverbunds – nur bundeseinheitlich durchsetzen. Insofern hat er auch die anderen Datenschutzbeauftragten informiert und um entsprechende Aktivitäten gebeten. Ein Ergebnis liegt bislang noch nicht vor.

Anläßlich örtlicher Feststellungen wurde auch die datenschutzrechtlich bedeutsame Frage, wer in welchem Umfang Zugriff auf die (spezifisch in Rheinland-Pfalz entwickelten) „DAVID"-Dateien innerhalb der Finanzämter haben darf (zum Begriff dieser Dateien vgl. 12. Tb., Tz. 14.1), gegenüber dem Ministerium problematisiert. In diesen Dateien werden die Eingabespeicherungen aus den Steuererklärungen vorgehalten. Grundsätzlich hat der LfD das Verfahren begrüßt, die Zugriffsrechte auf die entsprechenden Dateien an den Funktionsstellen des Finanzamts zu orientieren.

Insbesondere die Freischaltung von Zugriffen für die Betriebsprüfung, für die Steuerfahndung sowie die Bußgeld- und Strafsachenstellen durch den jeweiligen Sachbearbeiter des Veranlagungsbezirks nach Erteilung eines Prüfauftrages bzw. nach Vorliegen einer entsprechenden Anforderung trägt aus datenschutzrechtlicher Sicht dem Erforderlichkeitsgrundsatz vorbildlich Rechnung.

Problematisch in diesem Zusammenhang erscheint allerdings der Umfang des Lesezugriffs des Finanzamtsvorstehers. Dieser hat nach den dem LfD vorliegenden Informationen einen umfassenden Lesezugriff auf die DAVID-Dateien seines gesamten Zuständigkeitsbereichs. Es ist fraglich, ob seine Aufsichtsfunktionen den Zugriff in diesem Umfang wirklich erfordern. In der Praxis jedenfalls scheint ein erheblicher Prozentsatz der Vorsteher bzw. Vorsteherinnen die vorhandenen Zugriffsmöglichkeiten nicht zu nutzen.

Unabhängig von der Frage der Erforderlichkeit der Einräumung einer solchen umfassenden Zugriffsbefugnis ist aber auch zu fragen, ob dann, wenn diese Abfragemöglichkeiten eingeräumt werden sollen, nicht durch Maßnahmen des technischen und organisatorischen Datenschutzes sicherzustellen ist, daß eine zweckwidrige Nutzung zumindest erschwert wird. Hierzu gehört jedenfalls eine stichprobenweise Protokollierung auch des Anlasses von Abfragen. Das Landesdatenschutzgesetz wird künftig eine solche stichprobenweise Protokollierung zwingend vorsehen (§ 9 Abs. 2 Nr. 6 des Entwurfs eines Landesdatenschutzgesetzes, Stand: 15. Januar 1993).

Aus der Sicht des LfD dürften die bislang bekannten Protokollierungen im Bereich des Lesezugriffs auf DAVID-Dateien hier unzureichend sein.

Vergleichbare Fragen – die allerdings eine geringere Dringlichkeit besitzen – stellen sich im Bereich des Lesezugriffs der Sachgebietsleiter. Das Ministerium hat bislang hierzu noch nicht Stellung genommen.

13.3 Welche Arbeiten dürfen private Datenverarbeiter den Finanzämtern abnehmen, ohne daß das Steuergeheimnis ausgehöhlt wird?

Die Finanzverwaltung hat vertraglich einer privaten Firma die Erfassung der steuerrelevanten Daten der Steuererklärung auf Medien der EDV übertragen. Von dieser Übertragung sind insbesondere Steuererklärungen aus dem Zuständigkeitsbereich des Finanzamts Ludwigshafen, aber auch Steuererklärungen von den übrigen Finanzämtern des Landes betroffen. Die sogenannten „Arbeitsspitzen" werden dadurch abgefangen, daß – in Zeiten verstärkten Arbeitsanfalls – entsprechende Erfassungsarbeiten der Privatfirma übertragen werden. Gegenstand der Datenerfassung sind Umsatzsteuer- und Einkommensteuerdaten.

Mit einer solchen Verlagerung der Datenerfassung auf eine private Firma ist verbunden, daß private Arbeitnehmer dieser Firma Daten zur Kenntnis nehmen, die dem Steuergeheimnis unterliegen. Diese Arbeitnehmer unterliegen grundsätzlich nicht der Strafdrohung des § 355 StGB (Verletzung des Steuergeheimnisses), Steuererklärungsvordrucke mit äußerst sensiblen Daten verlassen den Bereich der Finanzverwaltung und kommen in den privaten Bereich.

Der LfD hat dieses Verfahren wie folgt bewertet:

a) Zunächst hat er darauf hingewiesen, daß Datenverarbeitungsvorgänge solch sensibler Art nur ausnahmsweise Privaten übertragen werden dürfen. Im Regelfall sind diese Tätigkeiten dem öffentlichen Dienst und – im Zusammenhang mit dem Steuergeheimnis – der Finanzverwaltung vorbehalten.

   Der LfD hat die Finanzverwaltung wiederholt um Prüfung gebeten, ob die Beauftragung einer privaten Firma angesichts der Arbeitssituation in der Finanzverwaltung einerseits, aber auch angesichts der Sensitivität der Daten und der hier vorliegenden Gefährdung des Steuergeheimnisses andererseits tatsächlich als unabdingbar anzusehen ist.

   Die insoweit vorgetragenen Argumente der Finanzverwaltung ließen sich nicht widerlegen.

b) Ergänzend hat der LfD jedoch örtliche Feststellungen bei dem privaten Auftragnehmer durchgeführt, um das Umfeld der Datenerfassung beurteilen zu können. Auch dieses Umfeld ist sicherlich wichtig, um den Eingriff in das informationelle Selbstbestimmungsrecht der Bürger in diesem Zusammenhang gewichten zu können.

Grundsätzlich haben diese örtlichen Feststellungen keine Bedenken aus technischer und organisatorischer Sicht gegen eine Verlagerung der Datenverarbeitung auf private Stellen ergeben. Eine Reihe von Verbesserungsvorschlägen wurden zwar gemacht, die Zuverlässigkeit des Unternehmens insgesamt war jedoch nicht in Frage zu stellen.

Unabhängig davon ist der Landesbeauftragte für den Datenschutz der Auffassung, daß Anstrengungen unternommen werden müssen, um künftig ohne eine solche Beauftragung Privater in diesem Zusammenhang auskommen zu können.

13.4 Darf der Vollstreckungsbeamte Datenbanken pfänden und veräußern?

Bei dem Pächter einer Videothek hat das Finanzamt Vollstreckungsmaßnahmen durchgeführt. Im Rahmen dieser Vollstreckungsmaßnahmen wurde ein PC mit der Festplatte, auf der sich insbesondere Kundendaten befunden haben (Namen, Anschriften, entliehene Medien), freihändig an einen anwesenden Erwerber veräußert. Das Ministerium der Finanzen hat diesen Sachverhalt bestätigt. Es hat zudem erklärt, für die Zukunft solle dieses Problem so gelöst werden, daß in vergleichbaren Fällen vor Weitergabe bzw. Verwertung des Computers die darauf gespeicherten Daten – gegebenenfalls nach Erstellung einer Sicherungskopie – gelöscht werden.

In der Verwertungshandlung des Finanzamts, im freihändigen Verkauf des Computers inklusive der Festplatte und der darauf gespeicherten Daten an einen privaten Dritten, ist eine eigenständige Datenübermittlung durch eine öffentliche Stelle zu sehen. Als Veräußerer ist das Finanzamt aufgetreten, nicht aber der Pächter der Videothek oder die Verpächterin, die nachtäglich Eigentumsansprüche geltend macht. Dementsprechend lag in der konkreten Veräußerung eine Datenübermittlung durch das Finanzamt an den privaten Erwerber. Diese war und ist unzulässig, da nicht ersichtlich ist, inwiefern die Übermittlung der Daten der privaten Kunden der Videothek zur Erfüllung der Aufgaben des Finanzamtes (Verwertung des PC) erforderlich gewesen ist. Die Einwilligungserklärung des Besitzers des PC in die Weitergabe war in diesem Zusammenhang unerheblich. Betroffen von der Datenweitergabe waren die Kunden der Videothek, die weder um Einwilligung gefragt wurden noch eine solche erteilt haben.

Die in der beschriebenen Verwertunghandlung liegende Datenübermittlung war aus datenschutzrechtlicher Sicht zu beanstanden, der LfD hat dies gegenüber dem Ministerium getan.

Das Ministerium hat in der Folge eine allgemeine Weisung erlassen, wonach derartige Pfändungsmaßnahmen nur nach Berichterstattung gegenüber der Oberfinanzdirektion durchgeführt werden dürfen. Der LfD hat in diesem Zusammenhang Grundsätze entwickelt, die bei entsprechenden Verwertungsmaßnahmen zu beachten sind, und sowohl das Ministerium der Finanzen wie das Ministerium der Justiz gebeten, die Praxis entsprechend zu informieren.

13.5 Eingaben

13.5.1 Der verwechselte Steuerpflichtige

Ein Steuerpflichtiger war sehr erstaunt, als er seine an das Finanzamt zusammen mit der Steuererklärung übersandten Originalbelege zurückerhielt und dabei Unterlagen fand, die er noch nie gesehen hatte. Es waren Kontoauszüge und Quittungen, die eine andere Person betrafen und über deren Verhältnisse der Beschwerdeführer nun jedenfalls zum Teil recht gut unterrichtet war.

Aus der Stellungnahme des betroffenen Finanzamts ergab sich, daß die Belege, die mit dem Steuerfall nichts zu tun hatten, entweder bereits beim Eingang der Steuererklärung in der Poststelle oder später im „Arbeitnehmerbezirk" zu der Steuererklärung des Beschwerdeführers gelangt sind. Das Finanzamt hat dazu erklärt, daß bei der Vielzahl der eingehenden Steuererklärungen und Unterlagen, die häufig unzureichend gesichert und lose in den Erklärungsvordrucken oder in den Briefumschlägen lägen und die dann vom Umschlag befreit in Postmappen über den Sachgebietsleiter den zuständigen Sachbearbeiter erreichten, es vorkommen könne, daß Belege herausfallen oder ineinanderrutschen.

Nachdem das hier bestehende erhebliche Risiko erkannt sei, seien die Mitarbeiter dazu angehalten worden, bei der Zuordnung loser Belege sehr sorgfältig zu arbeiten, damit es künftig nicht mehr zu solchen fehlerhaften Zuordnungen wie in diesem Fall kommen kann. Der Vorsteher habe diesen Vorfall zum Anlaß genommen, die Poststelle und auch die Mitarbeiter in den Steuerbezirken nochmals auf sorgfältigen und umsichtigen Umgang mit der Eingangspost hinzuweisen.

Der LfD geht davon aus, daß aufgrund dieser Maßnahmen Vorfälle der hier eingetretenen Art künftig nicht mehr vorkommen. Bei diesem Vorgang dürfte es sich – jedenfalls nach bisheriger Kenntnis – um einen einmaligen Fall gehandelt haben.

13.5.2 Die ins Leere gehende Forderungspfändung

Ein Bürger mit hohen Steuerschulden beschwerte sich darüber, daß das Finanzamt bei einer Firma eine Lohnpfändung vorgenommen hätte, die er gar nicht kenne und mit der er nie in Beziehung gestanden habe. In der Pfändungsverfügung wären aber seine Steuerschulden genannt worden, über die diese Firma nun Bescheid wisse.

Die Aufklärung durch den LfD ergab, daß das Vollstreckungsfinanzamt auf folgende Weise die – unzutreffende – Information über den angeblichen Arbeitgeber erhalten hatte: Es hatte ein Finanzamt in einem anderen Bundesland um Amtshilfe gebeten. Der dortige Vollziehungsbeamte hatte ausweislich eines Protokolls auch einen Nachbarn des Betroffenen befragt. Dieser hatte erklärt, die fragliche Firma sei nunmehr der Arbeitgeber des Vollstreckungsschuldners.

Daraufhin führte das rheinland-pfälzische Finanzamt die Lohnpfändung bei dieser Firma durch.

Aus datenschutzrechtlicher Sicht war dies wie folgt zu beurteilen: Die Finanzbehörde hat auch im Rahmen der Vollstreckung den Sachverhalt von Amts wegen aufzuklären und zu ermitteln. Dabei bedient sie sich der Beweismittel, die sie nach pflichtgemäßem Ermessen für erforderlich hält (§§ 88, 92 AO, anzuwenden auch im Vollstreckungsverfahren gem. § 249 Abs. 2 AO; vgl. auch Abschnitt 20 der Vollstreckungsanweisung).

Es ist also zu fragen, ob das pflichtgemäße Ermessen im vorliegenden Fall geboten hätte, die Information durch das Finanzamt des anderen Bundeslandes noch zu erhärten. Dabei war sicher zu berücksichtigen, daß eine ins Leere gehende Pfändungsverfügung gegenüber einem Unbeteiligten als Drittschuldner einen Eingriff in das Steuergeheimnis des betroffenen Steuerschuldners mit sich bringt. Auf der anderen Seite war zu berücksichtigen, daß bei der Durchführung von Vollstreckungsmaßnahmen angesichts der häufig vorliegenden Eilbedürftigkeit entsprechende Maßnahmen zeitnah und ohne vermeidbare Verzögerungen erfolgen müssen, um dem Schuldner keine Gelegenheit zu geben, Vermögenswerte zu beseitigen bzw. den Zugriff auf sie zu erschweren. Dafür spricht auch § 91 Abs. 2 Nr. 5 AO, wonach eine Anhörung vor der Durchführung eines Verwaltungsaktes dann nicht geboten ist, wenn Maßnahmen in der Vollstreckung getroffen werden sollen. Der Gesichtspunkt der Beschleunigung und der Vereinfachung des Verfahrens durchzieht die Regelungen der Vollstreckung nach der Abgabenordnung durchgängig. Angesichts der erheblichen Höhe der im konkreten Fall noch zu vollstreckenden Forderung des Finanzamtes war auch aus datenschutzrechtlicher Sicht nicht zu fordern, daß weitere – möglicherweise zeitaufwendige – Aufklärungsmaßnahmen getroffen wurden, die ohnehin keine absolute Gewißheit über das Bestehen eines entsprechenden Arbeitsverhältnisses hätten erbringen können. Die verbindliche, im Rechtsverkehr bedeutsame Klärung dieser Frage konnte am schnellsten und wirksamsten durch die Abgabe der Drittschuldnererklärung der Stelle, die als Arbeitgeber vermutet wurde, erreicht werden. Auch andere Wege der Klärung hätten zudem mindestens erfordert, die betroffene Firma zu befragen. Auch dann hätten vom Steuergeheimnis geschützte Informationen übermittelt werden müssen.

Unter Berücksichtigung dieser Gesichtspunkte war auch aus datenschutzrechtlicher Sicht das Vorgehen der Vollstreckungsstelle des Finanzamtes im vorliegenden Fall nicht zu beanstanden.

13.5.3 Die gläsernen Taschen der Freiberufler in Fremdenverkehrsgemeinden

Freiberufler (insbesondere Zahnärzte) haben sich im Berichtszeitraum in größerer Zahl an den LfD gewandt und sich dagegen gewehrt, daß die Gemeinden im Zusammenhang mit der Festsetzung der Fremdenverkehrsabgabe den Gesamtumsatz ihrer Praxis erfahren. Dies mag unverhältnismäßig erscheinen, ist aber auch aufgrund der Rechtsprechung des OVG Koblenz nicht angreifbar, wenn die gemeindlichen Satzungen dies vorsehen. Erneut wurde auch problematisiert, ob im Zusammenhang mit der Erhebung von Fremdenverkehrsbeiträgen die Finanzämter in rechtlich zulässiger Weise Umsatzdaten eines Steuerpflichtigen an die Gemeinden weitergeben dürfen. Bedenken gründeten sich darauf, daß der Betroffene das Recht habe, an Stelle einer umsatzbezogenen Berechnung die Schätzung zu wählen.

Rechtsgrundlage für die Erhebung von Fremdenverkehrsbeiträgen A ist § 36 Kommunalabgabengesetz in Verbindung mit der jeweiligen gemeindlichen Satzung. Beitragsermittlung und Höhe der Fremdenverkehrsbeiträge sind in dieser Satzung festzulegen (§ 36 Abs. 8 KAG). Eine konkrete Beurteilung hängt also vom Inhalt der jeweiligen Satzung ab.

Unabhängig davon hat der LfD allgemein zu dieser Frage folgendes ausgeführt:

a) Es ist grundsätzlich rechtmäßig, die Berechnung der Höhe des Fremdenverkehrsbeitrages A von dem erzielten Umsatz abhängig zu machen. Dies ist ein Maßstab, der grundsätzlich sachangemessen ist (vgl. hierzu die Ausführungen des OVG Koblenz im Urteil vom 3. Juni 1980, Az.: 6 A 64/79).

b) Für das Verfahren der Ermittlung der Beitragsgrundlagen gilt neben dem Kommunalabgabengesetz die Abgabenordnung (insbesondere §§ 78 bis 133, vgl. § 39 Abs. 1 Nr. 3 Kommunalabgabengesetz). Danach sind die Besteuerungsgrundlagen von Amts wegen zu ermitteln (Amtsermittlungsgrundsatz, § 88 AO). Allerdings dürfen Dritte, auch andere Behörden, erst dann um Auskunft ersucht werden, wenn der Betroffene selbst erfolglos um Auskunft gebeten worden ist bzw. wenn eine entsprechende Anfrage wahrscheinlich nicht zum Erfolg führt (§ 93 Abs. 1 AO). Gerade auch im Zusammenhang mit der Erhebung von Fremdenverkehrsbeiträgen hat bereits die DSK in der Vergangenheit Verfahren (und die diesem Verfahren zugrundeliegenden Satzungen) beanstandet, in denen Datenübermittlungen ohne vorherige Befragung der Beitragspflichtigen unmittelbar vom Finanzamt an die Gemeinde erfolgt sind. Die Mustersatzung über die Erhebung eines Fremdenverkehrsbeitrages A vom 9. November 1979 (MinBl. S. 114) trägt dem bereits Rechnung. Nach § 3 Abs. 2 dieser Mustersatzung ist vorgesehen, daß grundsätzlich der Beitragspflichtige selbst eine Erklärung über die maßgeblichen Berechnungsgrundlagen abgibt.

c) Nach der Systematik des Gebühren- und Steuerrechts gibt es grundsätzlich keine echte Wahlfreiheit zwischen Schätzung und Steuerveranlagung nach den gesetzlichen Besteuerungsgrundlagen. Die Steuerschuld entsteht nach der steuerrechtlichen Dogmatik von Gesetzes wegen, ohne daß es dazu eines Verwaltungshandelns bedürfte. Die Steuererhebungsbehörde stellt diese entstandene Steuerschuld nur fest. Dieser Systematik widerspräche es, von einer Dispositionsbefugnis der Beteiligten in der Weise auszugehen, daß eine Wahlfreiheit bestünde, zur Vermeidung der Umsatzangaben die Schätzung zu wählen. Grundsätzlich kommt eine Schätzung der entstandenen Steuerschuld nur dann in Betracht, wenn objektive Hindernisse die Feststellung der gesetzlich entstandenen Steuerschuld unmöglich machen oder unzumutbar erschweren.

Aus datenschutzrechtlicher Sicht ist dieser dogmatische Ansatz sicherlich überdenkenswert. Gerade wenn – wie im Fall der Fremdenverkehrsbeiträge A – die Beitragshöhe relativ gering und der Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen, der der Beitragsfestsetzung vorausgeht, gewichtig ist, würde es dem informationellen Selbstbestimmungsrecht unter Beachtung des Verhältnismäßigkeitsgrundsatzes eher gerecht werden, eine echte Wahlfreiheit zwischen Schätzung und genauer Steuerfestsetzung aufgrund der Feststellung der Besteuerungsgrundlagen zu ermöglichen.

Dies würde jedoch voraussetzen, daß bezüglich der Fremdenverkehrsbeiträge A nicht auf die Systematik der Abgabenordnung verwiesen wird, sondern gesetzlich ein eigenständiges Verfahren geregelt wird.

Aus der Sicht des LfD wäre eine entsprechende Initiative etwa seitens der Vertretungskörperschaften der freien Berufe zu unterstützen.

14 Wirtschaft und Verkehr

14.1 Vereinfachung des Verfahrensablaufs zwischen Regierungshauptkassen und den Bußgeldstellen für Verkehrsordnungswidrigkeiten

Bei der Vollstreckung von Bußgeldbescheiden durch die Regierungshauptkassen erhielten diese in der Vergangenheit zur Wahrnehmung ihrer Aufgaben folgende Daten: Name und Anschrift des Zahlungspflichtigen, Daten des Bußgeldbescheids, Daten der Mahnung und Vollstreckung, Tattag und Tatort, Kraftfahrzeugkennzeichen, Höhe der einzelnen Beträge und Gesamtbetrag. Fernerhin waren auch die Angaben über die Ist-Beträge bekannt.

Mittels eines Online-Anschlusses (Teilnahme am Landesdatennetz) sollte es für die Regierungshauptkassen künftig möglich sein, Auskünfte über Zahlungspflichtige im Ordnungswidrigkeiten-Verfahren abzurufen. Örtliche Feststellungen ergaben, daß die entsprechende Datei Merkmale enthielt, die für die Vollstreckung von Bußgeldbescheiden durch die Regierungshauptkasse nicht erforderlich sind. Dabei handelte es sich, bezogen auf die geplante Struktur des Datensatzes, um den Zeitpunkt des erstmaligen Einlesens in die Automation, Angaben zum Halter, den Zeitpunkt des Anhörungsverfahrens, das Datum der Verkehrszentralregisteranfrage, das Datum der Verkehrszentralregisterauskunft, das Datum der Verfolgungsverjährung, die Tagebuchnummer, Angaben zu Beweismitteln, die Angabe über die Dauer eines Fahrverbotes und den Namen des den Betroffenen vertretenden Rechtsanwaltes. Die übrigen Feldinhalte des Ordnungswidrigkeiten-Verfahrens (z. B. Name, Vorname, Anschrift und Geburtstag des Betroffenen, Datum der Vollstreckungsverjährung usw.) werden in die den Regierungshauptkassen zur Verfügung gestellte Maske aufgenommen.

Die Feststellungen ergaben, daß eine datenmäßige Überfrachtung vermieden werden kann, wenn jedes einzelne Datenfeld unter dem Aspekt der Relevanz für die Aufgabenerfüllung geprüft wird.

14.2 Mitteilung von Daten aus abgeschlossenen Bußgeldverfahren an eine Handwerkskammer

Im Berichtszeitraum wurde die Frage an den LfD herangetragen, ob die Weitergabe von personenbezogenen Daten an eine Handwerkskammer nach Abschluß von Ordnungswidrigkeiten-Verfahren zur Bekämpfung von Schwarzarbeit datenschutzrechtlich zulässig ist. Eine Kreisverwaltung wurde gebeten, neben der Bußgeldstatistik 1991 eine Auflistung – bestehend aus Name, Anschrift, Bußgeldhöhe und betroffenem Gewerbe – zu übermitteln.

Fraglich war hier, in welchem Umfang die Handwerkskammern gegenüber bestimmten Behörden Amtshilfe in Anspruch nehmen können.

Aus der Pflicht zur Amtshilfeleistung (Art. 35 Abs. 1 GG; § 1 LVwVfG i. V. m. §§ 4, 5 VwVfG) folgt allerdings schon deshalb kein Recht zur Übermittlung personenbezogener Daten, weil die Amtshilfe nicht eigenständige Grundlage für Informationseingriffe in Rechte der Bürger sein kann.

Aus § 6 LDatG könnte unter Umständen ein solches Recht folgen, wenn die fraglichen Daten zur Aufgabenerfüllung der Handwerkskammer erforderlich wären.

Zunächst ist festzustellen, daß die Handwerkskammern im Bereich der Bekämpfung der Schwarzarbeit unter zwei Gesichtspunkten Kompetenzen zum Tätigwerden besitzen:

- Sie können gem. § 16 Abs. 3 Handwerksordnung einen Antrag an die zuständige Behörde auf Untersagung der Handwerksausübung durch einen Schwarzarbeiter stellen.
- In Wahrnehmung ihrer Aufgaben gem. § 91 Abs. 1 Nr. 1 Handwerksordnung, die Interessen des Handwerks zu fördern, sind sie auch befugt, Schwarzarbeiter bei den Stellen anzuzeigen, die zur Verfolgung und Ahndung von Ordnungswidrigkeiten nach §§ 117, 118 Handwerksordnung und § 1 des Gesetzes über die Bekämpfung der Schwarzarbeit zuständig sind. In diesem Zusammenhang umfaßt die Aufgabe der Handwerksorganisationen auch, den zuständigen Verwaltungsbehörden Hinweise auf das Vorliegen von Schwarzarbeit zu geben, zunächst vagen Verdachtsfällen nachzugehen und durch eigene Ermittlungen Erkenntnisse zu gewinnen, die schließlich eine Anzeige bei zuständigen Verfolgungsbehörden rechtfertigen.

Sinn der Regelung in § 16 Abs. 3 Handwerksordnung ist es nicht, der Handwerkskammer das Recht einzuräumen, im Wege der „Deanonymisierung" der Bußgeldstatistik Anträge auf Untersagung des Handwerks zu stellen.

Ebenso läßt sich aus der Befugnis, Schwarzarbeiter bei der zuständigen Behörde anzuzeigen, kein Recht ableiten, personenbezoge Daten aus allen der Bußgeldstatistik zugrundeliegenden abgeschlossenen OWiG-Verfahren zu erhalten und auszuwerten. Bereits begrifflich ist diese Vorgehensweise ausgeschlossen (Anzeige wegen Schwarzarbeit aufgrund eines abgeschlossenen Bußgeldverfahrens wegen Schwarzarbeit).

Nach allem gibt es keine gesetzliche Grundlage für die Übermittlung personenbezogener Daten aus allen abgeschlossenen Ordnungswidrigkeitenverfahren an die Handwerkskammern zur Bekämpfung von Schwarzarbeit.

Etwas anderes muß aber für jene Fälle gelten, in denen die Handwerkskammer selbst Schwarzarbeiter bei den zur Verfolgung und Ahndung von Ordnungswidrigkeiten nach den §§ 117, 118 Handwerksordnung und § 1 des Gesetzes über die Bekämpfung der Schwarzarbeit zuständigen Stellen angezeigt hat. In diesen Fällen muß die Handwerkskammer wissen, was aus ihrer Anzeige geworden ist. Es spricht auch nichts dagegen, daß die Handwerkskammer hier unaufgefordert über das Ergebnis der Verfahren unterrichtet wird.

14.3 Mitteilungen der Polizei an die Führerscheinstellen über Drogenkonsumenten

Nach Auskunft des rheinland-pfälzischen Innenministeriums erfolgt regelmäßig bei Abgabe der Ermittlungsakten an die Staatsanwaltschaft (wenn sich der Verdacht bestätigt hat) eine Mitteilung an die zuständige Straßenverkehrsbehörde, wenn die Polizei im Rahmen der Ermittlungsführung eines Verfahrens wegen Verstoßes gegen das Betäubungsmittelgesetz oder anderweitiger Anlässe feststellt, daß ein Fahrerlaubnisinhaber Konsument harter oder weicher Drogen ist. Grundlage für die Mitteilung sind dann entweder eigene Einlassungen des Betroffenen oder aber vorliegende Sachverständigengutachten. In einem Regierungsbezirk übermittelt die Polizei an die Straßenverkehrsbehörde entsprechende Daten lediglich, soweit der Betroffene wiederholt als Konsument harter oder weicher Drogen in Erscheinung getreten ist.

Es sind keine Fälle bekannt, in denen ausschließlich gefahrenabwehrende Maßnahmen getroffen wurden. Anlaßdelikt ist jeweils ein Verstoß gegen das Betäubungsmittelgesetz. Trifft die Polizei eine Person beim Führen eines Fahrzeuges unter Drogeneinfluß an, so nimmt sie die notwendigen Ermittlungen vor, um den Sachverhalt zu erforschen und stellt den Führerschein sicher bzw. beschlagnahmt ihn. Mit dem Antrag an die Staatsanwaltschaft zum vorläufigen Entzug der Fahrerlaubnis wird in der Regel zugleich die Straßenverkehrsbehörde unterrichtet. Grundlage für diese Mitteilung sind die jeweiligen Feststellungen der Polizeibeamten, die zur Aufnahme der strafrechtlichen Ermittlungen geführt haben. Sie werden durch gutachterliche Untersuchungen ergänzt.

Nach Auffassung des LfD ist es gerechtfertigt, wenn die Polizeidienststellen die Straßenverkehrsbehörden im Falle eines Verstoßes gegen das Betäubungsmittelgesetz über Konsumenten illegaler Drogen unterrichten, sofern der Polizei Erkenntnisse vorliegen, daß diese Personen im Besitz einer Fahrerlaubnis sind und Kraftfahrzeuge im öffentlichen Straßenverkehr führen. Denn die Teilnahme eines Fahrzeugführers, der Konsument illegaler Drogen ist, am öffentlichen Straßenverkehr stellt eine erhebliche Gefahr für die übrigen Verkehrsteilnehmer dar, da der Konsum illegaler Drogen die Fahrtauglichkeit erheblich beeinträchtigt. Dies gilt grundsätzlich auch für eine Reihe sog. weicher Drogen, vor allem aber für Halluzinogene. Diese sind, gerade bezogen auf das Führen eines Kraftfahrzeuges, besonders gefährlich, weil sie psychische Veränderungen und damit verminderte Leistungsstärke nicht nur in dem akuten Rauschzustand verursachen können, sondern diese auch nach dem Abklingen der Rauschsymptome jederzeit auftreten können (flashback).

Auf die besonderen Gefahren für Fahrzeugführer im Zusammenhang mit dem Konsum illegaler Drogen ist in dem Gutachten „Krankheit und Kraftverkehr" des Gemeinsamen Beirates für Verkehrsmedizin beim Bundesminister für Verkehr und beim Bundesminister für Jugend, Familie und Gesundheit hingewiesen worden.

Dementsprechend hält das Bundesverwaltungsgericht bereits den bloßen Besitz einer kleinen Menge von Haschisch oder Marihuana für ausreichend, um Zweifel an der Eignung zum Führen eines Kraftfahrzeuges zu begründen (Urteil vom 15. Dezember 1989; 7 C 52/88). Eine wesentlich differenziertere Betrachtungsweise kommt in dem Beschluß des Bundesver-

fassungsgerichts (1 BvR 689/92) vom 24. Juni 1993 zum Ausdruck. Dort wird zur Frage, unter welchen Voraussetzungen Haschischkonsum es rechtfertigen kann, gemäß § 15 b Abs. 2 StVZO ein medizinisch-psychologisches Gutachten über die Eignung zum Führen von Kraftfahrzeugen zu fordern, wie folgt Stellung genommen:

„Dem allgemeinen Persönlichkeitsrecht wird bei der Auslegung des § 15 b Abs. 2 StVZO unter Berücksichtigung der allgemeinen gesetzlichen Maßstäbe für die Erteilung und Entziehung der Fahrerlaubnis nur dann angemessen Rechnung getragen, wenn die Anforderung eines Gutachtens sich auf solche Mängel bezieht, die bei vernünftiger, lebensnaher Einschätzung die ernsthafte Besorgnis begründen, daß der Betroffene sich als Führer eines Kraftfahrzeugs nicht verkehrsgerecht und umsichtig verhalten wird. Außerdem ist nicht bereits jeder Umstand, der auf die entfernt liegende Möglichkeit eines Eignungsmangels hindeutet, ein hinreichender Grund für die Anforderung eines medizinisch-psychologischen Gutachtens. Vielmehr müssen der Entscheidung über die Anforderung tatsächliche Feststellungen zugrunde gelegt werden, die einen Eignungsmangel als naheliegend erscheinen lassen. Schließlich ist bei der Entscheidung über die Art des nach § 15 b Abs. 2 Nr. 1 bis 3 StVZO anzufordernden Gutachtens dem allgemeinen Persönlichkeitsrecht des Betroffenen Rechnung zu tragen. [. . .] Eine Auslegung des § 15 b Abs. 2 StVZO, wonach die Feststellung einmaligen Cannabisgebrauchs für sich genommen bereits ein hinreichend tragfähiger Anhaltspunkt für die Anforderung eines medizinisch-psychologischen Gutachtens ist, schränkt das allgemeine Persönlichkeitsrecht übermäßig ein. Angesichts des tiefgreifenden Grundrechtseingriffs, der mit der Anforderung eines solchen Gutachtens verbunden ist, sind deutlichere Anzeichen für einen Eignungsmangel zu fordern. Die derzeitigen Erkenntnisse über den Gebrauch von Cannabis erlauben nicht den Schluß, daß jeder, der mit einer Haschischzigarette angetroffen wird, gewohnheitsmäßiger Konsument sein könnte. Nach der Repräsentativerhebung des Bundesgesundheitsministeriums gelangt die Mehrzahl der Cannabiskonsumenten nicht über das Probierstadium hinaus. [. . .] Ferner bestehen im Hinblick auf den allgemeinen Gleichheitssatz (Art. 3 Abs. 1 GG) erhebliche Bedenken. Die Gerichte haben gebilligt, daß die Verkehrsbehörde bei der Anforderung des Gutachtens ungleich strengere Maßstäbe angewendet hat, als dies nach der allgemeinen Behördenpraxis bei Alkoholgenuß geschieht. [. . .] Hinreichende Gründe, die eine Ungleichbehandlung dieses Ausmaßes rechtfertigen könnten, sind nicht ohne weiteres ersichtlich."

14.4 Herausgabe von Daten aus Kaminfegerdateien (Kehrbücher)

Im Berichtszeitraum hat es zur Herausgabe von Daten aus Kehrbüchern mehrere Anfragen gegeben, wobei zwei Sachverhaltskonstellationen im Vordergrund standen: zum einen die Erstellung von Energiekonzepten durch Ingenieurbüros, zum anderen die Erfassung der Anschlußwerte für die Modifizierung von Grundpreisanteilen.

Es ist jeweils der öffentlich-rechtliche Bereich tangiert, da es sich bei den Bezirksschornsteinfegermeistern (Kehrbezirksinhaber) um beliehene Unternehmer handelt. Diese haben gegenüber der zuständigen Aufsichtsbehörde (Kreisverwaltung/Stadtverwaltung) die Kehrbücher – zu Prüfzwecken – zu öffnen. Entsprechende Regelungen finden sich in § 19 Schornsteinfegergesetz und § 18 der Verordnung über das Schornsteinfegerwesen. Freiberuflich tätige Ingenieure haben indes keinerlei Anspruch auf Einsicht in das Kehrbuch. Mithin kommt nur eine Datenübermittlung der Bezirksschornsteinfegermeister an die zuständige Behörde in Betracht. Diese Übermittlung würde allerdings nicht zu Prüfzwecken erfolgen, sondern z. B. der Erstellung eines Wärmekatasters dienen. Dafür wiederum gibt es keine bereichsspezifische Regelung, so daß § 6 LDatG anzuwenden ist. Danach ist die Übermittlung personenbezogener Daten an Behörden und sonstige öffentliche Stellen zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist.

Daß es sich bei den Daten aus den Kaminfegerdateien um personenbezogene Daten handelt, ist nicht zu bestreiten.

In den genannten Fällen haben Stadtverwaltungen die Erstellung eines Energiekonzeptes in Auftrag gegeben. Damit verbunden war die Erstellung eines Wärmekatasters, das Einzelangaben über sachliche Verhältnisse einer bestimmbaren Person enthält.

In § 4 LDatG ist die Verarbeitung personenbezogener Daten im Auftrag geregelt. Eine Datenverarbeitung im Auftrag liegt vor, wenn eine öffentliche Stelle (Auftraggeber) personenbezogene Daten durch eine andere Stelle oder Person (Auftragnehmer) verarbeiten läßt. Zur Einhaltung der Bestimmungen des LDatG ist auch im Falle der Auftragsdatenverarbeitung der Auftraggeber als speichernde Stelle verpflichtet. Fernerhin war darauf hinzuweisen, daß einer Datenverarbeitung im Auftrag eine schriftliche Vereinbarung zugrunde liegen soll, die den Gegenstand der Datenverarbeitung und die Weisungen der auftraggebenden Stelle für die Verarbeitung umfaßt. Findet das LDatG auf den Auftragnehmer (z. B. freiberuflich tätige Ingenieure) keine Anwendung, hat der Auftraggeber vertraglich sicherzustellen, daß die Vorschriften dieses Gesetzes beachtet werden. Um die Einhaltung der Bestimmungen des LDatG überprüfen zu können, muß sich der Auftraggeber ein Prüfungsrecht beim Auftragnehmer einräumen lassen. Auch sollte der Auftrag an eine nichtöffentliche Stelle eine Regelung über das Recht zur fristlosen Kündigung bei der Verletzung von Datenschutzbestimmungen vorsehen.

Teilweise wird, um die Kehrbuchdaten – beispielsweise an die Stadtwerke – übermitteln zu können, auch die Verordnung über allgemeine Bedingungen für die Gasversorgung von Tarifkunden (GVBGasV) vom 21. Juni 1979 (BGBl. I Nr. 29) herangezogen. Bei dieser Vorschrift, die in § 16 das Zutrittsrecht zur Ermittlung tariflicher Bemessungsgrundlagen einräumt, handelt es

sich allerdings nicht um eine Datenübermittlungsregelung. Die Festlegung, daß der Kunde den Beauftragten des Gasversorgungsunternehmens in bestimmten Fällen Zutritt zu seinen Räumen zu gestatten hat, umfaßt noch nicht die Einwilligung des Kunden, auch die Einsichtnahme in die vom Bezirksschornsteinfegermeister geführten Kehrbücher zu gestatten. Für die Datenübermittlung ist mithin § 7 LDatG einschlägig. Soweit die Kehrbezirksinhaber ein automatisiertes Verfahren zur Datenverarbeitung benutzen, wäre hier gem. § 7 Abs. 1 LDatG eine Übermittlung der Daten nur zulässig, wenn der Betroffene hiermit ausdrücklich einverstanden ist. Für den Fall, daß im entsprechenden Einzugsbereich auch Bezirksschornsteinfegermeister tätig sind, die ihre Daten im nichtautomatisierten Verfahren verarbeiten, war darauf hinzuweisen, daß eine Übermittlung der gesamten Daten aus den Kehrbüchern auch dann nicht zulässig wäre. So muß nach § 7 Abs. 2 LDatG der Empfänger der Daten ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft machen. Davon kann aber bei der Übermittlung der gesamten Daten aus den Kehrbüchern, also z. B. auch Eintragungen über festgestellte Mängel usw., nicht ausgegangen werden. Soweit sich die Datenübermittlungen jedoch nur auf die Ermittlung der Anschlußwerte der jeweils beim Kunden installierten Heizung beziehen, ist von einem berechtigten Interesse auszugehen.

Der LfD hat die Aufsichtsbehörde um entsprechende Hinweise an die betroffenen Kehrbezirksinhaber gebeten.

15 Landwirtschaft und Weinbau

15.1 Weinkontrolle: Ist das Abschreibungsverfahren anstelle des Kontrollzeichenverfahrens zulässig?

Das Ministerium für Landwirtschaft, Weinbau und Forsten hat als Maßnahme der Weinkontrolle inzwischen das sog. „Abschreibeverfahren" eingeführt. Dieses beruht darauf, daß zentral erfaßt wird, welche Weinmengen ein Erzeuger im Rahmen der Regelungen zur Begrenzung des Hektarhöchstmengenertrages produzieren darf; die veräußerten Weinmengen werden dann gemeldet und von den Zahlen der zulässigen Erträge abgezogen. Der LfD hat dieses Vorhaben aus datenschutrzrechtlicher Sicht wie folgt beurteilt:

Das behördliche Abschreibesystem erfordert eine umfassende zentrale Erfassung der Warenströme der einzelnen Betriebe. Dabei sollen neben fünf vorhandenen Meldungen (von denen zwei bislang nicht obligatorisch sind) drei weitere Meldungen eingeführt werden:

- Meldung der Abgabe abgefüllter Erzeugnisse;
- Verwendungsnachweise vom Erzeuger für offen abgegebene Erzeugnisse (z. B. Federweißer);
- Abschlußmeldung zum Ende des Weinwirtschaftsjahres am 31. August (Bestandsmeldung).

Die bislang freiwilligen Meldungen

- Formblatt zur betriebsinternen Kontrolle,
- Geschäftspapier beim Handel mit nicht abgefüllten Erzeugnissen

müßten obligatorisch werden. Außerdem sollen die bislang schon vorhandenen Informationen aus folgenden Meldungen bzw. Datenbeständen genutzt werden:

- Rebflächenverzeichnis als Teil der Weinbaukartei;
- Traubenernte/Weinerzeugungsmeldung;
- Antrag/Bescheid der amtlichen Qualitätsweinprüfung.

Die zuständige Behörde müßte alle Zu- und Abgänge an Wein und anderen Traubenerzeugnissen aufgrund der genannten Meldungen und sonstigen Informationen erfassen. Die gewonnenen Erkenntnisse sollen auch der Weinüberwachung für Kontrollzwecke zur Verfügung gestellt werden.

Das Abschreibeverfahren führt zu einer Erweiterung der bestehenden Meldepflichten sowie zu einer umfassenden Datenspeicherung bei der Kontrollbehörde. Dies würde u. a. auch dazu führen, daß die im Juli 1991 aufgrund einer Intervention des Landesrechnungshofes aufgehobenen Meldungen nach § 4 der 5. Landesverordnung erneut eingeführt würden. Die seinerzeitige Veränderung ist durch den LfD nachdrücklich befürwortet und vom Staatssekretär des Ministeriums für Landwirtschaft, Weinbau und Forsten auch als Erfolg des Datenschutzes bezeichnet worden (Schreiben vom 10. September 1991, Az.: 755.299/ 3).

Aus datenschutzrechtlicher Sicht stößt das Abschreibeverfahren auf grundsätzliche Bedenken und besitzt gegenüber dem Kontrollzeichenverfahren gravierende Nachteile.

Außerdem besteht nach Auffassung des LfD derzeit keine hinreichende Verordnungsermächtigung.

Für die Auslegung einer Verordnungsermächtigung ist entscheidend, welche Regelungsentscheidung des Gesetzgebers vorliegt, die es näher auszufüllen und auszuführen gilt. Die gesetzliche Regelungsentscheidung im Weingesetz ist allerdings die, daß in bezug auf die Kontrolle des zulässigen Hektarertrages vorrangig das Kontrollzeichenverfahren einzuführen ist. Der Gesetz-

geber hat deutlich entschieden, daß nur dann, wenn ergänzend zum Kontrollzeichenverfahren weitere Kontrollen nach Auffassung des Verordnungsgebers erforderlich sind, solche ergänzenden Maßnahmen ebenfalls durch Erlaß einer Rechtsverordnung vorgesehen werden können.

Die Einführung anderer Kontrollmaßnahmen als „Alternative" zum Kontrollzeichenverfahren ist vom gesetzgeberischen Willen nicht gedeckt.

Auch das vom Ministerium vorgetragene Argument, der Bund sei für die Einführung des Kontrollzeichens verantwortlich, die Länder hätten ihrerseits unabhängig von den Maßnahmen des Bundes für ausreichende Kontrollen zu sorgen, kann keine andere Wertung rechtfertigen:

Zum einen ist das Tätigwerden des Bundes im Sinne der Einführung des Kontrollzeichens gesetzliche Voraussetzung dafür, daß die Länder ergänzende andere Kontrollmaßnahmen einführen können. Zum anderen beruht die Tatsache, daß der Bund das Kontrollzeichen ursprünglich erst 1996, nunmehr überhaupt nicht mehr (zwischenzeitlich besteht die Absicht, die gesetzliche Pflicht zur Einführung von Kontrollzeichen gänzlich abzuschaffen) vorsehen will, darauf, daß die Länder dies ihrerseits gewollt haben. Bund und Länder haben sich darauf verständigt, daß in allen weinbautreibenden Bundesländern statt dessen ein auf einem Meldesystem beruhendes behördliches Abschreibeverfahren als Alternative zum Kontrollzeichen eingeführt wird. Daraus ergibt sich, daß Bund und Länder einvernehmlich den klar erkennbaren Willen des Gesetzgebers in bezug auf die Kontrolle der Hektarmengenbegrenzung durch das jetzt geplante Abschreibungsverfahren umgehen wollten. Da das Abschreibungsverfahren im Vergleich zum Kontrollzeichenverfahren datenschutzrechtlich weitergehende und schwerwiegendere Eingriffe in das informationelle Selbstbestimmungsrecht der betroffenen Winzer mit sich bringt, hat der LfD seine datenschutzrechtlichen Bedenken gegen diese Verordnung aufrechterhalten.

Es ist daran festzuhalten, daß auf der Basis des geltenden Weingesetzes eine Rechtsverordnung des Landes, in der das Abschreibungsverfahren vorgeschrieben wird, so lange als rechtswidrig anzusehen ist, wie das Kontrollzeichenverfahren nicht eingeführt worden ist. Erst dann könnte erwogen werden – wenn sich dies dann noch als erforderlich und verhältnismäßig erweisen sollte –, ergänzend zusätzliche Kontrollen vorzusehen.

15.2 Das integrierte Verwaltungs- und Kontrollsystem der EG (Invekos) – Kommt der gläserne Landwirt?

Von der Öffentlichkeit nahezu unbemerkt ist es der EG gelungen, die Mitgliedsstaaten auf die Errichtung einer Datenbank zu verpflichten, die – zusammen mit den vorgesehenen Überwachungsmaßnahmen – bislang beispiellos sein dürfte (Verordnung EG vom 27. November 1992 zur Einführung eines integrierten Verwaltungs- und Kontrollsystems für bestimmte gemeinschaftliche Beihilferegelungen, Nr. 3508/92, Amtsblatt der Europäischen Gemeinschaften vom 5. Dezember 1992, Nr. L 355/1).

Grund der Errichtung dieser Datenbank ist, daß die EG eine völlig neue Struktur ihrer landwirtschaftlichen Fördermaßnahmen eingeführt hat und eine Fehlleitung von Fördermitteln durch effektive Kontrollmaßnahmen verhindern will. Es werden nicht mehr die landwirtschaftlichen Produkte, sondern die bewirtschafteten Flächen gefördert. In diesem Zusammenhang ist zunächst die Information über alle Flächen erforderlich, die in die Förderung einbezogen sind. Jedes Mitgliedsland soll eine Datenbank nach einheitlichen Kriterien errichten, in der alle Landwirte mit ihren Flächen erfaßt werden, die an den EG-Fördermaßnahmen teilnehmen. Die lückenlose Erfassung aller Flächen der betroffenen Landwirte und der Flächennutzungsarten ist also Bestandteil dieser Datenbank. Weiterhin ist beabsichtigt, Daten zur wirtschaftlichen Situation der Betriebe zu erfassen. Alle förderungsrelevanten Informationen sind automatisiert zu speichern. Die Grundstücke sollen nach einheitlichen Kriterien so bezeichnet werden, daß eine Kontrolle der angegebenen Nutzungsarten durch einen Vergleich mit Satellitenaufnahmen möglich wird. Die Überwachung mit Hilfe der Satellitentechnik ist ein wesentlicher, integraler Bestandteil des Konzepts.

Im Bereich der EG kann wohl kaum ein Landwirt ohne Beteiligung an einer Fördermaßnahme existieren. Damit ist die Erfassung nahezu aller Landwirte in der landwirtschaftlichen Betriebsdatenbank unausweichlich. Das integrierte Verwaltungs- und Kontrollsystem führt also zu einer nahezu lückenlosen Erfassung der Landwirte zum Zweck der Kontrolle im Bereich landwirtschaftlicher Förderungsmaßnahmen. Wegen der mißbräuchlichen Inanspruchnahme und zweckwidrigen Verwendung von EG-Fördermitteln scheint gerade das sinnvoll zu sein. Andererseits darf die Kontrolle bei der Vergabe staatlicher Leistungen nicht dazu führen, daß die rechtsstaatlichen Grundsätze der Verhältnismäßigkeit und der Achtung vor dem Bürger als Subjekt staatlicher Maßnahmen völlig vernachlässigt werden. Die Kontrollmaßnahmen müssen dem Gebot der Verhältnismäßigkeit entsprechen; die Einschränkung des informationellen Selbstbestimmungsrechts darf nicht weitergehen als es zum Schutz öffentlicher Interessen unerläßlich ist. Ein amtshilfefester Schutz gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote ist erforderlich. Diese Überlegungen haben zu folgenden Anforderungen aus der Sicht des LfD an die landwirtschaftliche Betriebsdatenbank und an die dabei eingesetzten Kontrollmechanismen geführt:

a) Flächen dürfen nur dann in die Betriebsdatenbank aufgenommen werden, wenn dies entweder zur Berechnung der Förderung oder zum Zweck der wirksamen Kontrolle unabdingbar ist.

b) Vorgesehene Kontrollmaßnahmen müssen verhältnismäßig sein. Angesichts der Tatsache, daß bereits jetzt in einigen Bundesländern (noch nicht in Rheinland-Pfalz) die Satellitenüberwachung in diesem Zusammenhang eingesetzt wird, kommt folgenden Gesichtspunkten in diesem Zusammenhang besondere Bedeutung zu:

- Es darf keine flächendeckende, lückenlose Kontrolle geben, die Kontrolle ist auf Stichproben zu beschränken.
- Nach Möglichkeit sind die Betroffenen (etwa durch konkrete Informationen vor der Durchführung von Prüfmaßnahmen) zu beteiligen.
- Die Verantwortung für die Überprüfungsverfahren und auch für die Durchführung der Überwachungsmaßnahmen sollte nicht zentralisiert werden, sondern bei den für die Förderung zuständigen Stellen liegen. Dies betrifft sowohl die Anordnung der Durchführung von Kontrollen wie die Auswertung entsprechender Informationen.
- Von landwirtschaftlichen Fördermaßnahmen nicht betroffene Grundstücke müssen auch bei Luftüberwachungsmaßnahmen ausgeblendet werden. Wenn dies nicht schon bei der Erfassung möglich sein sollte, ist dies spätestens bei der Speicherung bzw. Auswertung technisch zu gewährleisten.

c) Auch die Einhaltung der Zweckbindung der gespeicherten Daten ist datenschutzrechtlich bedeutsam. Dies bedeutet hier konkret: Die landwirtschaftliche Betriebsdatenbank ist errichtet worden, um die Fördermaßnahmen im Sektor der pflanzlichen Produktion gem. EGVO Nr. 1765/92 sowie im Sektor der tierischen Produktion gem. EGVO Nrn. 805/68, 3013/89 sowie 2328/91 durchzuführen. Soweit eine Erweiterung der Nutzungsmöglichkeiten in der EGVO angesprochen ist, bedarf jede konkrete Erweiterung der Zweckverwendung der in den landwirtschaftlichen Betriebsdatenbanken gespeicherten Daten jeweils einer eigenen Rechtsgrundlage. Solche ergänzenden Rechtsgrundlagen sind insbesondere dann nötig, wenn Kontrollzwecke außerhalb des landwirtschaftlichen Förderbereichs mit den Daten erfüllt werden sollen (beispielsweise im Rahmen der Besteuerung oder im Rahmen der Klärschlammaufbringung). Sie sind aber auch schon bei der Erstreckung der Nutzung dieser Daten auf andere Fördermaßnahmen erforderlich.

Im Zusammenhang mit dieser Datenbank und den hier eingesetzten Überwachungsmaßnahmen wird erneut das Problem der Zunahme der allgemeinen Kontrolldichte deutlich: Die hier dargestellte Maßnahme kann zwar nicht grundsätzlich aus datenschutzrechtlicher Sicht abgelehnt werden, sie ist jedoch als weiterer Baustein zu einer wirksamen und umfassenden Kontrolle und Erfassung eines bedeutsamen Teils der Bevölkerung anzusehen.

In diesem Zusammenhang ist auch das Problem deutlich geworden, daß EG-Recht nationale Grundrechte einschränken kann. Fraglich ist, wie weit diese EG-Kompetenz tatsächlich reicht und inwieweit das informationelle Selbstbestimmungsrecht beim Europäischen Gerichtshof für Menschenrechte durchsetzbar wäre. Diese Fragen werden in der Zukunft sicher noch in vielen anderen Zusammenhängen Bedeutung erlangen.

Der LfD jedenfalls wird sich dafür einsetzen, daß auf der nationalen Ebene alle Maßnahmen getroffen werden, um die oben genannten Anforderungen zu erfüllen.

16 Statistik

16.1 Zählkarten für Geburts- und Sterbefälle auf der Grundlage des Bevölkerungsstatistikgesetzes

Die Anfrage eines Krankenhauses, dessen Verwaltung Zählkarten des Statistischen Landesamtes für Geburts- und Sterbefälle auszufüllen hatte, ließ wieder einmal die Unzulänglichkeiten des Gesetzes über die Statistik der Bevölkerungsbewegung und die Fortschreibung des Bevölkerungsstandes (Bevölkerungsstatistikgesetz) erkennen. Es werden beispielsweise Fragen gestellt nach Totgeburten, Religionszugehörigkeit, Legitimität des Kindes (eheliche, nichteheliche Geburt), Zahl der zuvor lebend- oder totgeborenen Kinder, Geburtsgewicht und Körperlänge des Neugeborenen. Als Rechtsgrundlage der Datenerhebung durch die Krankenhäuser und die Übermittlung an die Standesbeamten werden die §§ 18, 19 und 34 Personenstandsgesetz, § 398 der Dienstanweisung für Standesbeamte i. V. m. § 2 Abs. 2 des Bevölkerungsstatistikgesetzes herangezogen. So geht § 398 der Dienstanweisung zwar von einer Mitwirkungspflicht der Anstalten (Krankenhäuser) aus. Eine Befugnis für Informationseingriffe indes kann durch die Dienstanweisung nicht begründet werden.

Das Bevölkerungsstatistikgesetz vom 12. Juli 1957 in der Fassung der Bekanntmachung vom 14. März 1980 (BGBl. I, S. 308) entspricht nicht mehr den datenschutzrechtlichen Anforderungen; zehn Jahre nach Verkündung des Urteils sind die Novellierungsbestrebungen wiederum ins Stocken geraten. Aus der Sicht des Datenschutzes sollte das Gesetz schleunigst verfassungsgemäß überarbeitet werden. So ist u. a. die Erforderlichkeit der o. g. Datenerhebungen in Zweifel zu ziehen. Auch gehen Fragen nach ehelicher oder nichtehelicher Geburt und nach der Zahl der zuvor lebend- oder totgeborenen Kinder weit in den von der Verfassung geschützten, einer amtlichen Statistik nicht zugänglichen Intimbereich hinein.

Ein weiteres Problemfeld ergibt sich aus der Verflechtung von amtlicher Statistik und Verwaltungsvollzug bei der Erhebung der Daten. Die genannten Angaben werden zur Zeit, wie oben dargestellt, lediglich aufgrund einer Dienstanweisung erhoben,

obwohl sie für Verwaltungszwecke (des Standesamtes) nicht erforderlich sind. Diese Verfahrensweise verstößt nach Auffassung des LfD gegen das im Volkszählungsurteil postulierte Prinzip der Trennung von Statistik und Verwaltung.

16.2 Gemeindestatistiken

Aufgrund einer Eingabe hatte sich der LfD mit folgendem Vorbringen zu befassen:

In den Mitteilungsblättern für den Bereich einer Verbandsgemeinde waren Gemeindestatistiken veröffentlicht, u. a. auch für eine Ortsgemeinde mit etwa 300 Einwohnern. Insbesondere bezüglich der dort ausgewiesenen „Tabellen-Einsen" wurde um Prüfung gebeten, ob nicht eine entsprechende Anonymisierung geboten wäre.

Bei den Daten, die in den Verbandsgemeindeblättern veröffentlicht wurden, handelte es sich um Ergebnisse des Einwohnerwesens. Diese Ergebnisse werden im Auftrag der jeweiligen Kommunalverwaltung vom Landesrechenzentrum als Auftragnehmer ermittelt. Zuständig und verantwortlich für eine Weitergabe dieser Daten ist allein die betreffende Verwaltung. Bei sehr kleinen Gemeinden hat die jeweilige Gemeinde zu prüfen, ob aufgrund der Veröffentlichung im Gemeindeblatt echte Einzelfalldarstellungen denkbar sind. Diese Prüfung ist insbesondere deshalb erforderlich, weil die Gemeindestatistik zum Teil personenbeziehbare Angaben enthält, die nach § 16 Bundesstatistikgesetz geheimzuhalten sind.

In dem von dem Petenten genannten Beispiel wurde allerdings deutlich, daß es sich bei den dortigen „Tabellen-Einsen" keineswegs zwangsläufig um Einzelangaben gehandelt hat. Da jede der fünf Merkmalsgruppen (z. B. Familienstand, Religion, Altersgruppe) nur einmal untergliedert war, nämlich nach dem Geschlecht, war die „1" der einen Merkmalsgruppe nicht auf die „1" der anderen Merkmalsgruppe beziehbar. In jeder Merkmalsgruppe gab es eine männliche Person, auf die eine der Merkmalsausprägungen zutraf.

Erst eine Darstellung, die alle diese Merkmale miteinander verknüpfen und in der eine „1" durch alle Untergliederungen gehen würde, könnte tatsächlich das detaillierte Bild einer bestimmten Person aufzeigen und zu deren Identifizierung führen oder Kenntnisse aus ihrem Persönlichkeitsbereich offenbaren, die nicht allgemein (äußerlich) erkennbar sind.

Nach allem war im vorliegenden Fall ein Gesetzesverstoß nicht erkennbar. Die Veröffentlichung bzw. Weitergabe kleinräumig gegliederter statistischer Ergebnisse ist rechtmäßig, wenn die geforderte organisatorische Trennung zwischen Verwaltungsvollzug und Statistik gegeben und eine Reidentifzierung nicht möglich ist. Werden aggregierte, anonymisierte Daten zum Anlaß genommen, Verwaltungsvollzugsmaßnahmen etwa durch gezielte Betrachtung bestimmter Personengruppen oder Gebiete, z. B. bestimmte Blockseiten, vorzubereiten, widerspricht dies weder dem Grundsatz der Trennung von Statistik und Vollzug noch dem Gebot einer Zweckbindung der erhobenen Daten zu statistischen Zwecken, wenn und soweit kleinraumbezogene Spezialaufbereitungen nicht die Grenze der Reidentifizierbarkeit überschreiten. Das Recht auf informationelle Selbstbestimmung ist Ausprägung des allgemeinen Persönlichkeitsrechts; es schützt den einzelnen nicht davor, daß hinreichend anonymisierte Ergebnisse statistischer Erhebungen beispielsweise für Planungen verwendet werden.

16.3 Monatsberichte zur Einzelhandelsstatistik

Ein Petent rügte, er werde seit 1984 vom Statistischen Landesamt Jahr für Jahr verpflichtet, monatliche Angaben zu seinem Betrieb zu machen. Man habe ihm mitgeteilt, daß die Berichtspflichtigen aus einem Bestand von 35 000 Unternehmen per Computer in einem bestimmten Rhythmus ausgewählt würden. Da er „zufällig" nunmehr seit neun Jahren Bericht zu erstatten habe, verfestige sich bei ihm der Eindruck, daß hier etwas nicht mit rechten Dingen zugehe.

Eine Überprüfung durch den LfD hat folgendes ergeben: Die Auswahl des Berichtskreises erfolgte im Anschluß an die Handels- und Gaststättenzählung nach einem bundeseinheitlichen Verfahren, zuletzt im Jahre 1985. Aus methodischen Gründen war es erforderlich, daß der Berichtskreis bis zur nächsten Auswahl konstant gehalten wird. Daher sind Befreiungen von der Auskunftspflicht grundsätzlich nicht möglich.

Geregelt ist dies in § 1 Abs. 2 Nr. 4 des Gesetzes über die Statistik im Handel und Gastgewerbe (Handelsstatistikgesetz), das u. a. Stichprobenerhebungen mit Auskunftspflicht für die Bereiche Großhandel, Einzelhandel, Handelsvermittlung sowie das Gastgewerbe vorschreibt. Dabei begrenzt es gem. § 2 die Zahl der monatlich, jährlich und mehrjährig zu erfassenden Unternehmen auf bestimmte Höchstzahlen, im Großhandel und in der Handelsvermittlung auf jeweils 10 000, im Einzelhandel auf 35 000 und im Gastgewerbe auf 8 000 Unternehmen. Die Monatserhebungen dienen in erster Linie konjunkturanalytischen Zwecken und liefern Angaben über den Gesamtumsatz und die Zahl der Voll- und Teilzeitbeschäftigten, während die Jahreserhebungen und die in mehrjährigem Abstand erfolgenden Ergänzungserhebungen einen umfassenden Einblick in die im Zuge der wirtschaftlichen Entwicklungen eingetretenen wichtigsten Änderungen in den einzelnen Teilbereichen geben sollen. Bis 1985 basierten die Stichprobenerhebungen auf der Handels- und Gaststättenzählung 1978. Da die Ergebnisse von Stichprobenerhebungen mit wachsendem zeitlichen Abstand zur Auswahlgrundlage ungenauer werden, ist es grundsätzlich sinnvoll, von Zeit zu Zeit eine

neue Stichprobe zu ziehen. Mit der Handels- und Gaststättenzählung 1985 stand eine neue Auswahlgrundlage für die Stichprobenziehung zur Verfügung. Das frühere Verfahren sah eine einstufige Auswahl proportional zur Umsatzgröße der Unternehmen vor. Es wurde im neuen Stichprobenplan aus methodischen Gründen nicht beibehalten. Folge der größenproportionalen Auswahl war u. a., daß die Ergebnisqualität für die Zahl der Beschäftigten nicht immer befriedigen konnte, da die Merkmale Umsatz und Beschäftigte vor allem im Großhandel nur wenig korreliert sind. Nach umfangreichen Voruntersuchungen wurde entschieden, eine geschichtete Zufallsauswahl von Unternehmen durchzuführen und die Ergebnisse durch eine Verhältnisschätzung unter Bezugnahme auf die Merkmale Umsatz und Beschäftigte aus der Handels- und Gaststättenzählung 1985 zu ermitteln. Dieses Verfahren hat gegenüber der größenproportionalen Auswahl auch den Vorteil, daß bei der Hochrechnung die Beschäftigten berücksichtigt werden können. Aus der Auswahlgrundlage wurden nach dem Stichtag der Handels- und Gaststättenzählung erloschene Unternehmen herausgenommen. Die Auswahlgesamtheit bildeten somit alle übrigen Unternehmen der Handels- und Gaststättenzählung, die 1984 einen Jahresumsatz von mindestens 1 000 000,– DM ohne Mehrwertsteuer im Großhandel, 50 000,– DM ohne Mehrwertsteuer in der Handelsvermittlung, 250 000,– DM mit Mehrwertsteuer im Einzelhandel und 50 000,– DM mit Mehrwertsteuer im Gastgewerbe hatten. Die Stichprobenunternehmen wurden im Statistischen Landesamt mit einem Standardprogramm gezogen. Vor der Ziehung wurde das Einzelmaterial der Handels- und Gaststättenzählung innerhalb jeder Schicht nach Wirtschaftsklassen und Umsatz angeordnet. Durch die Anordnung nach Wirtschaftsklassen wird bei einer Ergebnisgliederung nach Wirtschaftsklassen ein genauigkeitssteigernder Effekt erzielt. Der frühere Berichtsfirmenkreis wurde in der Weise ausgetauscht, daß ein ausgewähltes Unternehmen, das schon zur alten Stichprobe auskunftspflichtig war, durch ein benachbartes derselben Wirtschaftsklasse und derselben Schicht, das bisher nicht gemeldet hatte, ersetzt wurde.

Mithin hat das Statistische Landesamt durch die Anforderung statistischer Daten mittels auszufüllender Erhebungsbögen (Monatsberichte) lediglich von einer Befugnis Gebrauch gemacht, die ihm durch das Handelsstatistikgesetz sowie das Gesetz über die Statistik für Bundeszwecke (BStatG) eingeräumt ist. Das Verfahren war nicht zu beanstanden.

16.4 Probleme mit der Doppelkarte bei Monatsberichten

Ein zur amtlichen Statistik auskunftspflichtiger Petent trug vor, er hätte aus Versehen die Ausfertigung der Statistik, die im Betrieb bleiben soll, an das Statistische Landesamt (im Briefumschlag) übersandt und dies wiederum das Firmen-Doppel an ihn, allerdings „ganz offen", zurückgeschickt.

Es hat sich herausgestellt, daß für die Monatsberichte eine Doppelkarte verwendet wird. Zu Beginn eines jeden Jahres erhalten die Auskunftspflichtigen neben einem Begleitschreiben und einem Merkblatt zwölf solcher Doppelkarten. Im Feld „Firma" wird neben der Kennummer auch die vollständige, beim Statistischen Landesamt gespeicherte Firmenanschrift eingedruckt. Dies soll den Berichtspflichtigen die Möglichkeit geben, auf Fehler oder Veränderungen hinzuweisen. Da dieser Teil der Doppelkarte bei dem Berichtspflichtigen verbleibt, hat das Statistische Landesamt bislang keine datenschutzrechtlichen Bedenken gesehen.

Das von dem Petenten vorgetragene Geschehen war nicht mehr aufklärbar. Bei einem durchschnittlichen täglichen Postaufkommen beim Statistischen Landesamt von etwa 2 500 Sendungen konnte allerdings ein Versehen im Bereich der Poststelle nicht gänzlich ausgeschlossen werden.

Das Statistische Landesamt hat diesen Vorfall jedenfalls zum Anlaß genommen, künftig auf den Eindruck der Firmenanschrift (Straße, Hausnummer, Postleitzahl und Ort) zu verzichten, so daß die vom Petenten geschilderte offene Rücksendung fehlgeleiteter Erhebungsunterlagen künftig ausgeschlossen ist.

17 Personaldatenverarbeitung

17.1 Landesregelungen zur Personaldatenverarbeitung

17.1.1 Landespersonalvertretungsgesetz

Im Berichtszeitraum ist das neue LPersVG in Kraft getreten. Aus datenschutzrechtlicher Sicht sind grundsätzlich zwei Bereiche dieses Gesetzes bedeutsam:

a) Bestimmungen, welche die Mitwirkung des Personalrats bei der Datenverarbeitung durch die Dienststelle mit dem Ziel der Wahrung des informationellen Selbstbestimmungsrechts der Bediensteten zum Gegenstand haben;

b) Bestimmungen, welche die Wahrung des informationellen Selbstbestimmungsrechtes der Bediensteten bei Datenverarbeitungen durch den Personalrat selbst betreffen.

§§ 78 Abs. 3 Nr. 1, 80 Abs. 1 Nr. 2 sowie 80 Abs. 1 Nr. 3 behandeln den unter a genannten Bereich.

Die Regelungen betreffen trotz unterschiedlicher Formulierungen immer gleiche Sachverhalte. Im Entwurfsstadium bestehende Unklarheiten wurden beseitigt. Sie bezogen sich auf Begriffsbildungen, die mit dem Datenschutzgesetz nicht übereinstimmen und auf die Frage, ob die Mitbestimmungspflicht auch die automatisierte Verarbeitung anderer Daten als die der Bediensteten (z. B. von Sachdaten oder Informationen über Bürger) betrifft. Die im Gesetz unter Mitwirkung des LfD gefundenen Formulierungen dürften nunmehr insofern klar regeln, daß nur die Bedienstetendaten Gegenstand der Mitbestimmung sind.

Zum unter b genannten Themenkomplex enthält § 72 Regelungen, die grundsätzlich dem Datenschutz der betroffenen Bediensteten dienen und die das bisherige Recht präzisieren. Dies ist zu begrüßen. Auch insofern hat der LfD erreicht, daß wünschenswerte Klarstellungen erfolgten.

17.1.2 Landesbeamtengesetz

Das Beamtenrechtsrahmengesetz des Bundes hat verbindliche Vorgaben für die Länder geschaffen, wie die Personalakten der Beamten zu führen sind, insbesondere welche Datenübermittlungen und -verwendungen zulässig sind.

Auf der Ebene des Landes ist dieses Bundesgesetz noch zu übernehmen. Ein entsprechender Entwurf liegt vor. Die aus datenschutzrechtlicher Sicht bestehenden Grundsatz- und Detailprobleme konnten frühzeitig erörtert werden. Der LfD begrüßt, daß eine Reihe seiner Anregungen Eingang in den Entwurf gefunden hat. Folgende Vorschläge, die aus der Sicht des LfD besonders bedeutsam sind, sind jedoch bislang nicht berücksichtigt worden:

a) Abschottung der Beihilfestellen

   Die Sollvorschrift über die Trennung der Beihilfestellen von der übrigen Personalverwaltung sollte in eine zwingende Regelung umgewandelt werden.

   Nach wie vor läßt die Begründung nicht erkennen, warum eine Sollvorschrift vorgeschlagen wird. Es wird vielmehr in begrüßenswerter Weise dargestellt, welche Bedeutung der Abschottung zukommt. Gründe der Verwaltungspraxis können eine Ausnahme von der Abschottung nicht rechtfertigen: Selbst wenn ein Sachbearbeiter in kleineren personalverwaltenden Behörden mit der Bearbeitung von Beihilfevorgängen nicht ausgelastet ist, müßte es möglich sein, ihm daneben andere Aufgaben als solche der Personalverwaltung zuzuweisen. Dies gilt auch für die Ebene der Referenten, Dezernenten und Abteilungsleiter. In Bayern wird schon seit Jahren entsprechend verfahren (vgl. Grundsätze des bayerischen Staatsministers der Finanzen zum Persönlichkeitsschutz bei Beihilfedaten aus dem Jahr 1985).

b) Die Herausgabe von Beamtenhandbüchern (z. B. Lehrerhandbücher; Richterhandbücher) könnte privilegiert werden; nur müßte dies dann im Landesbeamtengesetz geregelt werden. Nach der jetzigen Regelung ist eine ausdrückliche Einwilligung der betroffenen Bediensteten in entsprechende Datenübermittlungen an die Herausgeber solcher Werke erforderlich (§ 102 d Abs. 2 des Entwurfs). Damit würde die bewährte und langjährig befolgte Praxis der Widerspruchslösung beispielsweise in bezug auf die Richterhandbücher und Lehrerhandbücher künftig geändert werden müssen. Aus datenschutzrechtlicher Sicht ist dies jedenfalls nicht zwingend zu fordern.

c) Die Veröffentlichung von Geschäftsverteilungsplänen und Telefonlisten sollte im Gesetz geregelt werden. Nach § 102 d Abs. 2 des Entwurfs ist – bei einer engen Auslegung – weder die ungehinderte Verbreitung von Geschäftsverteilungsplänen noch von Telefonlisten zulässig. Zweifelhaft wäre auch, ob z. B. der Organisationsplan der Landesregierung (Drs. 12/1600) künftig noch in dieser Form veröffentlicht und verbreitet werden dürfte. Das Landesbeamtengesetz sollte eine entsprechende klarstellende Regelung enthalten, die derartige Veröffentlichungen ausdrücklich zuläßt.

d) Zum Umfang der zulässigen Datenerhebung im Bewerbungs- und Einstellungsverfahren sollte eine genauere Regelung getroffen werden. Bislang enthält § 102 Abs. 4 Satz 1 nur eine Regelung, die auf den Erforderlichkeitsgrundsatz für die Datenerhebung abstellt. Damit bleiben die in der Praxis bedeutsamen Bereiche der Fragen nach laufenden Strafverfahren, die Datenerhebung im Zusammenhang mit der Verfassungstreueprüfung, die Zulässigkeit von Tests und Untersuchungen im Rahmen des Einstellungsverfahrens ungeklärt. Hier sollte der Gesetzgeber die Grenzen des Zulässigen deutlicher formulieren.

e) Eine Regelung der Datenübermittlung zwischen dem Amtsarzt und dem Dienstherrn für die Befunde, die anläßlich einer Einstellungsuntersuchung erhoben worden sind, steht noch aus. Übermittlungsregelungen in diesem Zusammenhang betreffen bislang amtsärztliche Untersuchungen zur Feststellung der Dienstunfähigkeit (§ 56), zur Feststellung der Wiederverwendung von Ruhestandsbeamten (§ 61), und zur Feststellung der Dienstunfähigkeit beim Fernbleiben vom Dienst (§ 81). Eine entsprechende Regelung sollte auch für Datenübermittlungen durch den Amtsarzt getroffen werden, soweit dieser Erkenntnisse aus einer Einstellungsuntersuchung gewinnt.

f) Nr. 4 der Verwaltungsvorschrift des Ministeriums für Umwelt und Gesundheit über die Einschränkung der Weitergabe von Daten aus amtsärztlicher Untersuchungstätigkeit vom 5. Februar 1986 (Minbl. S. 148) sollte gesetzlich verankert werden. Diese Regelung hat die Begrenzung und Konkretisierung des amtsärztlichen Untersuchungsauftrags zum Gegenstand. Sie

lautet: „Die anfordernden Stellen werden gebeten, bei der Anforderung von Gesundheitszeugnissen den Untersuchungszweck möglichst genau zu beschreiben und etwaige besondere Anforderungen, die sich aus der vorgesehenen Verwendung des Bewerbers oder Bediensteten ergeben, zu nennen. Bei Dienstunfähigkeitsuntersuchungen sind dem Gesundheitsamt alle Umstände mitzuteilen, die für die Beurteilung von Bedeutung sein können. Hierunter fallen insbesondere längere Fehlzeiten, bestehende Minderungen der Erwerbsfähigkeit usw."

Das Landesbeamtengesetz sollte entweder um eine derartige Regelung ergänzt werden, oder es sollten die Voraussetzungen geschaffen werden, sie in eine Rechtsverordnung zu übernehmen.

g) Schließlich ist nach wie vor die Grundsatzfrage des Verhältnisses von allgemeinem Datenschutzrecht (LDatG, BDSG) zu den Regelungen des Personalaktenrechts nicht deutlich geklärt. § 31 des vorliegenden Referentenentwurfs zum Landesdatenschutzgesetz Rheinland-Pfalz enthält eine eigene Regelung über die Verarbeitung personenbezogener Daten bei Dienst- und Arbeitsverhältnissen. Nach diesem Referentenentwurf wird die Verweisung auf das Bundesdatenschutzgesetz für dienst- und arbeitsrechtliche Rechtsverhältnisse nicht geregelt. Es würde zur Klarheit beitragen, wenn die genannte Vorschrift in das Landesbeamtengesetz einbezogen würde. Die im LDatG-E enthaltene besondere Regelung über die Erhebung, Speicherung und Übermittlung von Beschäftigtendaten hat einen Anwendungsbereich, der sich jedenfalls mit dem Geltungsbereich des § 102 LBG des Entwurfs überschneidet. Hier sollte die Chance genutzt werden, nachdem sich beide Gesetze derzeit im Entwurfstadium befinden, eine abgestimmte Lösung zu finden, die zum Zweck der Erzielung von Normenklarheit am sinnvollsten in einer einheitlichen Regelung im Rahmen des Landesbeamtengesetzes erfolgen sollte. Eine Übernahme für den Bereich der Angestellten und Arbeiter des öffentlichen Dienstes könnte auf dem gleichen Weg, der für andere beamtenrechtliche Regelungen üblich ist, erfolgen.

Die geforderten Klarstellungen wären sicherlich für die Praxis hilfreich und würden dazu beitragen, das informationelle Selbstbestimmungsrecht der Bediensteten auch tatsächlich künftig stärker zu sichern.

17.1.3 § 31 Landesdatenschutzgesetz-Entwurf

Der Entwurf eines Landesdatenschutzgesetzes (Näheres hierzu Tz. 2) regelt in § 31 Fragen des Arbeitnehmerdatenschutzes. Der LfD hat zunächst grundsätzliche Bedenken wegen des Nebeneinanders besonderer datenschutzrechtlicher Regelungen zur Personaldatenverarbeitung im Landesbeamtengesetz und im Landesdatenschutzgesetz geäußert und angeregt, die Rechtsmaterie abschließend im Landesbeamtengesetz zu regeln. Die Übertragung auf die Angestellten und Arbeiter könnte dann durch die Mechanismen erfolgen, die hierfür üblich sind (Tarifvertrag u. ä.). Dem ist die Landesregierung bislang nicht gefolgt.

Hilfsweise hat der LfD darauf hingewirkt, daß der Datenschutzstandard im Landesdatenschutzgesetz nicht hinter dem des Landesbeamtengesetzes zurückbleibt. Dies hätte zur Folge, daß Angestellte und Arbeiter datenschutzrechtlich schlechter als Beamte behandelt werden würden. Ein Grund ist hierfür nicht ersichtlich. Dieses Ziel des LfD dürfte – nach dem derzeitigen Erkenntnisstand – auch erreicht werden.

17.1.4 Verwaltungsvorschriften zur Einstellung in den öffentlichen Dienst

Anläßlich des Außerkrafttretens und der Neuverkündung von Verwaltungsvorschriften ist deutlich geworden, daß eine größere Zahl von untergesetzlichen Regelungen existiert, die das Einstellungsverfahren in den öffentlichen Dienst zum Gegenstand haben. Insbesondere können folgende Verwaltungsvorschriften genannt werden:

a) VV über den Nachweis der Rechtsstellung als Deutscher im Sinne des Artikels 116 des Grundgesetzes bei der Einstellung in das Beamtenverhältnis vom 18. November 1980, MinBl. S. 776,

b) VV über die Ausstellung von Gesundheitszeugnissen bei schwerbehinderten Beamten und bei der Einstellung von schwerbehinderten Bewerbern in das Beamtenverhältnis vom 22. Juli 1981, MinBl. S. 618,

c) Behandlung von Personalfragebögen und von Unterlagen über erfolglose Bewerber vom 14. April 1986, MinBl. S. 258,

d) Stellenausschreibungen, VV vom 20. November 1986, MinBl. S. 572,

e) Vorlage von Führungszeugnissen und Einholung von unbeschränkten Auskünften aus dem Zentralregister bei Einstellung in den Landesdienst, VV vom 17. Dezember 1986, MinBl. 1987, S. 42,

f) Pflicht zur Verfassungstreue im öffentlichen Dienst vom 27. Dezember 1990, MinBl. 1991, S. 15,

g) Kosten der amtsärztlichen und ärztlichen Gutachten im Zusammenhang mit der Einstellung, Anstellung und Tätigkeit im öffentlichen Dienst vom 28. Oktober 1986, MinBl. S. 544.

Allen genannten Vorschriften ist gemeinsam, daß sie jedenfalls hauptsächlich Vorgänge im Zusammenhang mit der Einstellung zum Gegenstand haben. Alle regeln auch Sachverhaalte mit datenschutzrechtlichem Gehalt. Unter datenschutzrechtlichen Gesichtspunkten betrifft ihr wesentlicher Inhalt die Erhebung von Daten anläßlich der Bewerbung für den öffentlichen Dienst sowie den weiteren Umgang mit den erhobenen Daten bei dieser Gelegenheit (Übermittlung, Löschung, sonstige Nutzung).

Dabei ist einheitlich von folgenden datenschutzrechtlichen Grundsätzen auszugehen:

„Es ist für den Bewerber transparent festzulegen,

- welche personenbezogenen Informationen von ihm verlangt bzw. über ihn eingeholt werden dürfen, wie sie genutzt werden dürfen und wann sie zu löschen sind;
- ob und unter welchen Voraussetzungen und in welchem Stadium des Verfahrens der Bewerber sich Tests, Untersuchungen und Überprüfungen zu unterziehen hat;
- ob und inwieweit private Institutionen daran mitwirken und welche vertraglichen Sicherungen zum Schutz personenbezogener Daten zu vereinbaren sind;
- daß die Daten jeweils erst zu dem Zeitpunkt, in dem sie für das Verfahren erforderlich werden, und mit dem geringstmöglichen Eingriff erhoben werden"

(so wörtlich der Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. September 1991 zum Datenschutz im Recht des öffentlichen Dienstes, vgl. Anlage 1).

Danach ist Transparenz eine wesentliche datenschutzrechtliche Kategorie in diesem Zusammenhang. Es würde zur Verstärkung dieser Transparenz erheblich beitragen, wenn es möglich wäre, die für das Einstellungsverfahren maßgeblichen Regelungen möglichst umfassend in eine einzige Verwaltungsvorschrift aufzunehmen. Die Zusammenfassung würde zudem den Bestrebungen zur Verwaltungsvereinfachung (Reduzierung der Zahl der Verwaltungsvorschriften) dienen.

Da einige der genannten Verwaltungsvorschriften (insbesondere Nrn. 1, 2, 3) nur einen sehr geringen Umfang haben (etwa ein Drittel einer Druckspalte), würde auch die Übersichtlichkeit der Regelungen bei einer Zusammenfassung gesteigert werden; praktische Schwierigkeiten wären kaum zu erwarten.

Eine entsprechende „Kodifikation" könnte schließlich dazu führen, daß möglicherweise noch vorhandene Regelungslücken besser erkannt und geschlossen werden.

Der LfD hat dies gegenüber dem Ministerium des Innern und für Sport angeregt. Dieses hat angekündigt, nach Erlaß des Landesbeamtengesetzes entsprechende Vorschläge vorzulegen.

17.2 Personalverwaltungs-/Personalinformationssysteme

Die Ausstattung der Personalverwaltungen mit EDV-Anlagen ist im Berichtszeitraum erheblich vorangeschritten. Die Personalverwaltungen größerer Behörden nutzen die EDV im Rahmen von Personalinformations- oder Personalverwaltungssystemen nahezu flächendeckend für ihre Zwecke.

Die Unterscheidung der Begriffe Personalverwaltungs- und Personalinformationssystem war in der Vergangenheit für die Frage der Mitbestimmung bedeutsam. Auf der Grundlage des neuen Personalvertretungsgesetzes (s. o. 17.1.1) besitzt diese Unterscheidung keine praktische Bedeutung mehr; auch bloße Personalverwaltungssysteme unterliegen der Mitbestimmung.

Der LfD hat auf folgende Gesichtspunkte bei der Einführung entsprechender Systeme besonderes Gewicht gelegt:

- Auch innerhalb der Personalverwaltung müssen Zugriffsbeschränkungen existieren, die sich strikt am Erforderlichkeitsgrundsatz orientieren.

- Durch geeignete Maßnahmen ist sicherzustellen, daß sensible Merkmale (etwa Informationen über Prüfungs- und Beurteilungsnoten; Ausübung von Nebentätigkeiten u. ä.) nur dann genutzt werden, wenn dies erforderlich ist. Geeignete Mittel in diesem Zusammenhang, die der LfD empfohlen hat, sind etwa: Protokollierung auch des Lesezugriffs auf diese Daten unter Speicherung des Anlasses; Aufruf dieser Informationen nur durch Eingabe besonderer Befehle, nicht dagegen im Zusammenhang mit den sogenannten „Personalstammdaten" beim routinemäßigen Aufruf von Datensätzen.

- Zur Erfüllung der gesetzlichen Anforderungen (§ 2 Abs.3 LDatG i. V. m. § 33 BDSG) sollte bei der Einführung des Personalinformationssystems jedem Beschäftigten ein Ausdruck mit den über ihn gespeicherten Daten zur Verfügung gestellt

werden. Dies hat sich (u. a. unter dem Aspekt der Kontrolle der Richtigkeit der gespeicherten Daten) bewährt, auch wenn die gesetzliche Pflicht schon durch eine Benachrichtigung von der Speicherung und der Art der Daten erfüllt ist (§ 33 Abs. 1 S. 1 BDSG). Es ist sicherzustellen, daß ein solcher Ausdruck jederzeit auf Verlangen einer mit ihren Daten gespeicherten Person gefertigt werden kann (vgl. § 12 LDatG).

17.3 Zeiterfassungssystem

Auch der Einsatz von Zeiterfassungssystemen, die die automatisierte Datenverarbeitung nutzen, ist weiter vorangeschritten.

In der Öffentlichkeit hat besondere Beachtung gefunden, daß die obersten Landesbehörden ein entsprechendes System einsetzen. Das Augenmerk des LfD war in diesem Zusammenhang in erster Linie auf folgende Punkte gerichtet:

- Die Auswertung der gespeicherten detaillierten Daten zu jedem einzelnen Bediensteten darf – entsprechend der Anforderung in der Arbeitszeitverordnung – nur zum Zweck der Überwachung der Arbeitszeiten erfolgen. In diesem Zusammenhang hat der LfD allerdings keine Bedenken dagegen geäußert, daß die Gründe für das Fernbleiben vom Dienst – Urlaub, Krankheit, Dienstbefreiung etc. – ebenfalls in das Zeiterfassungssystem eingegeben werden. Auch diese Speicherung kann dem genannten Zweck zugeordnet werden.

- In Dienstanweisungen oder auch Dienstvereinbarungen mit dem Personalrat ist genau zu regeln, welche Stellen innerhalb einer Personalverwaltung und innerhalb einer Behörde insgesamt welche Informationen aus dem Zeiterfassungssystem erhalten dürfen. Dies muß zu einer konkreten Regelung von Nutzungsprofilen einzelner Stellen führen. Auf der Ebene des Landes ist dies im Rahmen der Formulierung einer Musterdienstvereinbarung in Zusammenarbeit mit dem Ministerium der Finanzen erfolgt.

- Technische und organisatorische Datenschutzmaßnahmen müssen diese Vorgaben absichern. Der LfD hat sich bemüht, durch intensive Begleitung der Einrichtung entsprechender Verfahren hierauf hinzuwirken.

17.4 Beihilfeverfahren

17.4.1 Zentralisierung der Verfahren

Bereits seit langem ist die Zentralisierung der Beihilfebearbeitung auf einige wenige Beihilfestellen in Rheinland-Pfalz geplant. Aus datenschutzrechtlicher Sicht ist damit für die Bediensteten der faktische Zwang verbunden, höchst sensible Gesundheitsdaten an eine andere als die bisher zuständige Stelle zu offenbaren.

Die neu zuständigen Beihilfestellen werden zudem zentral eine Reihe sensibler Daten der betroffenen Bediensteten im Zugriff haben (unter Nutzung des unter Tz. 17.4.2 geschilderten BABSY-Systems).

Dem stehen aus datenschutzrechtlicher Sicht allerdings auch gewichtige Vorteile gegenüber: So ist die Einhaltung der im Beamtenrechtsrahmengesetz verankerten Pflicht, Beihilfedaten grundsätzlich nur zweckgebunden und nicht für Zwecke der allgemeinen Personalverwaltung zu nutzen, dann auch verfahrenstechnisch abgesichert, wenn die Beihilfesachbearbeitung organisatorisch völlig von der Personalverwaltung getrennt ist. Zudem ist gerade in kleineren Verwaltungen die unangenehme Situation, daß ein Kollege, der sich in einer ständigen Nähe zum Betroffenen befindet, intimste Details über dessen gesundheitliche Situation und die seiner Familie kennt, vermieden. Grundsätzlich ist diese Entwicklung also zu begrüßen.

Dennoch stellt sich angesichts der eingangs skizzierten Situation die Frage, ob die geplante Zentralisierung der Beihilfestellen nicht einer gesetzlichen Grundlage bedarf.

Hierfür sprechen folgende Gesichtspunkte:

- Mit der Zentralisierung der Beihilfebearbeitung ist nicht nur die Verlagerung einer technischen Aufgabe verbunden, die als technische Hilfstätigkeit bezeichnet werden könnte. Es handelt sich auch nicht nur um die Begründung eines datenschutzrechtlichen Auftragsverhältnisses. Die personalverwaltenden und personalaktenführenden Stellen geben vielmehr einen Teil ihrer Zuständigkeit an eine andere Stelle ab, die eigene Prüfungen und in Einzelfällen auch Ermessensentscheidungen vorzunehmen hat.

- Außerdem ist § 7 des Verkündungsgesetzes zu beachten, wonach die Verlagerung von Zuständigkeiten einer gesetzlichen Grundlage bedarf.

- Schließlich ist an den Parallelvorgang des Übergangs von Kompetenzen im Rahmen der Gehaltszahlung auf die Zentrale Besoldungs- und Versorgungsstelle (ZBV) zu erinnern: Auch dort hat man – zutreffenderweise – den Zuständigkeitsübergang durch eine gesetzliche Grundlage (die ZBV-Zuständigkeitsverordnung vom 22. Mai 1985, BS 2032-22) geregelt.

Aus der Sicht des LfD ist insbesondere angesichts der geschilderten Auswirkungen des geplanten Zuständigkeitsübergangs auf das informationelle Selbstbestimmungsrecht der Betroffenen eine gesetzliche Grundlage für diese Zentralisierung erforderlich.

Das Ministerium der Finanzen hat am 27. Juli 1993 eine entsprechende Rechtsverordnung erlassen (GVBl. S. 428).

17.4.2 Automatisiertes Beihilfeverfahren „BABSY"

a) Das zentrale Beihilfeverfahren BABSY hat Grundsatzfragen aufgeworfen. Die zentralisierte Datenverarbeitung führt im vorliegenden Zusammenhang dazu, daß – im Endausbaustadium des Verfahrens – für alle Landesbediensteten an einer zentralen Stelle Gesundheitsdaten automatisiert gespeichert werden. Diese Gesundheitsdaten sind zum Teil überaus sensitiver Natur (beispielsweise wenn Speicherungen im Zusammenhang mit Aufwendungen für psychologische Behandlungen betroffen sind). Die Datenschutzbeauftragten des Bundes und der Länder haben wiederholt gefordert, gesetzlich zu regeln, daß weder Diagnosen noch sonstige medizinische und psychologische Einzelangaben von Arbeitnehmern durch den Arbeitgeber (bzw. den Dienstherrn) automatisiert gespeichert werden dürfen.

   In diesem Zusammenhang ist auch von Bedeutung, welche Zugriffsmöglichkeiten die ZBV unmittelbar bzw. die bei der ZBV einzurichtende Leitstelle besitzen.

b) Zum Datensatz

   BABSY ändert die derzeit eingesetzten Abrechnungssysteme bei der Automatisierung der Beihilfeverfahren grundsätzlich, weil hier konkrete Krankheitsdaten automatisiert gespeichert werden sollen. So wird beispielsweise bezüglich der Sehhilfen detailliert gespeichert, welche Brille mit welchen Korrekturmöglichkeiten verordnet worden ist. Bei Krankenhausaufenthalten werden das Einlieferungsdatum, das Entlassungsdatum, der allgemeine Pflegesatz, die Anzahl der Tage, die Unterbringung in Ein- oder Zweibettzimmern und Krankenhausnebenkosten gespeichert. Es werden Informationen gleicher Art über Sanatoriumsaufenthalte und Aufenthalte in anderweitigen Unterbringungsorten gespeichert, ebenso Informationen über Heilkuren. Aus der Sicht des LfD wäre hier eine Reduzierung der Datenfelder anzustreben. Im übrigen ist sehr fraglich, ob die detaillierten Angaben insoweit wirklich für längere Zeit gespeichert werden müssen. Besonders bedeutsam sind aus datenschutzrechtlicher Sicht wohl die Angaben über psychologische Behandlungen. Hier sind Angaben zum Antrag auf Genehmigung gespeichert: Eine Gruppe mit maximal 30 Ausprägungen ermöglicht detaillierte Angaben. Außerdem wird die GOÄ-Ziffer, die vom Psychologen abgerechnet wird, gespeichert. Eine derart umfassende Datenspeicherung sollte unterbleiben.

   Bereits die dauerhafte automatisierte Speicherung der eingereichten Rechnungen mit den Angaben Datum, Höhe des Rechnungsbetrages, Art der Leistung (differenziert nach neun Gruppen) bedeutet einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen und stellt eine qualitativ neue Situation gegenüber dem bisherigen Zustand dar.

c) Insbesondere war zu kritisieren, daß ein solch detailliertes Konzept erarbeitet wurde, ohne bereits konkrete Löschungsfristen festzulegen.

d) Die Funktionen der Leitstelle als zentrale Meldestelle für Abrechnungsfehler, als abschließend bearbeitende Stelle der Buchungsbelege (Auszahlungsanordnung) und als Verbindungsstelle zur auszahlenden Stelle (OFK) sind aus datenschutzrechtlicher Sicht ebenfalls zu konkretisieren und ggf. zu beschränken. Dies gilt insbesondere, soweit weder das Finanzministerium noch die ZBV als Festsetzungsstelle fungieren.

17.4.3 Das neue Antragsformular

Von einem Bezirkspersonalrat für Lehrer ist der LfD auf folgende Problematik im Zusammenhang mit der Gestaltung des Beihilfeformulars aufmerksam gemacht worden:

Bei erstmaliger Antragstellung mit dem Vordruck seien alle Fragen, insbesondere auch die Fragen 2 bis 7, die den Ehegatten des Antragstellers betreffen, auszufüllen, unabhängig davon, ob für den Ehegatten überhaupt Beihilfeleistungen beantragt würden.

Fraglich ist, ob diese Anforderung dem Erforderlichkeitsgrundsatz entspricht. In den Fällen, in denen für den Ehegatten des Beihilfeberechtigten keine Beihilfe beansprucht wird, etwa weil er grundsätzlich keine Beihilfe geltend machen will oder weil er anderweitig vollständig abgesichert ist (als Mitglied der gesetzlichen oder einer privaten Krankenversicherung), dürften für die Beihilfestelle nur die Informationen erforderlich sein, die für die Berechnung der Beihilfe des Beihilfeberechtigten selbst maßgeblich sind. Dies sind also die Informationen, die die Erhöhung des Beihilfeprozentsatzes beim Antragsteller begründen. Ob unter diesem Aspekt in jedem Fall die Information über die Berufstätigkeit oder eine Berufsausbildung des Ehegatten

erforderlich ist, ob der Arbeitgeber bzw. die Beschäftigungs-/Ausbildungsstätte des Ehegatten von Bedeutung für diese Frage ist sowie ob die Information über das Getrenntleben beihilferechtliche Folgen hat, ist für den LfD derzeit noch zweifelhaft (vgl. § 12 BeihilfenVO).

Schließlich ist die Information über das genaue Datum/Jahr der Eheschließung, Verwitwung, Scheidung oder des Getrenntlebens wohl kaum erforderlich. Bedeutsam dürfte nur sein, ob die Tatbestände „verheiratet" oder „Bezieher von Witwengeld" im Zeitpunkt der Antragstellung vorlagen (§ 12 BVO).

Die Erörterung dieser Fragen ist noch nicht abgeschlossen.

17.4.4 Beiziehung externer Gutachter

Nach § 3 Abs. 1 der Beihilfenverordnung sind die notwendigen Aufwendungen in angemessenem Umfang beihilfefähig. Über die Notwendigkeit und den angemessenen Umfang der Aufwendungen entscheidet die Festsetzungsstelle; sie kann hierzu Gutachten einholen.

Aus einer Eingabe ergab sich, daß es aus datenschutzrechtlicher Sicht problematisch ist, wenn die Beihilfestelle ohne vorherige Unterrichtung des Antragstellers eine dritte Stelle (im vorliegenden Fall ein Gesundheitsamt) mit der Erstellung eines entsprechenden Gutachtens beauftragt. Es kann vielmehr durchaus berechtigte Interessen des Antragstellers geben, die gerade die Einschaltung des vorgesehenen Gutachters als bedenklich erscheinen lassen (wenn etwa Personen aus dem persönlichen oder beruflichen Umfeld des Betroffenen Kenntnis von dem Gutachtenverfahren erlangen können).

Aus der Sicht des LfD ist es deshalb angemessen, grundsätzlich vorzusehen, daß vor der Einholung eines externen Gutachtens der Antragsteller über die entsprechende Absicht sowie über den vorgesehenen Gutachter zu informieren ist. Der Antragsteller sollte dadurch Gelegenheit erhalten, etwa bestehende Einwendungen geltend zu machen oder auch ggf. seinen Beihilfeantrag zurückzuziehen.

Das Ministerium der Finanzen hat diese Anregung aufgegriffen und ein entsprechendes Rundschreiben erlassen.

17.4.5 Verfahren bei Sterilisationen/Abtreibungen

Die zentrale Erfassung der Beihilfeanträge in Fällen nicht rechtswidriger Sterilisationen und nicht rechtswidriger Schwangerschaftsabbrüche beim Ministerium der Finanzen war Gegenstand der Berichterstattung im letzten Tätigkeitsbericht (13. Tb., Tz. 17.9.2). Zwischenzeitlich ist – entsprechend der Ankündigung des Ministeriums – die Beihilfenverordnung so geändert worden, daß eine zentrale Entscheidung in diesen Fällen im Regelfall unzulässig geworden ist: § 10 a Abs. 2 der BVO (in der Fassung vom 1. März 1993) sieht keine besondere Behandlung dieser Aufwendungen vor. Das Problem wird zudem für eine große Zahl von Bediensteten durch die Zentralisierung der Beihilfestellen entschärft: Dann ist auch die Kenntnisnahme von derart sensiblen Vorgängen in der eigenen Kollegenschaft grundsätzlich nicht mehr möglich.

Allerdings bleibt es datenschutzrechtlich unbefriedigend, daß die Verfahrensweise der Vergangenheit Spuren hinterlassen hat, die nicht einfach zu beseitigen sind. So ergab eine Eingabe, daß in der Personalakte eines Beamten noch der gesamte Schriftwechsel mit dem Ministerium der Finanzen über die vor sechs Jahren beantragte Beihilfe zu einer Sterilisation aufbewahrt wurde. Erst nach Einschaltung des LfD wurden diese Vorgänge vernichtet. Die personalaktenführenden Stellen hätten von Amts wegen solche Vorgänge aus den Personalakten entfernen müssen. Die praktische Umsetzung einer solchen Anforderung ist allerdings deshalb schwierig, weil es keine zentrale Erfassung derjenigen Bediensteten gibt, die in der Vergangenheit Beihilfe zu einer der hier relevanten Fallgruppen beantragt haben. Ein Hinweis des oder der Betroffenen selbst auf die Entfernung entsprechender Vorgänge in der sie betreffenden Personalakte dürfte also in jedem Fall zumindest hilfreich sein.

17.4.6 Beauftragung externer Unternehmen

Es dürfte inzwischen eine große Zahl von rheinland-pfälzischen Gemeinden die Pfälzische Pensionsanstalt in Anspruch nehmen, um die Beihilfesachbearbeitung durchzuführen. Außerdem wird diskutiert, ob und auf welcher Basis private Versicherungen die Aufgabe der Beihilfegewährung, insbesondere für Gemeinden gegenüber deren Bediensteten, wahrnehmen können.

Grundsätzlich bietet eine solche Verlagerung auch erhebliche datenschutzrechtliche Vorteile für die Betroffenen (s. o. Tz. 17.4.1). Auch hier stellt sich allerdings die Frage, welche Rechtsgrundlage als Basis einer solchen Verfahrensänderung zu fordern ist. Ohne besondere Rechtsgrundlage wäre dies möglich, wenn es sich hier um eine Datenverarbeitung im Auftrag handeln würde. Eine besondere Rechtsgrundlage wäre erforderlich, wenn ein ganzer Aufgabenkomplex an eine andere Stelle übertragen würde.

Im letzteren Fall wäre eine Aufgabenwahrnehmung durch die beauftragte Stelle wohl nur auf der Basis einer Rechtsverordnung oder – im gemeindlichen Bereich – möglicherweise auf der Grundlage einer gemeindlichen Satzung zulässig.

Diese Frage beurteilt sich wesentlich danach, ob die beauftragte Institution hier ausschließlich Hilfstätigkeiten ausübt, die als „Auftragsdatenverarbeitung" angesehen werden können, ob sie z. B. nur Daten nach bestimmten Vorgaben verarbeitet, oder ob sie auch eigene Entscheidungen trifft. Nach den dem LfD vorliegenden Verträgen entscheiden die beauftragten Institutionen z. B. über folgende Fragen:

- Einschaltung eines Gutachters gem. § 3 Abs. 1 der Beihilfenverordnung;
- Anerkennung von Belegen;
- Entscheidung über die Angemessenheit von ärztlichen Leistungen;
- Vorschlag bei der Gewährung von Kann-Leistungen, über den von der Gemeinde entschieden wird.

Bedeutsam dürfte auch sein, wer jeweils Urheber des Beihilfebescheides ist.

Dieser Fragenkomplex wird derzeit auch im Kreis der Landesbeauftragten für den Datenschutz erörtert. Eine abschließende Beurteilung ist dem LfD noch nicht möglich.

17.4.7 Schutz der Daten Angehöriger gegenüber dem Beihilfeberechtigten?

Der LfD hat bereits im letzten Tätigkeitsbericht dargestellt, daß es durchaus berechtigte Anliegen der Angehörigen geben kann (etwa bei getrennt lebenden Ehegatten, bei erwachsenen in Ausbildung befindlichen Kindern u. ä.), ihre Krankheiten gegenüber dem Beihilfeberechtigten nicht zu offenbaren (13. Tb., Tz. 17.9.3). Erneute Eingaben haben gezeigt, daß es sich hier um ein reales und im Einzelfall sogar existentielles Problem für die Betroffenen handelt.

Auch andere Datenschutzbeauftragte haben die hier bestehenden datenschutzrechtlichen Fragen bereits mit den in ihrem Bereich zuständigen Ressorts erörtert. Folgende Verfahrensweisen haben hier zu Verbesserungen geführt:

a) In Bremen können Familienangehörige von Beihilfeberechtigten selbständig die Erstattung beihilfefähiger Aufwendungen beantragen, ohne daß der Beihilfeberechtigte darüber informiert wird. Die Erstattung wird auf das vom Antragsteller angegebene Konto überwiesen. Die Unterlagen werden im geschlossenen Umschlag für fünf Jahre zur Beihilfeakte des Beihilfeberechtigten genommen und dürfen nur unter bestimmten Voraussetzungen geöffnet werden. Dem Beihilfeberechtigten selbst dürfen nur bei Vorliegen eines berechtigten Interesses, etwa bei Verfahren gegen getrenntlebende Ehepartner, mitgeteilt werden, daß z. B. Arztkosten oder Arzneikosten erstattet worden seien. Der Antragsteller wird mit einem Merkblatt darauf hingewiesen, daß der Beihilfeberechtigte unter bestimmten Voraussetzungen Auskunft erhält.

b) Die Bundesbehörden verfahren auf folgender Grundlage: Der Innenausschuß des Deutschen Bundestages hat sich in seiner Sitzung am 7. Oktober 1992 der Auffassung der Bundesregierung angeschlossen, daß der datenschutzrechtlichen Interessenlage der Angehörigen durch eine vernünftige, praxisorientierte Verfahrensgestaltung im Rahmen des geltenden Rechts Rechnung getragen werden kann. So können die betreffenden Familienangehörigen ihre Belege unmittelbar der Beihilfestelle zuleiten, während der Beihilfeberechtigte hierauf lediglich pauschal Bezug nimmt. Die Belege werden dann von der Beihilfestelle auch unmittelbar an das betroffene Familienmitglied zurückgesandt. Unter diesen Umständen hat der Innenausschuß davon abgesehen, dem Bundestag eine Rechtsänderung zur Schaffung eines eigenen Beihilfeanspruchs für Angehörige vorzuschlagen.

c) Der Hamburgische Senat hat in diesem Zusammenhang erklärt, die zuständige Besoldungs- und Versorgungsstelle werde im Rahmen des geltenden Rechts weiterhin den datenschutzrechtlichen Belangen der Angehörigen im Beihilfeverfahren Rechnung tragen. Dies geschehe dadurch, daß z. B. Beihilfeanträge von Angehörigen in Vollmacht des Berechtigten gestellt werden oder daß Angehörige ihre Belege direkt einreichen und unmittelbar zurückerhalten könnten.

Nach wie vor ist der LfD der Auffassung, daß die grundsätzlich wirksamste Lösung des Problems darin bestehen würde, volljährigen Angehörigen des Beihilfeberechtigten einen unmittelbaren Beihilfeanspruch gesetzlich zuzubilligen. Die genannten Beispiele zeigen aber, daß es bei gutem Willen der Landesbehörden möglich ist, auch bereits auf der Basis des geltenden Rechts auf die Besonderheiten in Einzelfällen Rücksicht zu nehmen.

Das Finanzministerium hat sich bislang einer generellen Lösung dieser Frage verschlossen. Der LfD erwartet jedoch, daß die genannten Beispiele aus dem Bund und aus anderen Bundesländern dazu beitragen, die Kompromißbereitschaft des Ministeriums zu erhöhen.

17.5 Befugnisse des behördlichen Datenschutzbeauftragten in bezug auf die Personalaktenführung

Schon jetzt, vor einer gesetzlichen Verpflichtung aller Behörden, unter bestimmten Voraussetzungen behördliche Datenschutzbeauftragte zu benennen (wie sie im Entwurf des LDatG vorgesehen ist), haben viele Verwaltungen als Maßnahme des organisatorischen Datenschutzes einen Bediensteten mit der Wahrnehmung dieser Aufgabe betraut. Fraglich war, ob der interne behördliche Datenschutzbeauftragte die Befugnis hat, personenbezogene Daten von Bürgern und Bediensteten zur Kenntnis zu nehmen, wenn dies der datenschutzrechtlichen Kontrolle dient. Nach der Auffassung des LfD ist hier § 56 Abs. 3 Beamtenrechtsrahmengesetz (bzw. künftig die inhaltsgleiche Vorschrift im Landesbeamtengesetz) bedeutsam. Danach dürfen nur solche Beschäftigte Zugang zur Personalakte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit es zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist; dies gilt auch für den Zugang im automatisierten Abrufverfahren.

Nach dem allgemeinen Datenschutzrecht wird die Ausübung von Kontrollen und von Aufsicht nicht als anderer Zweck im Vergleich zum ursprünglichen Speicherungszweck angesehen (vgl. z. B. § 14 Abs.3 Satz 1 BDSG). Demnach ist die datenschutzrechtliche Kontrolle der ordnungsgemäßen Personalaktenführung als Maßnahme der Personalverwaltung anzusehen. Auch unter diesem Aspekt hat der LfD die Auffassung vertreten, daß es der Dispositionsbefugnis des öffentlichen Arbeitgebers unterliegt, ob er seine Pflicht zur Aufsicht über den Einsatz der EDV im Personalbereich mit Unterstützung des behördlichen Datenschutzbeauftragten erfüllen will, oder ob er diese Aufgabe den Mitarbeitern der Personalabteilung selbst überläßt. Er kann jedenfalls nicht unter Berufung auf zwingende datenschutzrechtliche Überlegungen eine Einschränkung der Befugnisse des behördlichen Datenschutzbeauftragten begründen.

Ein Blick auf die Befugnisse der behördlichen Datenschutzbeauftragten im Bereich der Sozialleistungsträger, die dem Sozialgeheimnis unterworfen sind, bestätigt dieses Ergebnis. Auch in diesem Zusammenhang hat der LfD die Auffassung vertreten, daß der behördliche Datenschutzbeauftragte nach dem Sozialgesetzbuch im Rahmen seiner Kontrolltätigkeit auch das Recht auf Einsicht in Vorgänge hat, die dem Sozialgeheimnis unterliegen.

Etwas anderes dürfte allerdings im Bereich des Arztgeheimnisses für Krankenhausdatenschutzbeauftragte gelten.

Derzeit ist noch nicht abzusehen, ob das neue LDatG hierzu Klarstellungen enthalten wird.

18 Datenschutz im kommunalen Bereich

18.1 Novellierung kommunalrechtlicher Vorschriften

Die Novellierung kommunalrechtlicher Vorschriften zielte zwar hauptsächlich auf die Einführung der Urwahl von Bürgermeistern und Landräten, erstreckte sich aber auch auf Bestimmungen mit Datenschutzrelevanz, wie z. B. die Schweigepflicht von Bürgern und Einwohnern, die zu einem Ehrenamt oder zu einer ehrenamtlichen Tätigkeit berufen werden (§ 20 Gemeindeordnung – GO –, § 14 Landkreisordnung – LKO –). Die frühere Fassung der Vorschrift entsprach nicht mehr einem zeitgemäßen Verständnis von Datenschutz in der öffentlichen Verwaltung, denn die Einschränkung der Verschwiegenheitspflicht auf solche Angelegenheiten, deren Geheimhaltung besonders vorgeschrieben ist, kollidiert, soweit personenbezogene Daten betroffen sind, mit dem umfassenden Geltungsanspruch des Datenschutzgesetzes und der Geheimhaltungspflicht nach § 30 Verwaltungsverfahrensgesetz. Soweit berechtigte Interessen einzelner berührt sind, bedarf es zu deren Schutz keines Beschlusses der Vertretungsorgane, denn dieser Schutz besteht aufgrund der datenschutzrechtlichen Vorschriften und ihrer Strafbewehrung. Die Änderungsempfehlung des LfD zum Referentenentwurf wurde im weiteren Gesetzgebungsverfahren berücksichtigt.

Mit dem Verzicht auf die Angabe des Geburtsdatums in Unterschriftenlisten für Bürgerinitiativen (§ 17 Abs. 2 GemO) wird einer Empfehlung der Enquete-Kommission „Möglichkeiten direkter Bürgerbeteiligung und -entscheidung der repräsentativen Demokratie" – Drs. 11/4707, Tz. III.4 – gefolgt. Der LfD begrüßt diese Problemlösung, weil gerade die Angabe des Geburtsdatums in der Vergangenheit immer wieder in Eingaben beklagt wurde.

Empfehlungen des LfD zur Änderung der Vorschriften über das Unterrichtungsrecht des Gemeinderats (§ 33 GemO) und des Kreistags (§ 26 LKO) wurde zwar nicht vollständig entsprochen. Die schließlich gewählte Fassung ist geltendem Datenschutzrecht, aber weitestgehend angenähert: Die Bestimmungen über die Aushändigung der Prüfungsmitteilungen, über das Verlangen auf Akteneinsicht und über Mündliche Anfragen gelten nicht, wenn und soweit für die Vorgänge eine Geheimhaltung besonders vorgeschrieben ist oder überwiegende schutzwürdige Interessen Betroffener entgegenstehen. Damit sind alle Vorgänge, die dem Steuergeheimnis, dem Personalaktengeheimnis, dem Sozialgeheimnis und dem Statistikgeheimnis unterliegen, hinreichend geschützt. Eine gesetzlich vorgeschriebene Abwägung zwischen dem Informationsinteresse und den schutzwürdigen Interessen Betroffener entspricht geltendem Datenschutzrecht. Die weitergehende Empfehlung des LfD ging dahin, die Übermittlungs- oder Nutzungsrestriktionen, die sich aus dem novellierten Datenschutzgesetz ergeben werden, in den Anwendungsbereich der Gemeindeordnung einzubeziehen.

18.2 Bürgerfreundlichkeit

Die Anforderungen des Datenschutzes stehen dem Bemühen um Bürgerfreundlichkeit grundsätzlich nicht entgegen. Das Datenschutzrecht bietet genügend Gestaltungsmöglichkeiten, um die Verwaltung bürgernah zu organisieren – beispielsweise durch Einrichtung von Bürgerbüros – oder Verfahren zu realisieren, die gleichermaßen bürgerfreundlich wie datenschutzgerecht sind.

So ist beispielsweise unter Datenschutzgesichtspunkten grundsätzlich nichts dagegen einzuwenden, daß bei einer Verbandsgemeinde beantragte Personalausweise oder Reisepässe nach ihrer Fertigstellung dem Ortsbürgermeister zugeleitet werden, der sie dann den Antragstellern aushändigt. Dieses Verfahren ist bürgerfreundlich, weil es den Antragstellern den erneuten Weg zur Verbandsgemeindeverwaltung erspart.

Voraussetzung für diesen Bürgerservice ist indessen, daß sich die Antragsteller damit einverstanden erklären, denn der Ortsbürgermeister ist eine in das Verwaltungsverfahren von Gesetzes wegen nicht einbezogene öffentliche Stelle.

In seiner Stellungnahme zu einer Eingabe meinte der Bürgermeister einer Verbandsgemeinde, die Sache hätte keinen Datenschutzbezug, denn die den Ortsbürgermeistern zur Weiterleitung übergebenen Ausweise enthielten lediglich Daten, die ihnen ohnehin bekannt seien. Dabei blieb freilich unberücksichtigt, daß bereits die Tatsache der Beantragung eines Reisepasses eine Information darstellt, die dem Ortsbürgermeister üblicherweise nicht bekannt ist. Unbekannt sind ihm beispielsweise auch die Seriennummer von Ausweisdokumenten, die grundsätzlich den schutzwürdigen Daten zuzurechnen ist, sowie die Gültigkeitsdauer, die beispielsweise in Fällen des § 7 Abs. 2 Paßgesetz – Beschränkung der Gültigkeitsdauer an Stelle einer Paßversagung – von besonderer Sensitivität sein kann.

Die mit Hinweisen zur datenschutzrechtlichen Beurteilung verbundene Empfehlung des LfD, ein Zustimmungsverfahren einzuführen, wurde von der Verbandsgemeinde akzeptiert.

18.3 Auskunftsrechte von Ratsmitgliedern versus Persönlichkeitsrechte Betroffener

Ein Bürgermeister beschwerte sich beim LfD darüber, daß einem Mitglied des Kreistags vom Landrat die Gründe bekanntgegeben wurden, die der Ansiedlung eines Gewerbebetriebs in einem Landschaftsschutzgebiet entgegenstanden. Von datenschutzrechtlicher Relevanz war der Vorgang insoweit, als die Kreisverwaltung dem Ratsmitglied die Ergebnisse von Anfragen beim Grundbuchamt mitteilte und aufgrund dieser Ergebnisse landespflegerisch weniger empfindliche Alternativen zu der Gewerbeansiedlung aufzeigte.

Im datenschutzrechtlichen Sinne stellten die Angaben über die Eigentumsverhältnisse personenbezogene Informationen dar, die offenbart wurden. Eine solche Offenbarung ist zulässig, wenn die betroffenen Grundstückseigentümer zustimmen – was konkret nicht der Fall war – oder wenn sie auf eine gesetzliche Offenbarungsbestimmung gestützt werden kann. An einer solchen Offenbarungsbestimmung fehlte es. Zwar kann § 26 Landkreisordnung – der das Unterrichtungsrecht des Kreistags regelt – grundsätzlich Informationseingriffe rechtfertigen. Dieses Unterrichtungsrecht steht aber, von nicht einschlägigen Sonderregelungen in Absatz 3 abgesehen, nur dem Kreistag in seiner Gesamtheit zu.

Im Rahmen der rechtlichen Würdigung des Vorganges war aber auch zu berücksichtigen, daß Informationen über das Eigentum an Grundbesitz für jedermann leicht zu beschaffen sind. Die Grundbuchordnung wie auch das Katastergesetz nennen als Zugangsvoraussetzung zu derartigen Informationen im Grundbuch und im Liegenschaftskataster lediglich das „berechtigte Interesse". Angesichts der vielfältigen Verpflichtungen, die sich aus dem Grundeigentum ergeben, wäre eine höhere Zugangsschwelle zu Informationen hierüber nicht verhältnismäßig.

Wegen der geringen Sensitivität der offenbarten Informationen ließ es der LfD dabei bewenden, die Kreisverwaltung über die rechtliche Würdigung zu unterrichten. Von einer förmlichen Beanstandung wurde abgesehen.

18.4 Datenschutz und Öffentlichkeitsarbeit

Es ist eine beklagenswerte Tatsache, daß geheimhaltungsbedürftige Vorgänge von Mitgliedern kommunaler Vertretungskörperschaften bisweilen unter Verstoß gegen gesetzliche Verschwiegenheitspflichten an die Presse weitergegeben werden. Diese Thematik war des öfteren Gegenstand von Eingaben an den LfD. Einschlägige Erfahrungen gaben deshalb Veranlassung, gegen eine Ausweitung der Auskunfts- und Akteneinsichtsrechte von Ratsmitgliedern im Rahmen einer Novellierung der Gemeindeordnung zu votieren.

Der für die Festsetzung eines Ordnungsgeldes erforderliche Nachweis eines Verstoßes gegen gesetzliche Vorschriften ist mit den einer Kommunalverwaltung zur Verfügung stehenden Aufklärungsmitteln kaum zu führen. Weil staatsanwaltschaftliche Ermittlungen zweifellos erfolgversprechender sind, macht der LfD von seinem Strafantragsrecht nach § 27 LDatG Gebrauch, sofern die unbefugte Übermittlung von Daten aus dem Anwendungsbereich des Landesdatenschutzgesetzes in Rede steht und

die Anschuldigungen substantiiert sind. In aller Regel werden indessen die durch ein Ratsmitglied offenbarten Daten nicht in den formalen Anwendungsbereich des Landesdatenschutzgesetzes (Dateiverarbeitung, automatisiertes Verfahren) fallen.

Eine Offenbarung von Informationen, die dem Aktengeheimnis des § 30 Verwaltungsverfahrensgesetz unterliegen, wird allgemein als zulässig angesehen, soweit sie für die Richtigstellung unwahrer Tatsachenbehauptungen des Betroffen erforderlich ist. In Fällen, in denen derartige Behauptungen öffentlich erhoben wurden, ist auch eine öffentliche Richtigstellung unter Beachtung des Verhältnismäßigkeitsgrundsatzes zulässig.

Sofern es indessen nicht um die Information der Presse durch den Betroffenen, sondern um personenbezogene Informationen geht, die der Presse durch ein der Verwaltung nicht bekanntes Ratsmitglied zur Verfügung gestellt wurden, ist zu berücksichtigen, daß sowohl die Bestätigung der Richtigkeit der veröffentlichten Informationen wie auch deren Richtigstellung eine Offenbarung i. S. des § 30 Verwaltungsverfahrensgesetz darstellt. Im rechtlichen Sinne ist diese Offenbarung als Eingriff in die Persönlichkeitsrechte des Betroffenen zu qualifizieren. Da eine gesetzliche Eingriffsgrundlage nicht existiert, ist die Offenbarung personenbezogener Daten im Rahmen einer öffentlichen Stellungnahme nur mit der Zustimmung des Betroffenen zulässig.

Sofern diese Zustimmung nicht eingeholt oder erteilt wird, kann nur eine Stellungnahme in allgemeiner Form in Betracht kommen.

Die Verwaltung wird die Öffentlichkeit darüber unterrichten dürfen, daß ein Sachverhalt in der Presse unrichtig dargestellt wurde; sie wird im übrigen aber – erforderlichenfalls unter Hinweis auf datenschutzrechtliche Beschränkungen – eine Stellungnahme ablehnen müssen. Es müßte eine sehr schwerwiegende Beeinträchtigung des Erscheinungsbildes der öffentlichen Verwaltung in Rede stehen, um in der Abwägung Persönlichkeitsrechte der Betroffenen zurückstehen zu lassen (vgl. § 30 Abs. 4 Nr. 5 Buchst. c Abgabenordnung).

18.5 Bewirtschaftung von Verfügungsmitteln und Datenschutz

Nach § 11 Abs. 1 Nr. 1 Gemeindehaushaltsverordnung (GemHVO) können in kommunalen Haushalten Verfügungsmittel veranschlagt werden. Dies sind Beträge, die allein dem Bürgermeister zu dienstlichen Zwecken, für die keine Ausgaben veranschlagt sind, zur Verfügung stehen (§ 45 Nr. 30 GemHVO).

Ein Bürgermeister wollte wissen ob, es zulässig ist, im Rahmen des Entlastungsverfahrens nach § 114 Gemeindeordnung Art und Inhalt der Mittelbewirtschaftung in öffentlicher Ratssitzung zu erörtern. Es stellte sich damit die Frage, ob und inwieweit sich Amtsträger auf den Datenschutz oder auf das Recht auf informationelle Selbstbestimmung berufen können, denn es ist davon auszugehen, daß von einer öffentlichen Erörterung der Mittelbewirtschaftung in erster Linie das Handeln des Bürgermeisters als Amtsträger betroffen wäre. Der LfD vertritt hierzu – ebenso wie früher die DSK – die Auffassung, daß ein Amtsträger, der im Rahmen seiner amtlichen Tätigkeit nach außen für Dritte erkennbar handelt, nicht durch ein eigenes informationelles Selbstbestimmungsrecht geschützt ist (vgl. 13. Tb., Tz. 17.3). Konkret bedeutet dies, daß datenschutzrechtliche Gesichtspunkte der Wahrnehmung von Kontrollaufgaben durch den Stadtrat insoweit nicht entgegenstehen, als sich diese Kontrolle auf das Verhalten als Bürgermeister bezieht. Ob die Kompetenzzuweisungen der Gemeindeordnung der Erörterung in einer Ratssitzung entgegenstehen, ist nicht datenschutzrelevant und deshalb vom LfD nicht zu beurteilen.

Eine datenschutzrechtliche Relevanz besteht indessen in solchen Fällen, in denen durch die Erörterung des Inhalts der Mittelbewirtschaftung schutzwürdige Belange von Bürgern betroffen werden. Dies könnte etwa dann der Fall sein, wenn aus den Verfügungsmitteln Zahlungen an bestimmte Personen geleistet wurden.

Auch in diesen Fällen hat der örtliche Rechnungsprüfungsausschuß ein umfassendes Informationsrecht. Es fehlt indessen an einer Rechtsgrundlage für die Weitergabe personenbezogener Informationen an den Stadtrat und für die Weiterübermittlung von Daten durch diesen im Rahmen einer öffentlichen Erörterung.

18.6 Benutzerberechtigung für Rechnungsprüfer

Eine Stadtverwaltung, die ein Bürokommunikationssystem AS 400 nutzt, wollte vom LfD wissen, ob dem Rechnungsprüfungsamt eine inhaltlich und zeitlich unbegrenzte Berechtigung zum lesenden Zugriff erteilt werden könne. Zutreffend wurde schon in der Anfrage darauf hingewiesen, daß die Rechnungsprüfung nach § 14 Abs. 3 BDSG keine Nutzungsänderung darstellt.

Es ist zu berücksichtigen, daß nach § 8 Abs. 1 LDatG den bei der Datenverarbeitung beschäftigten Personen untersagt ist, geschützte personenbezogene Daten unbefugt zu einem anderen als den zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekanntzugeben, zugänglich zu machen oder sonst zu nutzen. Handelte es sich bei der Rechnungsprüfung um einen „anderen als den zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck" so wäre nach der Befugnisnorm für die „Zugänglichmachung" zu fragen. Auch ohne ausdrückliche Erwähnung der Rechnungsprüfung im Landesdatenschutzgesetz wird indessen auch jetzt schon von einer Zweckeinheit ausgegangen.

Ein Lösungsansatz ist dem auch ohne spezielle gesetzliche Normierung verfassungsrechtlich gebotenen Verhältnismäßigkeitsgrundsatz zu entnehmen. Für den Geltungsbereich des Bundesdatenschutzgesetzes verweist § 10 auf diesen Grundsatz: Die Einrichtung automatisierter Abrufverfahren ist zulässig, soweit dieses Verfahren ... angemessen ist. Das novellierte Landesdatenschutzgesetz wird eine ähnliche Regelung enthalten.

Die Angemessenheit von On-line-Anschlüssen für Prüfungszwecke wird gegenwärtig im Zusammenhang mit dem vom Bundesminister der Finanzen vorgelegten Entwurf einer Steuerdaten-Abruf-Verordnung (StDAV) diskutiert. Nach dem gegenwärtigen Diskussionsstand ist nicht beabsichtigt, einen On-line-Anschluß für ständige und unbegrenzte Abrufe einzurichten. Vielmehr soll eine Abrufberechtigung nur für die Dauer und den Umfang eines konkreten Prüfungsauftrags erteilt werden, wenn eine Prüfung durch die Amtsträger der Rechnungsprüfungsbehörden ergibt, daß ein On-line-Zugriff für eine ordnungsgemäße Rechnungsprüfung notwendig ist. Der LfD teilt die in der Diskussion um den o. a. Entwurf deutlich gewordene Auffassung, daß weitergehende On-line-Anschlüsse mit dem Verhältnismäßigkeitsgrundsatz nicht zu vereinbaren wären.

18.7 Auskunftsverpflichtung der datenverarbeitenden Stellen nach § 20 LDatG

§ 20 LDatG begründet für Behörden und sonstige öffentliche Stellen sowie deren Auftragnehmer die Verpflichtung, den LfD und die Beamten seiner Behörde bei der Erfüllung ihrer Aufgaben zu unterstützen. Diese Unterstützungspflicht erstreckt sich nach dem Willen des Gesetzgebers u. a. darauf, Auskünfte auf Fragen zu erteilen, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen.

Die gesetzliche Auskunftspflicht der datenverarbeitenden Stellen bildet eine wichtige Grundlage effektiver Datenschutzkontrolle. Diese wäre mit dem vorhandenen Personal und den zur Verfügung stehenden Sachmitteln nicht zu leisten, wenn die Behörde des LfD zur Bearbeitung von Eingaben in jedem Falle Prüfungen vor Ort durchführen müßte.

Daß die betroffenen Behörden nicht gerade mit Begeisterung ihrer Auskunftspflicht nachkommen, versteht sich von selbst. Bisweilen wird dies aus dem Inhalt von Antwortschreiben, sehr viel häufiger aber aufgrund des Zeitablaufs bis zu deren Eingang erkennbar. Zweite und dritte Erinnerungen an die Beantwortung sind leider keine Seltenheit; gelegentlich werden Anfragen erst nach Einschaltung der Aufsichtsbehörde beantwortet. Das beklagenswerte Antwortverhalten einer obersten Landesbehörde änderte sich rasch und nachhaltig, nachdem der zuständige Ressortchef vom LfD auf die zögerliche Bearbeitung hingewiesen wurde.

Natürlich fehlt es auch nicht an Versuchen, konkrete Fragen ungenau oder ausweichend zu beantworten, der Antwortpflicht also nur zum Schein zu genügen. Eindeutig dieser Strategie zuzuordnen waren drei Antworten eines Oberbürgermeisters auf die konkrete Frage, aus welchen Datenbeständen eine Liste mit Winzeranschriften herrühre, die dem Fremdenverkehrsamt zur Verfügung stand und von diesem ohne Zustimmung der Betroffenen an ein Ratsmitglied weitergegeben worden war. Die Hinweise des Oberbürgermeisters, daß es sich um keine besonders schutzbedürftigen Daten handele, daß solche Daten auch dem Fernsprechbuch entnommen werden könnten, daß die Verwendung der Daten durch das Ratsmitglied einem förderungswürdigen Zweck gedient habe usw. waren allesamt nicht falsch, beantworteten aber nicht die Frage, die vor dem Hintergrund gestellt wurde, daß die Verwendung besonders geschützter Steuerdaten in Betracht zu ziehen war. Selbstverständlich war auch begründet worden, warum es auf die Beantwortung der Frage bei der datenschutzrechtlichen Beurteilung des Vorganges ankam.

Schließlich kam es dann doch zu einer Klärung: Vorschriften zum Schutze des Steuergeheimnisses waren nicht verletzt worden.

Zur Sache selbst ist darauf hinzuweisen, daß kein Hinderungsgrund besteht, im Fremdenverkehrsamt für Werbezwecke entweder einen Datenbestand der Betriebe, die Öffentlichkeitsarbeit und Werbung betreiben wollen, auf der Basis der informierten Einwilligung jedes Betriebes zu erstellen oder aber veröffentlichte Unterlagen zu verwenden, denen zu entnehmen ist, daß die aufgeführten Betriebe mit Werbemaßnahmen einverstanden sind.

18.8 Veröffentlichung von Personenstandsfällen

In Eingaben an die Behörde des LfD wird immer wieder beklagt, daß Standesämter die aus der Streichung des § 104 der Allgemeinen Verwaltungsvorschrift zum Personenstandsgesetz (DA) folgende Rechtslage nicht beachten und Personenstandsfälle ohne Zustimmung der Betroffenen oder ihrer Angehörigen veröffentlichen. Es besteht daher Veranlassung, das Rundschreiben des Ministeriums des Innern und für Sport vom 17. Mai 1985, Az.: 157-09/8, in Erinnerung zu rufen, in dem klargestellt wird, daß die Städte und Gemeinden bei der Veröffentlichung von Standesamtsnachrichten die allgemeinen datenschutzrechtlichen Vorschriften zu beachten haben. Danach ist, so wird in diesem Rundschreiben hervorgehoben, die wirksame Einwilligungserklärung aller von einem Personenstandsfall Betroffenen in jedem Einzelfall erforderlich.

18.9 Erstellung und Weitergabe von Vereinsverzeichnissen

Eine Verbandsgemeinde hatte ein Verzeichnis aller Vereine im Verbandsgemeindegebiet mit den Namen und Anschriften der Vorsitzenden erstellt. Dieses Verzeichnis sollte nur internen Zwecken dienen, fand aber, nachdem seine Existenz bekannt wurde, starkes Interesse bei den Vereinen selbst und bei anderen Einrichtungen und Personen, die über das Vereinsleben berichten oder für die Teilnahme am Vereinsleben werben wollten. Der LfD wurde um Stellungnahme gebeten, ob die Weitergabe des Vereinsverzeichnisses zulässig ist.

Eine nähere Prüfung des Vereinsverzeichnisses ergab, daß Organisationen unterschiedlichster Rechtsform zusammengefaßt waren. Es enthielt die Anschriften von Vorsitzenden eingetragener Vereine und der Organe von Körperschaften des öffentlichen Rechts, aber auch die Anschriften von Repräsentanten kirchlicher Einrichtungen und auch nichteingetragener Vereine.

Nach der Rechtsform der jeweiligen Organisation richtet sich die datenschutzrechtliche Beurteilung der mit der Weitergabe des Verzeichnisses verbundenen Datenübermittlung. Die Anschriften der Vorsitzenden eingetragener Vereine unterliegen keinerlei Übermittlungsrestriktionen, denn diese Daten sind nach den Bestimmungen des BGB (§ 79) öffentlich. Im Rahmen der Offenbarung aller anderen Anschriften – ausgenommen die von Körperschaften des öffentlichen Rechts – könnten schutzwürdige Belange der Betroffenen beeinträchtigt werden. Dies ist eindeutig nur dann nicht der Fall, wenn die Daten zum Zwecke der Aufnahme in ein Register, dessen Inhalt zur Übermittlung bestimmt ist, erhoben wurden und die Betroffenen in Kenntnis der Datenerhebung und der möglichen Übermittlung entweder zugestimmt oder nicht widersprochen haben. Sofern diese Voraussetzungen nicht vorliegen, ist die Übermittlung zwar nicht in jedem Falle ausgeschlossen, es bedarf aber eingehender Prüfungen, welche Datenschutzvorschriften unter Berücksichtigung der Rechtsform der Organisation anzuwenden sind.

Der LfD empfahl, alle möglichen Bedenken dadurch auszuräumen, daß die Betroffenen über die Aufnahme in die Liste und deren Zweckbestimmung, insbesondere die Übermittlung an Interessenten, informiert und entweder um Zustimmung gebeten werden oder eine Widerspruchsfrist eröffnet wird.

18.10 Aufstellung der Schöffenvorschlagsliste nach den Vorschriften des Gerichtsverfassungsgesetzes (GVG)

Mehrere Eingaben an den LfD betrafen Grundsatzfragen der Gesetzesanwendung im Zusammenhang mit der Aufstellung von Schöffenvorschlagslisten. In einer größeren Stadt wurde die Vorgehensweise bei der Aufstellung überprüft. Das Verfahren war in einer unter Datenschutzgesichtspunkten befriedigenden Weise wie folgt organisiert:

Nach Bestimmung der Schöffenzahl durch den Präsidenten des Landgerichts werden die im Stadtrat vertretenen Fraktionen aufgefordert, Vorschläge zu unterbreiten. Zugleich erstellt das Einwohnermeldeamt nach dem Zufallsverfahren aus dem Melderegister eine Liste von Personen, die für das Schöffenamt wählbar sind. Das Einwohnermeldeamt geht dabei so vor, daß es zunächst die Gesamtzahl der in Betracht kommenden Personen unter Berücksichtigung der Altersbegrenzungen, der in § 32 GVG genannten Ausschließungsgründe und eventuell ins Melderegister eingetragener Sperrvermerke ermittelt. Die so gewonnene Zahl wird durch die Anzahl der für die Vorschlagsliste benötigten Adressen geteilt. Der Teiler wird für die Auswahl in der Weise genutzt, daß die Liste der in Betracht kommenden Einwohner im maschinellen Verfahren durchgezählt und jede dem Teiler entsprechende Adresse in eine Liste aufgenommen wird.

Im Anschluß wird die so gewonnene Liste mit den Fraktionsvorschlägen zusammengefaßt. Die Betroffenen werden angeschrieben und um Mitteilung gebeten, ob sie das Schöffenamt annehmen würden oder welche Ablehungsgründe bestehen. Zugleich werden sie gebeten, im Falle der Annahmebereitschaft den Beruf anzugeben.

Nachfolgend wird die Liste mit den Anschriften der Personen, die zur Annahme bereit sind, entsprechend den gesetzlichen Vorschriften, ausgelegt. Die ausgelegte Vorschlagsliste weist folgende Datenarten aus: laufende Nummer, Familien- und Vorname, Geburtsname, Beruf, Geburtstag, Geburtsort, Wohnanschrift.

Nach Ablauf der Auslegungsfrist wird die Liste dem Stadtrat vorgelegt, der hierüber beschließt. Den Stadtratsmitgliedern wird die Liste vollständig mit der Einladung übermittelt.

Nach der Beschlußfassung durch den Stadtrat wird die Schöffenvorschlagsliste dem Gericht übersandt.

Der Stadtrat wählt ferner die Vertrauenspersonen zum Schöffenwahlausschuß.

Verwaltungsinterne Erkenntnismöglichkeiten außerhalb des Melderegisters werden nicht genutzt.

Dieses Verfahren war nach Auffassung des LfD nur insoweit verbesserungsbedürftig, als in dem Anschreiben an die Betroffenen auf die Hinderungsgründe für die Ausübung des Schöffenamtes nach § 32 GVG hingewiesen werden sollte.

Die von einer Stadtverwaltung vorgetragenen Anregungen, auf eine Änderung der Verwaltungsvorschrift über Vorbereitung und Durchführung der Schöffenwahl dahin gehend hinzuwirken, daß auf die Bekanntgabe des Berufs der Vorgeschlagenen verzichtet wird, konnte schon deshalb nicht aufgegriffen werden, weil sich die entsprechende Bestimmung wortgleich auch im Gerichtsverfassungsgesetz findet. Eine Initiative müßte also auf die Änderung dieses Bundesgesetzes gerichtet sein.

Nach dem oben geschilderten Verfahren werden in die auszulegende Schöffenliste auch nur solche Personen aufgenommen, die zuvor erklärt haben, daß sie das Schöffenamt im Falle der Wahl annehmen würden, und in diesem Zusammenhang ihren Beruf mitgeteilt haben. Da jeglicher Einwand von Betroffenen gegen das Verfahren, also auch gegen die öffentliche Auslegung der Schöffenliste, als Grund für die Nichtberufung akzeptiert wird, läßt diese „Widerspruchslösung" aber auch mögliche Bedenken bezüglich der Beeinträchtigung von Persönlichkeitsrechten durch die Auslegung zur Einsichtnahme zurücktreten.

Im übrigen ist zu berücksichtigen, daß der Beruf wohl unverzichtbar ist, denn die Vorschlagsliste soll alle Gruppen der Bevölkerung angemessen berücksichtigen. Durch die öffentliche Auslegung unter Angabe dieses Merkmals soll erreicht werden, daß dies überprüft werden kann.

18.11 Ergebnisse örtlicher Feststellungen in Verbandsgemeindeverwaltungen

Im Berichtszeitraum wurden mehrere Verbandsgemeindeverwaltungen auf die Einhaltung datenschutzrechtlicher Vorschriften überprüft. Insgesamt stellte sich die Situation positiv dar. Ersichtlich war jedoch auch, daß derzeit ein Wandel in der Technik vonstatten geht. Einzelplatzsysteme werden zunehmend durch vernetzte Personalcomputer ersetzt. Im wesentlichen führten die örtlichen Feststellungen zu folgenden Ergebnissen:

- Die geprüften Verbandsgemeindeverwaltungen waren ihrer Verpflichtung, automatisierte Verfahren zum Datenschutzregister anzumelden (§ 10 LDatG) nicht vollständig nachgekommen.

- Im Sozialleistungsbereich ist nach § 79 Abs. 1 SGB X i. V. m. § 36 BDSG ein Beauftragter für den Datenschutz zu bestellen, wenn mehr als fünf Bedienstete in der automatisierten Datenverarbeitung tätig sind. Bei mehreren Verbandsgemeindeverwaltungen ist eine derartige Bestellung unterblieben.

- Eine Verbandsgemeindeverwaltung hatte dem Internationalen Suchdienst Arolsen die Durchsicht archivierter Melderegisterkarteikarten gestattet. Dies war nach den gesetzlichen Bestimmungen nicht zulässig (vgl. Tz. 4.5).

- Mehrere Verbandsgemeindeverwaltungen waren ihrer Pflicht, eine Dienstanweisung über den technischen und orgnisatorischen Datenschutz zu erlassen (§ 9 Abs. 2 LDatG), nicht nachgekommen oder hatten eine vorhandene Dienstanweisung nicht dem veränderten Stand der Automationstechnik angepaßt.

- Bei zwei Verbandsgemeindeverwaltungen befanden sich Unterlagen über die Beihilfegewährung bei den Personalakten der beihilfeberechtigten Bediensteten. Der LfD wies in seinen Prüfungsmitteilungen darauf hin, daß nach § 56 a Beamtenrechtsrahmengesetz die Beihilfeunterlagen stets getrennt von den übrigen Personalakten aufzubewahren sind. Weiterhin war anzumerken, daß Beihilfeangelegenheiten nach den genannten Vorschriften in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden sollen.

- In einer Verbandsgemeindeverwaltung werden in einem Großraumbüro des Meldeamtes bis zu drei Meldevorgänge in Anwesenheit von Antragstellern usw. gleichzeitig bearbeitet. Da eine kurzfristige Veränderung der räumlichen Situation in absehbarer Zeit nicht möglich war, hat der LfD die Aufstellung von Sicht- und Schallschluckwänden empfohlen. Langfristig wird die Bearbeitung von Meldevorgängen in Einzelbüros angestrebt.

- In einer Verbandsgemeindeverwaltung wird auf freiwilliger Grundlage an Bedürftige eine Weihnachtszuwendung gewährt. Der Gemeinderat hat sich jedoch vorbehalten, die Zuwendung aufgrund einer ihm vorzulegenden Liste der Sozialhilfeempfänger zu überprüfen. Diese Verfahrensweise ist mit den gesetzlichen Bestimmungen zum Schutze von Sozialdaten (insbesondere § 35 SGB I) nicht vereinbar. Angesichts der bisherigen Praxis ist die Gewährung derartiger Zuwendungen eine Aufgabe der laufenden Verwaltungsgeschäfte; für die Datenübermittlung an den Gemeinderat besteht insoweit keine Rechtsgrundlage.

Die Verbandsgemeindeverwaltungen sind den Empfehlungen des LfD im wesentlichen nachgekommen.

19 Medien

19.1 Novellierung des Landesrundfunkgesetzes

Der LfD wurde frühzeitig in die Beratungen zum Gesetzentwurf der Landesregierung eingebunden. Er hat eine schriftliche Stellungnahme abgegeben und an der Anhörung durch den Medienpolitischen Ausschuß teilgenommen.

Zu begrüßen ist ausdrücklich, daß dem LfD gemäß § 35 Landesrundfunkgesetz (LRG) die Überwachung der Einhaltung der Datenschutzbestimmungen bei der Landeszentrale für private Rundfunkveranstalter (LPR) und den Veranstaltern obliegt.

Außerdem sind zusätzliche Verfahrensregelungen eingeflossen, die dem Schutz der Betroffenen dienen. Wenn diese beispielsweise gegenüber dem Fernsehveranstalter eine Gegendarstellung, eine Unterlassung oder einen Widerruf durchsetzen, sind diese Erklärungen nach § 31 Abs. 2 LRG zu den gespeicherten Daten zu nehmen. Sie sind dort für dieselbe Zeitdauer aufzubewahren wie die Daten selbst und bei einer Übermittlung der Daten gemeinsam mit diesen zu übermitteln. Deshalb muß der Fernsehveranstalter bei einem Verkauf der Sendungen diese Erklärungen dem Käufer mitgeben.

Obwohl sie die verfassungsrechtlich garantierte Rundfunkfreiheit nicht tangiert hätten, fanden folgende Vorschläge des LfD keine Berücksichtigung:

Im Rahmen der Beratungen wurde angeregt, in die Beschreibung des Rundfunkbegriffs auch das „Computer-Daten-Fernsehen" (Videodat, Videoprint, Data Broadcasting) aufzunehmen. Es nutzt, ähnlich wie Videotext, die Austastlücke bei Fernsehsendungen zur Übertragung von Informationen. Bereits in Betrieb ist das System „Channel-Videodat" (Veranstalter ist „PRO 7"), das sich als zuschauerorientierter Datenkanal versteht. Der Videodat-Empfang setzt einen Decoder voraus, der die empfangenen Signale in digitale Daten umsetzt und diese an einen angeschlossenen Personalcomputer weiterleitet. Bei den Daten handelt es sich um ablauffähige Computerprogramme und um Textdateien, die auch personenbezogene Daten enthalten können. Durch die per Rundfunk verteilten Decoder-Nummern ist auch nachvollziehbar, welcher Teilnehmer welche Dienste in Anspruch nimmt.

Weiterhin sollte – so der Vorschlag des LfD – ergänzend eine Regelung der Datenverarbeitung für Zwecke der Kommunikations- und Meinungsforschung aufgenommen werden, die sich an § 12 Abs. 2 Btx-Staatsvertrag hätte orientieren können. Mit dieser Regelung würde für die Kommunikationsforschung eine Verwendung der für sie wichtigen Daten mit Einwilligung der Betroffenen ermöglicht.

Im Bereich der Bestimmungen zur Datenverarbeitung für journalistisch-redaktionelle Zwecke (§ 31 LRG) ist nach Auffassung des LfD klärungsbedürftig, ob im Rahmen des datenschutzrechtlichen Medienprivilegs die Voraussetzung „ausschließlich zu eigenen Zwecken" auch vorliegt, wenn eine Übermittlung an andere Unternehmen des Medienbereichs für deren (ausschließlich eigene) journalistisch-redaktionelle Zwecke erfolgt. Es wäre sinnvoll gewesen, hier eine eindeutige Regelung zu schaffen. Ferner ist zu beachten, daß die Verwendung des Begriffspaares „Veranstalter und ihre Hilfsunternehmen" zu Auslegungsschwierigkeiten führen könnte. So ist nicht ersichtlich, ob unter den Begriff „Hilfsunternehmen" die sog. Medienbetriebsgesellschaften fallen. Demzufolge wäre klarzustellen, inwieweit die Medienbetriebsgesellschaften, die als solche wohl nicht in den Regelungsbereich des Rundfunkstaatsvertrages fallen, den Bestimmungen zum Datenschutz unterworfen sind.

Auch ist das Auskunftsrecht wesentlicher Bestandteil des Grundrechts auf informationelle Selbstbestimmung. Ohne die vorhandenen Daten zu kennen, kann kein Betroffener seine weiteren Rechte wie die Berichtigung oder das Hinzufügen einer eigenen Darstellung wahrnehmen. Eine Auskunftsverweigerung stellt stets einen Eingriff dar, der nur im überwiegenden Allgemeininteresse gerechtfertigt sein kann. Wird die Auskunft von einer vorangegangenen Beeinträchtigung des Betroffenen in seinem Persönlichkeitsrecht abhängig gemacht, ist eine nicht hinnehmbare Aushöhlung des Grundrechts die Folge; es wird damit praktisch wirkungslos. Auf die Vorbedingung der bereits erfolgten Beeinträchtigung (§ 31 Absatz 3 LRG) sollte daher verzichtet werden. Die Problematik hat der LfD hinsichtlich des ZDF-Staatsvertrages auch schon im 13. Tb. (Tz. 18.1) angesprochen.

Abschließend sei zu diesem Themenkreis die kritische Einordnung des datenschutzrechtlichen Medienprivilegs durch den damaligen Präsidenten des Bundesverwaltungsgerichts, Prof. Dr. Horst Sendler, wiedergegeben, die er anläßlich seines Vortrages auf dem Deutschen Anwaltstag in München am 4. Mai 1989 vorgenommen hat:

„Schizophrenien ... lassen sich auch sonst gelegentlich feststellen, wo handfeste Interessen auch in Gestalt von heißen Eisen aufeinanderprallen, eines dieser Eisen aber besonders heiß ist. Das ist etwa beim Datenschutz der Fall. Seit Jahren ist man bemüht, das vom Bundesverfassungsgericht kreierte Recht auf informationelle Selbstbestimmung in allen möglichen Bereichen festzuzurren. Nur von dem Medienprivileg, nach dem personenbezogene Daten und damit auch jenes schöne informationelle Selbstbestimmungsrecht im Bereich der Medien nicht geschützt werden, spricht niemand – die Medien aus naheliegenden Gründen nicht, weil sie Privilegien nicht gern opfern; und die anderen schweigen, weil sie sich den Zorn jener, von deren Wohlwollen in der Berichterstattung sie sich abhängig fühlen, natürlich nicht zuziehen wollen, und dies, obwohl so mancher gewiß sehr interessiert daran wäre, mittels eines Auskunftsanspruchs, wie er gegenüber sonstigen – auch privaten – Dateien besteht, zu erfahren, was in so manchen Pressearchiven an Information über ihn versteckt ist, um dann im günstigen Moment als Bombe in die Öffentlichkeit zu gelangen. Man wundert sich auch deswegen, weil man doch spätestens seit Oscar Wilde weiß, daß die moderne Presse die unmittelbare Fortsetzung der mittelalterlichen Folter ist, und man erst kürzlich wieder lesen konnte, daß es Nachrichten gibt, die töten (und dies wollen), während sie zu informieren vorgeben – auch dies dürfte ein Problem des Rechtsstaats sein."

19.2 Reality-TV und Datenschutz im Fernsehen

Die neue Sendeform des Reality-TV wirft eine Fülle von Fragen im Bereich des Medienrechts und des Datenschutzes auf (vgl. dazu auch Tz. 5.23).

Es werden zunehmend Versuche von (privaten) Fernsehsendern registriert, Mitarbeiter von Feuerwehren, Hilfs- und Rettungsdiensten zur Mitwirkung an derartigen Sendungen zu gewinnen, indem man beispielsweise komplette Videoausrüstungen zur Verfügung stellt, um authentisches Bildmaterial zu erhalten. Zur Befriedigung reiner Unterhaltungsinteressen sollen das Leid und die Not Betroffener ohne Rücksicht auf deren Intimsphäre hautnah – womöglich in Zeitlupe und Großaufnahme – auf Film gebannt werden.

Das Zurschaustellen menschlicher Notlagen sollte nicht nur als ein Schandfleck für die allgemeine Programmkultur gebrandmarkt werden, sondern für die Aufsichts- und Kontrollbehörden auch Anlaß sein, gemeinsam aktiv zu werden, um dieser Fehlentwicklung im Interesse unserer Verfassungsordnung mit allen rechtsstaatlichen Mitteln Einhalt zu gebieten.

Der rechtliche Hintergrund stellt sich, bezogen auf das oben beschriebene Szenario, wie folgt dar:

Unabhängig von Kontrollzuständigkeiten sind Filmaufnahmen, die anläßlich solcher Einsätze angefertigt werden, Datenerhebungen. Gem. § 28 Abs. 1 Rundfunkstaatsvertrag (RundfunkStV) i. V. m. § 3 Abs. 3 Bundesdatenschutzgesetz (BDSG) gilt das Datenschutzrecht gegenüber Rundfunkveranstaltern auch für Bild- und Tonträger, die wie Akten behandelt werden. Derartige Datenerhebungen sind allenfalls mit schriftlicher Einwilligung der Betroffenen zulässig. In diesem Zusammenhang ist zu beachten, daß nach allgemeinen Grundsätzen eine Einwilligung, die in einer konkreten Notsituation abgegeben wird, regelmäßig bereits wegen der Art und Weise ihres Zustandekommens treuwidrig und das Berufen auf die Einwilligung sittenwidrig ist. Grundsätzlich sind Ausnahmen nur dann denkbar, wenn das öffentliche Interesse eine Dokumentation erforderlich machen würde. Selbst wenn der Notfall auf der Straße nicht zu der durch Gesetz geschützten Intimsphäre eines Patienten gehören würde, so ist doch davon auszugehen, daß die Ausstrahlung von Reality-TV-Sendungen in der Regel das informationelle Selbstbestimmungsrecht der Betroffenen verletzt. Dieses Recht wird nach höchstrichterlicher Rechtsprechung als Ausprägung des allgemeinen Persönlichkeitsrechts und der Menschenwürde verstanden.

Gleichzeitig liegt auch ein Verstoß gegen § 14 Landesrundfunkgesetz (LRG) vor, wonach zu den allgemeinen Programmgrundsätzen sowohl die Achtung der Menschenwürde als auch die verfassungsmäßige Ordnung gehören. Also ist auch hier das als Grundrecht anerkannte Recht auf informationelle Selbstbestimmung zu beachten. Fernerhin sind in § 23 Abs. 1 RundfunkStV und in Artikel 7 des Europäischen Übereinkommens zum grenzüberschreitenden Fernsehen entsprechende Grundsätze verankert.

Es erscheint ratsam, die Zuständigkeiten der Landeszentrale für private Rundfunkveranstalter (LPR) nach § 10 LRG und des LfD gem. § 35 LRG auszuschöpfen. Dabei sollte die aufsichtliche Verantwortung der LPR mit dem Überwachungsauftrag des LfD sinnvoll gekoppelt werden, um den effektiven Schutz des Grundrechts auf informationelle Selbstbestimmung zu gewährleisten.

Hierbei wird nicht verkannt, daß das Grundgesetz die Rundfunkfreiheit als eigenständiges kommunikatives Grundrecht anerkennt. So ist auch das datenschutzrechtliche Medienprivileg in § 31 Abs. 1 LRG normiert. Dem Medienprivileg unterfallen solche personenbezogenen Daten, die ausschließlich zu eigenen journalistisch-redaktionellen Zwecken verarbeitet werden. Derartige Daten sind weitgehend von dem Geltungsbereich der Datenschutzgesetze ausgenommen, denn es sind lediglich die Vorschriften im Hinblick auf die technischen und organisatorischen Maßnahmen nach § 9 BDSG anzuwenden. Dennoch darf das Medienprivileg nicht dazu führen, daß die Fernsehveranstalter von der Achtung der Menschenwürde und des Persönlichkeitsrechts faktisch befreit sind.

Das aufgezeigte Problem ist also im Spannungsfeld zwischen Informationsauftrag und Persönlichkeitsschutz angesiedelt. Was die datenschutzrechtliche Beherrschbarkeit anbelangt, wird darauf zu achten sein, daß sowohl die Rundfunkfreiheit als auch das Persönlichkeitsrecht Grundrechte sind, die im Falle des Konflikts einem Ausgleich zugeführt werden müssen. Der LfD ist bemüht, in diesem sensiblen Bereich Einvernehmen mit der LPR herzustellen.

20 Telekommunikation

20.1 Fernmeldewesen

20.1.1 Die Entwicklung der Vermittlungstechnik im Fernmeldewesen

Als das Telefon gegen Ende des vorigen Jahrhunderts eingeführt wurde, mußte der Anrufer die Vermittlungszentrale anwählen und dem „Fräulein vom Amt" mitteilen, mit welchem Anschluß er verbunden werden wollte. In der Regel notierte das „Fräulein vom Amt" die gewünschte Verbindung. Sie konnte auch in die Verbindung hineinhören, sich melden und mitreden. Sie erstellte auch einen Gesprächszettel, der nach heutigem Sprachgebrauch wohl dem Einzelentgeltnachweis entspricht.

Bei der elektromechanischen Vermittlung im analogen Fernmeldenetz ist grundsätzlich keine Erzeugung, Speicherung und Verarbeitung von Kommunikationsdatensätzen möglich. Bei dieser Vermittlungstechnik werden die gewählten Ziffern der Zielnummer dazu genutzt, die Wähler einzustellen und den entsprechenden Gebührentakt auszuwählen. Hierbei wird die gesamte Wählinformation zunächst in ein Register aufgenommen. Mit den letzten beiden Ziffern wird die Verbindung zum Angerufenen hergestellt. Danach wird das Register geleert und kann für weitere Verbindungswünsche genutzt werden. Nach Herstellen der Verbindung im herkömmlichen Fernsprechnetz der Telekom sind daher im Regelfall keine Datenspuren der Kommunikation mehr vorhanden. Das analoge System ist also vom Prinzip der Anonymität geprägt.

Der gegenwärtig sich vollziehende Systemwechsel ist mit der Digitalisierung der Vermittlungseinrichtungen verknüpft. Die Digitalisierung ist die zentrale technische Veränderung. Die Aufgabe der Drehwähler im elektromechanischen System übernehmen jetzt Rechner; sie stellen die Verbindung zwischen Anrufer und Angerufenem her. Dafür benötigen die Vermittlungsrechner deren Daten sowie die der beteiligten Endgeräte, um den Nachrichteninhalt korrekt weitervermitteln zu können. Verbindungsinformationen und Nachrichteninhalt werden in digitalisierter Form durch das Fernmeldenetz geschickt. Dabei können als Übertragungswege (von Vermittlungsstelle zu Vermittlungsstelle) herkömmliche Kabel, Glasfaserkabel, Richtfunkverbindungen oder Satellitenverbindungen eingesetzt werden.

Sowohl im Handvermittlungssystem als auch im digitalisierten System sind die Kommunikationsdaten über das Verbindungsende hinaus vorhanden, so daß sowohl das handvermittelte als auch das digitalisierte System unter Gesichtspunkten des Datenschutzes anders zu bewerten sind als das elektromechanische System.

Heute sind Telekommunikationsnetze zu einer Art elektronischer Autobahn geworden, die den Transport und die Verarbeitung von Informationen übernehmen. Im Laufe der letzten Jahre ist ISDN (Intergrated Services Digital Network = Dienstesintegrierendes digitales Fernmeldenetz) als neue Kommunikationstechnik auch in vielen Behörden eingeführt worden. Sehr leistungsstark ist insbesondere die ISDN-Sprachkommunikation. Hier können mehrere Dutzend verschiedene Leistungsmerkmale aktiviert werden; beispielsweise die Anruferidentifikation, der automatische Rückruf und die Anrufumleitung.

20.1.2 Funktionsweise von ISDN

Die bis zur ISDN-Einführung in den Kommunikationsnetzen angebotenen Dienstleistungen erfordern jeweils eine eigene technische Lösung. Bezogen auf das zur Selbstverständlichkeit gewordene Stromnetz (220 Volt) könnte man zur Verdeutlichung der bislang in den Kommunikationsnetzen vorhandenen Situation den folgenden Vergleich anführen: Man stelle sich vor, es müßte im häuslichen Alltag der Toaster an eine eigens dafür entworfene Toaster-Steckdose, der Mixer an eine spezielle Mixer-Steckdose, die Kaffeemaschine an eine Kaffeemaschinen-Steckdose etc. angeschlossen werden. Hinzu käme als Voraussetzung für den Betrieb, daß jede Steckdose mit eigener Leitung an das nächstgelegene Stromumspannhäuschen des Energieversorgungsunternehmens anzuschließen wäre und eine Einrichtung vorhanden wäre, die es erlaubt, die Stromkosten für jedes Gerät getrennt zu ermitteln. Glücklicherweise ist dies beim Stromnetz nicht notwendig.

Im Fernmeldenetz wird man nun dank ISDN denselben Komfort wie im Stromnetz haben. So sind über eine Anschlußleitung und eine einheitliche Kommunikationssteckdose alle Dienste verfügbar. Es wird also das Telefonieren, das Bildschirmtextbetreiben, das Bildschirmtelefonieren, das Datenübertragen, das Telefaxen und das Teletexen im ISDN genauso problemlos zu betreiben sein wie das Toasten, Mixen und Kaffeekochen im Stromnetz.

20.1.3 Zur Lage in Rheinland-Pfalz

Die Digitalisierung der Übertragungstechnik in Rheinland-Pfalz soll zeitgleich mit der flächendeckenden Inbetriebnahme der digitalen ISDN-fähigen Knotenvermittlungsstellen erfolgen. Zunächst ist das ISDN in den Verdichtungsräumen ausgebaut worden. So ist das ISDN in Koblenz, Bad Kreuznach, Mainz, Trier und Kaiserslautern bereits seit Ende 1990 verfügbar. Der vollständige Ausbau des ISDN in der Fläche soll bis Ende dieses Jahres abgeschlossen werden. Die Landesregierung hat zur Vorbereitung staatlicher Dienststellen auf die neue Kommunikationstechnik das Modellprojekt „Ressortübergreifende Kommunikation (RÜK)" entwickelt, das den Informationsaustausch zwischen der Staatskanzlei, dem Ministerium des Innern und für Sport und dem Ministerium für Wirtschaft und Verkehr verbessern soll. Eine der Projektstufen beinhaltet die Nutzung des ISDN für die Kommunikation zwischen Ressorts. Das Modell soll anschließend auf alle Ministerien übertragen werden.

20.1.4 Zur Lage in Europa

Ab Anfang 1994 soll mit dem Fleckenteppich der nationalen ISDN-Netze in Europa Schluß sein. Das Schlagwort heißt Euro-ISDN, mit dem eine europaweit befahrbare „Kommunikationsautobahn" für Sprache, Daten, Text und Bilder entsteht. Das Mindestangebot umfaßt u. a. die Dienstmerkmale Durchwahl zur Endstelle, Übermittlung der Rufnummer des A-Teilnehmers zum B-Teilnehmer und die Unterdrückung der Übermittlung der Rufnummer des A-Teilnehmers zum B-Teilnehmer. Die Telekom geht in ihren Planungen davon aus, daß im Laufe des Jahres 1994 jeder Kunde einen Euro-ISDN-Anschluß erhalten

kann. Parallel dazu bietet die Telekom in den nächsten Jahren weiterhin den nationalen ISDN-Anschluß an, so daß die Kunden zwischen beiden Anschlußvarianten wählen können. Eine Neuerung gibt es im Euro-ISDN bei der Zuordnung der Dienstmerkmale. Heute sind sie noch anschlußbezogen; d. h., bei der Anrufweiterschaltung wird der gesamte Anschluß mit allen daran befindlichen Endgeräten umgeleitet. Im Euro-ISDN sind die Dienstmerkmale gerätebezogen und damit für jede Rufnummer separat und individuell konfigurierbar. So kann am gleichen Anschluß der PC in den frühen Abendstunden zum günstigen Tarif Daten austauschen, während die Telefonanrufe nach Hause umgeleitet werden.

Im Zusammenhang mit Euro-ISDN ist auch der Vorschlag der EG-Kommission für eine Datenschutzrichtlinie in digitalen Telekommunikationsnetzen vom 18. Juli 1990 einzuordnen. In seiner Urfassung sah der Vorschlag – entsprechend den Forderungen der Datenschutzbeauftragten – z. B. eine generelle Verkürzung der Zielnummer im Einzelverbindungsnachweis des Anrufers um die letzten vier Ziffern vor. Kritisch anzumerken ist, daß diese datenschutzfreundliche Regelung in der aktuellen Fassung nicht mehr vorkommt, wohl als Reaktion auf die Kritik der nationalen Telekommunikationsorganisationen. Begrüßenswert ist indes der Vorschlag der Kommission, daß den Anrufer ein Signal erreichen soll, wenn die Möglichkeit besteht, daß seine Rufnummer beim Angerufenen angezeigt wird. Weiterhin sieht eine – aus der Sicht des Datenschutzes begrüßenswerte – Regelung vor, daß für den Anrufer grundsätzlich die Möglichkeit bestehen soll, seine Rufnummer im Einzelfall auf Knopfdruck zu unterdrücken.

20.1.5 Digitale Nebenstellenanlagen

ISDN-Nebenstellenanlagen verarbeiten personenbezogene Daten in automatisierter Form. Mit einer solchen Anlage werden Anschlußdaten (z. B. Name des Anschlußinhabers, Art der Berechtigung, zuletzt gewählte Verbindung) und Verbindungsdaten (z. B. Rufnummer des Anrufers und des Angerufenen, Zeitpunkt und Dauer des Gesprächs, Art der Verbindung) für jede abgehende Verbindung gespeichert. Es können auch ankommende Gespräche registriert werden. Universelle Auswertungen der Verbindungsdaten sind durch Standard-Software der meisten ISDN-Anlagen technisch möglich (z. B. Listen zur Abrechnung der Privatgespräche, „Hit-Listen" der längsten, teuersten und häufigsten Gespräche oder Listen der häufigsten Verbindungen). Es ist sicherzustellen, daß in ISDN-Anlagen gespeicherte Daten nur im Rahmen ihrer Zweckbestimmung verwendet werden.

Bei dienstlichen Verbindungen ist eine Vollspeicherung, d. h. eine Speicherung aller Verbindungsdaten einschließlich der vollständigen Rufnummer des Angerufenen, aus der Sicht des LfD zulässig, wenn diese Daten für Kontrollen der durchgeführten Verbindungen im Rahmen einer Fach- oder Dienstaufsicht oder für eine Datenschutzkontrolle benötigt werden. Die Daten dürfen nur für diese Zwecke verwendet und nicht mit anderen automatisierten Dateien (z. B. Personaldateien) verknüpft werden. Sie dürfen nur den mit der Kontrolle beauftragten Person zugänglich gemacht werden und sind nach Abschluß der Kontrolle – spätestens nach einer festzulegenden Frist – zu löschen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Entschließung vom 1./2. Oktober 1992 (vgl. Anlage 4) darauf hingewiesen, daß der Schutz des Fernmeldegeheimnisses und des nichtöffentlich gesprochenen Wortes beim Einsatz von digitalen Telekommunikationsanlagen auch im Arbeitsverhältnis gewahrt werden muß.

Bei Privatgesprächen sollte die Rufnummer des Angerufenen schon bei der Speicherung soweit verkürzt werden, daß eine Identifizierung des Angerufenen nicht mehr möglich ist. Daten über Privatgespräche dürfen nur zum Nachweis der Gespräche für den Betroffenen sowie zur Abrechnung der Gebühren verwendet werden; sie dürfen nur dem Betroffenen (direkt) zur Verfügung gestellt werden. Sie sind zu löschen, sobald die Gebühren ohne Vorbehalt bezahlt worden sind.

Bei der Auswahl und bei der Anwendung von ISDN-Leistungsmerkmalen sollte

- ein automatischer Rückruf so installiert sein, daß die Initiative, ob die Verbindung zustande kommt, vom Angerufenen ausgehen muß; solange dieser das Gespräch nicht annimmt, darf kein Signal beim Anrufer ertönen; der Rückruf im Freifall sollte auf jeden Fall nur mit Einverständnis des Teilnehmers geschaltet werden;

- bei Anrufumleitung dem Anrufer mitgeteilt werden, daß sein Anruf bei einem anderen Apparat als dem eigentlich angewählten einläuft; er sollte in diesem Fall die Möglichkeit haben, die Verbindung abzubrechen und die Anzeige seiner Rufnummer beim Umleitungsziel zu unterdrücken; die Anrufumleitung sollte weiter so gestaltet werden, daß zwingend der Teilnehmer, zu dem umgeleitet werden soll, die Schaltung bestätigen muß;

- bei der Zulassung der Anrufumleitung darauf geachtet werden, daß auch die Interessen externer Anrufer betroffen sein können; dies ist z. B. bei Anschlüssen von Teilnehmern bzw. Ämtern der Fall, die besonders schutzwürdige Daten (z. B. Sozial- oder Personaldaten) verarbeiten; ein Externer hat keine Möglichkeit, die Anrufumleitung zu erkennen;

- bei der Entscheidung über Anrufumleitungen besondere Amts- und Berufsgeheimnisse beachtet werden;

- für individuelle Kurzwahlregister sichergestellt werden, daß ihr Inhalt nicht über das Betriebsterminal abrufbar ist;

- jede Einrichtung zum Freisprechen oder Lauthören so ausgestattet sein, daß die Gesprächsteilnehmer im Raum bzw. die Telefonteilnehmer deutlich auf die Inbetriebnahme der Funktion durch ein Signal hingewiesen werden; es sollte ausgeschlossen werden, daß eine Freisprecheinrichtung – wegen der Gefahr des Abhörens – durch einen Anrufer aktiviert werden kann.

Zur Wahrung des informationellen Selbstbestimmungsrechts der Kommunizierenden und zur Gewährleistung des Fernmeldegeheimnisses sind technische und organisatorische Maßnahmen (§ 9 LDatG) zu treffen, die mißbräuchliche Nutzungen verhindern. Insbesondere ist der Zugang zu den ISDN-Servern besonders zu sichern. Mißbräuchliche Zugangsversuche sollten aufgezeichnet und nachfolgend aufgeklärt werden.

Zwischen dem Hersteller und dem Betreiber der Anlage sollten die zur Aufgabenerfüllung notwendigen Funktionen klar festgelegt werden, wobei die Funktionsbeschränkungen durch ein differenziertes Zugriffskontrollverfahren zu realisieren sind. Die Berechtigungsprofile und die Paßworte sollten zum Schutz gegen Manipulationsversuche verschlüsselt gespeichert werden. Die Paßwörter sollten vom Benutzer regelmäßig geändert werden, die Änderung in definierten Abständen erzwungen werden können. Die „Super-User-Kennung" sollte möglichst mit zwei Paßwörtern versehen werden, so daß Änderungen nach dem Vier-Augen-Prinzip nur durch zwei Personen gemeinsam erfolgen können.

Von besonderer Bedeutung ist angesichts der Variabilität der ISDN-Anlagen eine nicht manipulierbare Protokollierung des Systemzustandes. Hierzu gehören Aufzeichnungen über die Installation, Aktivierung und Deaktivierung von Leistungsmerkmalen sowie alle sonstigen Aktivitäten des Systembetreuers. Die Anlagen-Dokumentation sollte eine Beschreibung der technischen Realisierung des Protokolls und die Festlegung, wer auf die Protokolldaten zugreifen, sie löschen und auswerten darf, enthalten. Der Umfang der zulässigen Fernwartung und Ferndiagnose ist präzise festzulegen. Hier darf keine Möglichkeit bestehen, personenbezogene Daten der Behörde einzusehen, zu ändern oder zu kopieren. Wartungsmaßnahmen, bei denen der Zugriff auf personenbezogene Daten unerläßlich ist, sollten nur am Betriebsterminal und nur unter Mitwirkung des Systemverwalters vorgenommen werden.

Schließlich sollten die Kommunikationsteilnehmer umfassend und verständlich über die ihnen zur Verfügung gestellten Systemfunktionen und die gespeicherten Daten informiert werden.

Eine Löschung der gespeicherten Telefondaten hat spätestens nach der Klärung der mit der Telefonabrechnung in Verbindung stehenden Fragen zu erfolgen. Bereits mit Erstellung der Ausdrucke könnte auf die automatisierte Speicherung verzichtet werden, zur Sicherheit bei der Klärung von Zweifelsfragen könnte noch eine zusätzliche kurze Frist hinzugenommen werden.

Den LfD erreichten im Berichtszeitraum zunehmend Anfragen hinsichtlich der Gestaltung von Dienstvereinbarungen. Er hat daraufhin den Leitfaden „Hinweise zu ISDN-Nebenstellenanlagen" verfaßt, der als Anlage 10 abgedruckt ist.

Ein weiterer Schwerpunkt waren Anfragen in bezug auf das Sozialgeheimnis.

Normadressaten der Vorschriften zum Schutze des Sozialgeheimnisses (§ 35 SGB I, §§ 67 ff. SGB X) sind die Sozialleistungsträger, genauer die SGB-Stellen und die aufsichts-, rechnungsprüfungs- und weisungsberechtigten Stellen (§ 35 Abs. 1 Satz 4 SGB I). Letztere sind, soweit sie Aufsichts-, Rechnungsprüfungs- oder Weisungsaufgaben wahrnehmen, nicht Dritte, sondern im funktionalen Sinne Teile der SGB-Stelle. Werden Zielnummern von Antragstellern auf Sozialleistungen oder Leistungsempfängern erfaßt und für Kontrollzwecke genutzt, so liegt keine Offenbarung von Sozialdaten vor. Folgt man der Systematik des Bundesdatenschutzgesetzes (§ 14 Abs. 3), so liegt auch keine Zweckänderung vor. Hieraus folgt, daß gegen die Aufzeichnung und Nutzung von Zielnummern für Kontrollzwecke insoweit keine Bedenken zu erheben sind, als diese Daten „nur" durch die allgemeinen Vorschriften über das Sozialgeheimnis geschützt sind.

Im Sozialleistungsbereich kommen freilich auch Bestimmungen zur Anwendung, die nicht die „SGB-Stelle", sondern den einzelnen dort tätigen Mitarbeiter zur Geheimhaltung verpflichten. Dies sind zum einen Angehörige der in § 203 Abs. 1 StGB genannten Berufsgruppen, insbesondere Sozialarbeiter hinsichtlich solcher Geheimnisse, die ihnen in dieser Eigenschaft anvertraut worden sind, zum anderen Mitarbeiter eines Trägers der öffentlichen Jugendhilfe, die nach § 65 SGB VIII (KJHG) einen besonderen Vertrauensschutz in der persönlichen und erzieherischen Hilfe zu beachten haben.

Das Bundesarbeitsgericht hat in seiner Entscheidung vom 13. Januar 1987 (NJW 1987, 1509 ff.) festgestellt, daß der in einer Beratungsstelle für Erwachsene, Kinder und Jugendliche eines Landkreises tätige Psychologe mit staatlich anerkannter wissenschaftlicher Abschlußprüfung dem Landkreis als Arbeitgeber nicht berechtigt und verpflichtet ist, Auskunft darüber zu geben, mit welchen von ihm zu betreuenden Personen er ein Telefongespräch geführt hat. Danach darf sich der Arbeitgeber diese Kenntnis nicht dadurch verschaffen, daß er bei einer automatisierten Erfassung der vom Psychologen geführten dienstlichen Telefongespräche mit zu betreuenden Personen die Zielnummer dieses Telefongesprächs erfaßt. Diese Entscheidung, die anknüpft an die Strafbewehrung der Geheimhaltungsverpflichtung nach § 203 Abs. 1 StGB, ist auf die Angehörigen der anderen in dieser Vorschrift genannten Berufsgruppen, also beispielsweise auch auf Sozialarbeiter, übertragbar, soweit diese berufsspezifische Tätigkeiten ausüben. Hierzu zählen bei Sozialarbeitern insbesondere Beratungstätigkeiten.

§ 65 SGB VIII erstreckt die Schutzwirkung des § 203 StGB auf Daten, die dem Mitarbeiter eines Trägers der öffentlichen Jugendhilfe zum Zwecke persönlicher oder erzieherischer Hilfe – gemeint ist auch hier insbesondere Beratungstätigkeit – anvertraut worden sind. Die in der Vorschrift genannten Personen haben die Verschwiegenheitspflichten auch innerhalb der SGB-Stelle, der sie angehören, zu beachten. Die Offenbarungsbefugnisse sind – mit Ausnahme der Offenbarung an das Vormundschaftsgericht (§ 65 Nr. 2 SGB VIII) – identisch mit den Befugnissen, die den in § 203 StGB genannten Berufsangehörigen eine Offenbarung erlauben.

Zusammenfassend vertritt der LfD die Auffassung, daß die Vorschrift über den Vertrauensschutz in der persönlichen und erzieherischen Hilfe (§ 65 SGB VIII) einer Erfassung der Zielnummer durch den Arbeitgeber ebenfalls entgegensteht.

20.2 Funkverkehr der Polizei; Auswirkungen von EG-Vorschrifen auf die Innere Sicherheit

Zum 30. Juni 1992 wurde in Umsetzung der Richtlinie 92/31/EWG des Rates der Europäischen Gemeinschaften vom 28. April 1992 die Beschränkung der zulässigen Empfangsfrequenzbereiche aufgehoben, so daß es nunmehr zulässig ist, Rundfunkempfänger zu betreiben, die das Abhören des Funkverkehrs ermöglichen. Bis zu diesem Zeitpunkt war sogar der Besitz jener Geräte verboten. Ein Verstoß war mit Strafe und Beschlagnahme bedroht. Durch die Neuregelung ist nun der Besitz und auch der Betrieb von Empfängern erlaubt, mit denen diese Sonderfrequenzen abgehört werden können. Am 20. November 1992 hat die Ständige Konferenz der Innenminister und -senatoren der Länder gefordert, die bislang „geltenden Funkfrequenzbeschränkungen wieder einzurichten und darüber hinaus in das Gesetz über Fernmeldeanlagen (FAG) durchsetzbare Verbote für den Betrieb, Besitz und die Inbetriebnahme von Breitbandempfängern sowie das Abhören von geschützten Frequenzbereichen durch Unberechtigte aufzunehmen". Diese Maßnahme hätte zur Folge, daß wiederum bereits der Besitz von Geräten verboten wäre, mit denen die Sonderfrequenzen abgehört werden können. Diese in Erwägung gezogene Vorgehensweise der Wiedereinführung der früher geltenden Beschränkungen der Empfangsbereiche ist nach EG-Recht unzulässig. Ein Vertragsverletzungsverfahren der EG-Kommission gegen die Bundesrepublik Deutschland vor dem Europäischen Gerichtshof wäre mit großer Wahrscheinlichkeit die Folge.

Der Bundesminister für Post und Telekommunikation geht davon aus, daß der Empfang jener „Aussendungen, die nicht für die Allgemeinheit vorgesehen sind, zum Schutz des Fernmeldegeheimnisses untersagt" bleibt.

Die rechtliche Situation stellt sich wie folgt dar: Gemäß § 11 FAG sind sowohl die Weitergabe des Inhalts an andere als auch die Mitteilung über die Tatsache des Empfangs solcher Sendungen untersagt, da der Polizeifunk öffentlichen Zwecken dient. Verstöße gegen diese Geheimhaltungspflicht werden nach § 18 FAG strafrechtlich geahndet. Ob indes das bloße Mithören nicht für die Allgemeinheit bestimmter Aussendungen danach auch bestraft werden kann, ist umstritten. Gegen eine Strafbarkeit spricht, daß die Strafandrohung nach dem FAG die Verwertung der gewonnenen Erkenntnisse im Auge hat, nicht aber den dafür vorher erforderlichen Vorgang des unbefugten Mithörens.

Gemäß § 9 Abs. 1 Nr. 9 LDatG ist zu gewährleisten, daß bei der Übermittlung personenbezogener Daten diese nicht unbefugt gelesen werden können. Eine teleologische Auslegung der Vorschrift ergibt, daß unter dem Begriff des „Lesens" jede Kenntnisnahme durch Dritte, damit auch bei Verbalkommunikation das unbefugte Mithören zu verstehen ist. Erforderlich sind Maßnahmen, wenn ihr Aufwand unter Berücksichtigung der Art der zu schützenden personenbezogenen Daten und ihrer Verwendung in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die Verschlüsselung von Funkstrecken würde das Abhören unmöglich machen, zumindest ganz erheblich erschweren. Lediglich mit extrem hohem technischem Aufwand und großer krimineller Energie wäre ein Abhören möglich. Der Einsatz sicherer Verschlüsselungsgeräte ist freilich wegen der enormen (Umstellungs-) Kosten aus wirtschaftlichen Gründen gegenwärtig nicht vertretbar. Zudem soll bis zum Jahre 2000 ein europaweites digitales Funknetz der Polizeien aufgebaut werden.

Vor diesem Hintergrund war als Zwischenlösung in Rheinland-Pfalz geplant, die analogen Funkgeräte der Polizei lediglich mit einer „Einfach-Sprachverschleierung" auszustatten. Davon hat man jedoch wiederum Abstand genommen, als bekannt wurde, daß im Fachhandel Rundfunkempfänger mit integriertem Inverter legal erhältlich sind, mit denen das Mithören verschleierter Funkgespräche möglich ist. Hier wird seitens des Benutzers keine technische Manipulation am Gerät durchgeführt, so daß die „Allgemeingenehmigung" zum Betreiben von Rundfunkempfängern weiterhin vorhanden ist.

Nunmehr zeichnet sich eine technische Entwicklung ab, die es ermöglicht, eine größere „Schlüsseltiefe" zu erreichen. Es steht zu hoffen, daß damit die Beeinträchtigung des informationellen Selbstbestimmungsrechts der Betroffenen reduziert wird und die Funktionsfähigkeit des polizeilichen Funkverkehrs – jedenfalls bis Einführung der Digitaltechnik – ausreichend gesichert werden kann.

Schließlich ist darauf hinzuweisen, daß die dargestellte Problematik allgemein den Funkverkehr der Behörden und Organisationen im Sicherheitsbereich (BOS) betrifft, also nicht nur die Polizei, sondern auch Feuerwehr und Rettungsdienste.

20.3 Der Beschluß des Bundesverfassungsgerichts zur Fangschaltung

Mit dem Fangschaltungsbeschluß des Bundesverfassungsgerichts vom 25. März 1992 sieht der LfD seine im 13. Tb. (Tz. 19) zum Ausdruck gebrachte kritische Haltung im Hinblick auf die Regelungen der Verarbeitung von Verbindungsdaten in der Telekom-Datenschutzverordnung (TDSV) und der Teleunternehmen-Datenschutzverordnung (UDSV) bestätigt.

Das Gericht hat festgestellt, daß der TDSV mit § 30 Abs. 2 Postverfassungsgesetz keine ausreichende gesetzliche Ermächtigung zugrunde liegt. So genießen sämtliche der Post zur Beförderung oder Übermittlung anvertrauten Kommunikationsvorgänge und Kommunikationsinhalte den Schutz des Artikels 10 Abs. 1 Grundgesetz (GG). Danach ist die Vertraulichkeit der Kommunikation zu schützen; jede Kenntnisnahme, Aufzeichnung oder Verwertung von kommunikativen Daten durch die Telekom oder andere staatliche Stellen ist danach ein Grundrechtseingriff. In diesem Zusammenhang ist zu fragen, ob nach den Grundsätzen dieses Beschlusses die Erlaubnis zur umfassenden Erhebung und Verarbeitung von Telekommunikationsdaten nach § 5 TDSV aufrechterhalten werden kann.

Seitens des Datenschutzes wurde stets darauf verwiesen, daß es sich bei der Zielnummer um ein personenbezogenes Datum der Angerufenen handele, das nicht ohne deren Wissen und Einwilligung erhoben, gespeichert und übermittelt werden dürfe. Die Postjuristen haben dem stets entgegengehalten, daß das informationelle Selbstbestimmungsrecht der Anrufenden vor dem der Angerufenen Priorität habe, daß man mit der Teilnahme am Fernsprechverkehr in die Datenspeicherung einwillige und daß beim Einzelverbindungsnachweis der Antrag des Anschlußinhabers das Fernmeldegeheimnis auch für alle Angerufenen aufheben würde. Dieser Argumentation ist das Gericht nicht gefolgt. Zwar darf – so wird ausgeführt – „jeder Fernsprechteilnehmer ohne Grundrechtsverstoß Dritte von seinen Telefongesprächen unterrichten. Daraus folgt aber nicht, daß ein Fernsprechteilnehmer mit Wirkung für den anderen auch gegenüber der Telekom auf die Wahrung des Fernmeldegeheimnisses verzichten kann. Wenn der Zweck des Fernmeldegeheimnisses darin liegt, Kommunikationsvorgänge und Kommunikationsinhalte gegen staatliche Zugriffe abzuschirmen, so ist jede staatliche Einschaltung, die nicht im Einverständnis mit beiden Kommunikationspartnern erfolgt, ein Grundrechtseingriff".

Fernerhin ist klärungsbedürftig, wie weit der vom Bundesverfassungsgericht geforderte Gesetzesvorbehalt gehen muß. Wenn jede Registrierung von Fernmeldeverkehr ein Grundrechtseingriff ist und daher vom Gesetzgeber selbst geregelt werden muß, dann gilt dies nicht nur für den Telefondienst und Mobilfunk, sondern auch für Daten- und Textdienste.

Es sollte auch bedacht werden, daß die „Postreform II" weitere Neuregelungen erforderlich machen könnte. Nach einer möglichen Umwandlung in eine Aktiengesellschaft würde die Telekom wohl zum nichtöffentlichen Bereich gehören, so daß dann für die Kontrolle die Aufsichtsbehörden der Bundesländer zuständig wären.

Die im Beschluß des Bundesverfassungsgerichts gewährte Übergangszeit dürfte der laufenden Legislaturperiode (des Bundestages) entsprechen. So bleibt zu hoffen, daß diese Zeit genutzt wird, das leise Verschwinden des Fernmeldegeheimnisses zu stoppen und eine verfassungsgemäße Regelung im Hinblick auf Einzelverbindungsnachweis, Rufnummernanzeige, Anrufumleitung etc. zu finden. An dieser Stelle ist nochmals auf die Ausführungen im 13. Tb. (Tz. 19) hinzuweisen. Die dort beschriebenen Regelungsdefizite sind nach wie vor aktuell. Der LfD wird sich an der Diskussion um die Änderung des Postverfassungsgesetzes weiterhin beteiligen.

20.4 Einsatz von Telefaxgeräten

Faxen ist heute so üblich wie die Briefpost. Bezogen auf die Bundesrepublik, übermitteln die elektronischen Fernkopierer pro Tag rd. 13 Mio. DIN-A4-Seiten Text. Die Informationsübermittlung per Telefax ist schnell, erspart Verwaltungsarbeit und ist in vielen Fällen auch kostengünstiger als eine Briefsendung. Telefax ist aber auch eine recht unsichere Form der Informationsübermittlung, wie jeder weiß, dem schon einmal eine nicht für ihn bestimmte Information zugefaxt wurde. Auch die Dienststelle des LfD war schon wiederholt Empfänger – aber nicht Adressat – von Fernkopien mit recht empfindlichem Inhalt. Die Beachtung der von ihm herausgegebenen Hinweise für das Versenden von Fernkopien (vgl. Anlage 9) kann das Problem mildern, aber nicht grundsätzlich lösen.

Die Zahl der Telefaxgeräte als Mittel der schnellen Bürokommunikation steigt auch in der rheinland-pfälzischen Verwaltung ständig. Soweit es sich um Telekopien mit personenbezogenem Inhalt handelt, muß der gleiche Datenschutzstandard sichergestellt werden wie beim herkömmlichen Postversand, für den die absendende Stelle verantwortlich ist.

Als Gefahr für das informationelle Selbstbestimmungsrecht sind insbesondere das unbefugte Mitlesen, die unbefugte Einsichtnahme und technische Manipulationen zu nennen. Oft benutzen mehrere Verwaltungseinheiten aus Kostengründen ein Gerät gemeinsam, das frei zugänglich aufgestellt ist. Somit kann jeder Mitarbeiter, also auch der unzuständige oder unbefugte Mitarbeiter, die eingehenden Schreiben einsehen. Dies gilt erst recht für Räumlichkeiten mit Publikumsverkehr. Übernimmt die zentrale Poststelle auch die Bedienung des Fernkopierers, darf dies nicht dazu führen, daß aus diesem Grund die bisher geübte

Praxis, bestimmte besonders vertrauliche Schreiben ungeöffnet an die jeweiligen Stellen weiterzuleiten, aufgegeben wird. In diesen Fällen – betroffen sind etwa Schreiben an die Erziehungsberatungsstelle des Jugendamts oder der Schriftverkehr in Beihilfeangelegenheiten sowie alle Personalsachen – ist aus der Sicht des Datenschutzes nach wie vor nur der verschlossene Brief zu akzeptieren. Beim Fernkopieren ist auch die Wahrscheinlichkeit des unbeabsichtigten Verwählens erfahrungsgemäß größer als Fehler in der Briefanschrift. Ein falsch adressiertes Telefax wird vom Empfänger meist auch dann gelesen, wenn der Text nicht für ihn bestimmt ist. Besondere Sicherungsmaßnahmen, die bei der Versendung mit der Briefpost möglich sind, z. B. Einschreiben mit Rückantwortschein, haben beim Fernkopieren noch keinen Einzug gehalten.

Telefax-Geräte ermöglichen grundsätzlich zwei Arten des Fernkopierens: Die direkte Anwahl der Gegenstelle mit anschließendem sofortigem Sendevorgang oder die Eingabe von gewünschter Sendezeit, Sendedatum und Teilnehmernummer. Bei diesem zeitversetzten Senden – es wird häufig in den Nachtstunden zum Einsparen von Verbindungsgebühren eingesetzt – wird das zu kopierende Schriftstück im Sendespeicher des Telefax-Gerätes gespeichert und zum gewünschten Zeitpunkt übermittelt. Hier besteht die Gefahr darin, daß der Sendespeicher jederzeit ausgedruckt bzw. gelöscht werden kann. Die Sicherung von Telefax-Geräten gegen unberechtigten Zugriff auf das Gerät selbst und seiner Datenspeicher kann wesentlich erhöht werden, wenn künftig von Herstellerseite serienmäßig Geräteschlösser vorgesehen und Paßwortverfahren in die Geräte eingebaut werden. So könnte ein Systempaßwort bestimmte Gerätefunktionen schützen.

Manipulationen durch Dritte sind bei Telefax ebenfalls nicht auszuschließen. Dies wird als allgemeines „Netzrisiko" bezeichnet (der Telefaxdienst benutzt das Telefonnetz). Der Empfänger kann die Manipulation nicht ohne weiteres erkennen. Die Möglichkeiten reichen hier vom groben Unfug bis zur gezielten Urkundenfälschung; z. B. Fälschen der Sender-Kennung oder Verstellen der Systemuhr, deren Umstellung bei Faxgeräten kein Problem darstellt; erst recht nicht beim PC mit Faxkarte. Mithin sollte, was Fristsachen anbelangt, der Empfänger das ausgedruckte Protokoll an das Schriftstück heften oder bei Sammelprotokollen ein „Telefax-Eingangsbuch" führen. Dennoch ist in diesem Zusammenhang darauf aufmerksam zu machen, daß es nur einen sicheren Weg gibt, die Echtheit eines Telefax zu überprüfen, nämlich den Rückruf nach Erhalt mit schriftlicher Bestätigung auf dem Briefpostweg. Hier sollte der Grundsatz gelten: Fax allein genügt nicht!

Wenn ärztliche Gutachten per Fax übermittelt werden, ist dies mit dem Schutz des Patientengeheimnisses unvereinbar. Dasselbe gilt für den Bereich des Steuergeheimnisses und des Sozialgeheimnisses (vgl. Tz. 11.2.6). Der LfD vertritt die Auffassung, daß die Übermittlung von Sozialdaten durch Telefax wegen der Übermittlungsrisiken und wegen der Gefährdung des Datenschutzes auf der Empfängerseite gegenwärtig grundsätzlich nicht in Betracht kommen kann. Erst wenn die Entwickler und Hersteller von Telefax-Geräten wirksame Zugriffsschutz-Mechanismen für Sende- und Empfangsspeicher entwickelt haben, könnte die Situation anders beurteilt werden.

Abschließend sei auf einen Fall von Faxspionage, über den auch in der Presse berichtet wurde, hingewiesen. Im „Sicherheitsberater" (Ausgabe 10/93, S. 170) war zu lesen: „Einem Mitarbeiter aus dem Forschungsbereich eines Elektronikunternehmens war es gelungen, höchst sensible Informationen aus einem Faxgerät, das nach dem Thermotransferverfahren arbeitet, zu gewinnen. Die darin eingesetzte Folie ist, ähnlich wie die Matrize bei Druckverfahren oder das Karbonband in Schreibmaschinen, ein dauerhaftes Negativ des jeweiligen Dokuments. Durch Kopieren und Invertieren besitzen die so generierten ‚Originale' eine sehr hohe Qualität." Es sollte daher auf diese Sicherheitslücke bei den Faxgeräten, die nach dem Thermotransferverfahren arbeiten, geachtet und von deren Einsatz in sensiblen Bereichen abgesehen werden.

21 Technischer und organisatorischer Datenschutz

21.1 Einsatz der Informationstechnik (IT)

Die eingesetzten Systeme der Datenverarbeitung in Rheinland-Pfalz sind ausgeprägt heterogen. Neben Großrechner- und Midrangelösungen, insbesondere in den bisherigen Kristallisationspunkten der Datenverarbeitung wie staatliche/Kommunale Rechenzentren und Datenzentralen, sind auf allen Verwaltungsebenen in steigendem Maße Arbeitsplatzrechnerlösungen mit unterschiedlichem Vernetzungsgrad anzutreffen.

Der bereits seit längerem zu beobachtende Umbruch des IT-Einsatzes, bedingt sowohl durch die Entwicklung im Bereich der Hardware, Software und Preise als auch durch steigende Anforderungen an die Effektivität des Verwaltungshandelns, hat sich im Berichtszeitraum unverändert fortgesetzt. Entsprechend der Änderung der verwendeten Terminologie von Datenverarbeitung zu Informationstechnik zeigt sich der Wandel im IT-Einsatz auch in der zunehmenden Integration vorhandener und neugeschaffener IT-Strukturen. Im Gegensatz zur seitherigen Anbindung eines Arbeitsplatzes an Datenverarbeitungssysteme zur Nutzung aufgabenspezifischer Anwendungen lassen sich verstärkt folgende Entwicklungen feststellen:

- die Verwendung am Markt erhältlicher Standardsoftware mit leistungsfähigen Funktionen in den Bereichen Textverarbeitung, Datenbankverwaltung, Tabellenkalkulation und (Büro-)Kommunikation;

- die Abkehr von isoliert eingesetzten Systemen und der Aufbau behördeninterner Netze mit dem Bestreben, alle eingesetzten Systeme (Arbeitsplatzrechner, Anlagen der mittleren Datentechnik, Großrechner) einzubinden und umfangreiche Zugriffsmöglichkeiten zu schaffen;
- der Einsatz digitaler (rechnergestützter) Nebenstellenanlagen;
- die verstärkte beabsichtigte und praktizierte Nutzung öffentlicher Kommunikationsdienste;
- der Einsatz mobiler (tragbarer) Systeme in verschiedenen Bereichen der Verwaltung.

Die Entwicklung ist nicht auf bestimmte Bereiche der öffentlichen Verwaltung beschränkt, sondern betrifft Ministerien, Kreis- und Kommunalverwaltungen, Schulen, Gesundheitsämter, Krankenhäuser, Finanzämter, Gerichtsvollzieher, Schornsteinfeger und andere.

Die Veränderungen sind, selbst bei öffentlichen Stellen der gleichen Verwaltungsebene, durchaus unterschiedlich. Insbesondere im kommunalen Bereich sind zum Teil gravierende Unterschiede hinsichtlich der IT-Ausstattung feststellbar. Allgemein ist die naheliegende Tendenz zu beobachten, bei Erst- bzw. Ersatzbeschaffungen den akuellen Stand der Technik einzusetzen. In einer Untersuchung der staatlichen Datenverarbeitung in Rheinland-Pfalz wurde den geplanten IT-Ausgaben eine strategische Größenordnung zuerkannt. Insbesondere im Rahmen der Ablösung vorhandener Systeme nach einer Nutzungsdauer von fünf bis acht Jahren ist auch künftig mit bedeutsamen Investitionen in die IT-Infrastruktur zu rechnen.

Die Kenntnis der aktuellen Situation der Informationsverarbeitung ist für die Wahrnehmung der Aufgaben des Datenschutzes, insbesondere auch nach § 1 Abs. 2 LDatG, von zentraler Bedeutung. Erkenntnisse werden gewonnen bei örtlichen Feststellungen, bei Ausübung der Beratungstätigkeit und bei der Auswertung von Anmeldungen zum Datenschutzregister gemäß § 10 LDatG. Erfreulich ist in diesem Zusammenhang, daß die öffentlichen Stellen im Rahmen der Novellierung des Landesdatenschutzgesetzes verpflichtet werden sollen, ein Datei- und Geräteverzeichnis zu führen. Neben der Unterstützung der Verwaltung bei der Umsetzung datenschutzrechtlicher Anforderungen hinsichtlich der Koordination des IT-Einsatzes dient es der Bereitstellung aktueller Informationen zur behördlichen IT-Struktur.

21.2 Neuorganisation der Informationstechnik

Auf der Grundlage der von einem Wirtschaftsberatungsunternehmen durchgeführten Untersuchungen zur Situation der staatlichen und kommunalen Datenverarbeitung in Rheinland-Pfalz ist die Neuorganisation der Informationstechnik auf der Basis eines „IT-Organisationsgesetzes" vorgesehen. Wesentliche Ziele sind eine Steigerung der Effektivität, Kostenreduzierungen sowie eine verbesserte Koordinierung des IT-Einsatzes.

Erreicht werden soll dies u. a. durch die technische und organisatorische Zusammenfassung der derzeit bestehenden Rechenzentren der Finanzverwaltung und des Statistischen Landesamtes Bad Ems (RZ/Bad Ems und LRZ) in einem ausschließlich auf IT-Aufgaben ausgerichteten „Dateninformationszentrums (DIZ)" in der Form einer öffentlichen Anstalt, durch den Abbau redundanter Kommunikationsverbindungen und Nutzung eines gemeinsamen Kommunikationsnetzes (Landesdatennetz) sowie die Einrichtung einer IT-Führungsoganisation mit entsprechenden Kompetenzen. Kommunale Interessen sollen durch die Schaffung einer kommunalen Organisationseinheit innerhalb des DIZ und Vertretung der Kommunen in den Entscheidungsgremien berücksichtigt werden.

Der LfD wurde um Stellungnahme zum Entwurf einer Ministerratsvorlage gebeten.

Er begrüßte die beabsichtigte Schaffung einer allgemeinen gesetzlichen Grundlage für die Organisation der Informationstechnik in Rheinland-Pfalz. Neben gesetzlichen Aufgabenzuweisungen für das geplante DIZ sollte das Gesetz bislang fehlende, über § 9 LDatG hinausgehende verfahrensrechtliche Regelungen zum IT-Einsatz enthalten.

Durch die Festschreibung beispielsweise einer Pflicht zur Erstellung von Sicherheitskonzepten beim Einsatz der Informationstechnik oder von Rahmenbedingungen für die Nutzung gemeinsamer Kommunikationsnetze kann der vom Bundesverfassungsgericht erhobenen Forderung an den Gesetzgeber „mehr als früher auch organisatorische und verfahrensrechtliche Regelungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken" Rechnung getragen werden (BVerfGE 65, 1 [14]).

Neben den Vorteilen einer verbesserten Koordinierung, insbesondere hinsichtlich der Einheitlichkeit von Datenschutzmaßnahmen bzw. erweiterter Möglichkeiten der Umsetzung, birgt die beabsichtigte technisch-organisatorische Integration der bestehenden Rechenzentren aus der Sicht des Datenschutzes jedoch auch besondere Risiken.

Die durch die derzeitige räumliche und organisatorische Trennung der Rechenzentren bedingte faktische Trennung der Verantwortung und Zuständigkeiten, unterstützt durch die Zugehörigkeit zu verschiedenen Verwaltungseinheiten, wird aufgehoben oder aber in wesentlichen Teilen eingeschränkt. Unbefugte oder unzulässige Zugriffe werden dadurch erleichtert.

Der LfD sieht die effektive Abschottung der jeweiligen Datenbestände (Statistik-, Steuer-, Polizei-, Meldedaten etc.) durch technische, organisatorische und personelle Maßnahmen als Voraussetzung einer Zusammenführung an. Er wird die Umsetzung seiner Empfehlungen sowie die datenschutzgerechte Ausgestaltung der Neuorganisation mit kritischem Interesse weiter verfolgen. Die Beachtung des Grundsatzes der Trennung von Verwaltung und Statistik wie gleichermaßen die Wahrung des Statistik- und Steuergeheimnisses müssen in entsprechenden Maßnahmen, insbesondere der Zugangs-, Zugriffs-, Speicher- und Übermittlungskontrolle gemäß § 9 LDatG, zum Ausdruck kommen.

Gleiches gilt für die geplante Zusammenführung der Kommunikationsverbindungen und den Abbau redundanter Leitungen. Im Gegensatz zur bisherigen Situation, in welcher beispielsweise Daten der Finanzverwaltung allein auf ihren Leitungen übertragen werden, erfolgt künftig die Übertragung über ein gemeinsames, auch von anderen Stellen nutzbares Medium, woraus sich eine neue Qualität der Datenübertragung ergibt.

Der LfD hat die aus seiner Sicht erforderlichen technisch-organisatorischen Maßnahmen formuliert. Er wird die Umsetzung seiner Empfehlungen im Lauf der weiteren Entwicklung verfolgen (vgl. Tz. 21.5).

21.3 Neue Technik fordert neue Datenschutzlösungen

Die Nutzung neuer Formen der Informationsverarbeitung wirft im allgemeinen unter den Gesichtpunkten Datenschutz und Datensicherheit eher neue Fragen auf, als daß sie alte beantwortet. Aufgrund der in vielen Fällen zu verzeichnenden Abkehr von zentralen Datenverarbeitungsstrukturen sind einige der in der Vergangenheit tauglichen Instrumente zur Sicherstellung eines adäquaten Datenschutzes nicht mehr einsetzbar oder in ihrer Wirksamkeit in Frage gestellt (Funktionstrennung, räumliche und bauliche IT-Sicherheit, zentrale Befugnisse und Verantwortlichkeiten usw.). Die in der Einsatzstrategie begründete, unter Datenschutzgesichtspunkten aber mangelhafte Hard- und Softwarearchitektur vieler Systeme führt dazu, daß neue Lösungen gefunden werden müssen.

Aufgrund der mittlerweile anerkannten wirtschaftlichen Bedeutung des Gutes „Information" werden erfahrungsgemäß für erkannte technische Sicherheitsprobleme zwar Lösungen angeboten, jedoch nur nach entsprechender Problematisierung und mit Verzögerung. Bedingt durch die Dynamik der technischen Entwicklung ergibt sich hieraus ein permanenter Handlungsbedarf.

Daneben bereiten insbesondere die sich aus der strukturellen Umgestaltung ergebenden organisatorischen Konsequenzen Probleme. Die Dezentralisierung der Informationstechnik führt in vielen Fällen zur Herauslösung aus der Verantwortlichkeit einer zentralen Datenverarbeitung. Die Einsicht in die Notwendigkeit von Maßnahmen zur Sicherstellung der Verfügbarkeit und Integrität von Datenbeständen war dort in vielen Fällen vorhanden; ein Verdienst des Datenschutzes ist es, diesen Bereich zusätzlich für die Notwendigkeit entsprechender Maßnahmen im Hinblick auf die Vertraulichkeit von Daten sensibilisiert zu haben.

Bei der Übertragung der Verantwortlichkeit auf den Anwender ist in vielen Fällen ein vergleichbares Problembewußtsein nicht gegeben. Die Erkenntnis, daß Leistungen, die in der Vergangenheit durch eine zentrale DV „automatisch" erbracht wurden (Datensicherung, Benutzerverwaltung, Zugriffskontrolle, Datenträgerverwaltung etc.), nunmehr in der Verantwortung der Anwender selbst liegen, trifft viele unvorbereitet.

Hinzu kommt, daß häufig das hierfür eingesetzte Personal nicht über die erforderliche Ausbildung verfügt. Datenschutzprobleme ergeben sich dabei oftmals nicht aufgrund mangelnder Einsicht, sondern aus Unkenntnis. Betrachtet man die zunehmende Komplexität des IT-Einsatzes, so wird ersichtlich, daß die Strukturänderungen nicht aus einer einfachen Verlagerung ehemals zentral wahrgenommener Aufgaben auf dezentrale Anwender bestehen kann.

Der Vorwurf, es sei ein Rückfall in den Sicherheitsstandard der 70er Jahre zu verzeichnen, trifft in dieser Pauschaliertheit sicher nicht zu. Aus der Sicht des Datenschutzes ist jedoch zu fordern, daß eine Verlagerung nur auf der Grundlage vorhandener Einsatz-, insbesondere Sicherheitskonzepte, koordiniert und mit entsprechender Schulung der Anwender, erfolgen darf. Bestimmte Aufgaben (Systembetreuung, Datenträgerverwaltung, organisatorische Steuerung des IT-Einsatzes) müssen von zentralen Stellen wahrgenommen werden.

21.4 Ergebnisse der Kontroll- und Beratungstätigkeit

21.4.1 Allgemeines

Im Berichtszeitraum wurden örtliche Feststellungen unter technisch-organisatorischen Gesichtpunkten in unterschiedlichen Bereichen der staatlichen und kommunalen Verwaltung getroffen (Finanzämter, Gesundheitsämter, Staatsanwaltschaft, Kreisverwaltungen, Verbandsgemeindeverwaltungen, Ministerium, Rechenzentrum). Ferner wurde ein mit der Erfassung von Steuerdaten beauftragtes privates Unternehmen geprüft.

Die Prüfungen standen in der Regel im Zusammenhang mit der Beteiligung des LfD bei der Einführung neuer bzw. der Änderung bestehender Verfahren. Daneben wurde mit der systematischen Prüfung allgemeiner technisch-organisatorischer Maßnahmen beim Einsatz der Informationstechnik, außerhalb bestimmter Anwendungen, begonnen. Trotz der Gefährdungen durch unbefugte oder unzulässige Datenzugriffe oder Mißbrauch aufgrund der erweiterten Möglichkeiten der Informationstechnik ergibt sich im technisch-organisatorischen Bereich ein Großteil der Probleme aufgrund von Versäumnissen oder Nachlässigkeiten am „unteren Ende" der Maßnahmenskala. Insbesondere im Zusammenhang mit der unter Tz. 21.1 dargestellten Umgestaltung der IT-Strukturen sind hier Mängel zu beklagen.

Schwerpunkte der systematischen Prüfungen waren die Bereiche

- Anmeldungen zum Datenschutzregister,
- Existenz und Ausgestaltung von Dienstanweisungen zum technisch-organisatorischen Datenschutz,
- Existenz von Einsatz- und Sicherheitskonzepten,
- Einsatz von Sicherheitshard- und Software,
- Steuerung und Koordinierung des IT-Einsatzes (Beschaffung, System- und Anwenderbetreuung, Zuständigkeitsregelungen)
- Benutzerverwaltung (Zugangs- und Zugriffskontrolle),
- Regelung zur Nutzung privater Hard- und Software,
- Datenträgerverwaltung (Kennzeichnung, Ausgabe/Annahme, Transport, Versand, Aufbewahrung, Entsorgung),
- Ausbildung der Anwender und Systembetreuer.

Für die Zukunft ist beabsichtigt, mit gleichen Schwerpunkten Feststellungen in unterschiedlichen Verwaltungsbereichen zu treffen. Begonnen wurde 1993 mit Kreisverwaltungen; bei bislang fünf Landkreisen wurden Prüfungen vorgenommen. Festgestellte Defizite hinsichtlich technisch-organisatorischer Maßnahmen sind nachfolgend dargestellt. Allgemein ergibt sich ein durchaus unterschiedliches Bild und die sicherlich nicht neue Erkenntnis, daß die datenschutzgerechte Ausgestaltung nicht allein von technischen Rahmenbedingungen, sondern in hohem Maß vom Bewußtsein, Engagement sowie Ausbildungs- und Kenntnisstand der handelnden Personen abhängig ist.

Eine unter Datenschutzgesichtspunkten zufriedenstellende Situation ist, wie ein Quervergleich zeigt, im wesentlichen unabhängig von Größe, Verwaltungs- und Finanzkraft einer Verwaltungseinheit.

Ergänzt wurden die örtlichen Feststellungen durch Informationsbesuche bei unterschiedlichen Stellen, insbesondere im Hinblick auf die für die Überwachung der Einhaltung des Datenschutzes erforderliche Kenntnis der Art und Struktur des IT-Einsatzes.

Die Möglichkeit der Beratung durch den LfD in technisch-organisatorischen Datenschutzfragen wurde nur in Einzelfällen in Anspruch genommen.

Inwieweit die Zurückhaltung beim Herantreten an den LfD auf einer – unzutreffenden – Einschätzung des Datenschutzes als „schlafenden Hund", den es im Sinne einer reibungslosen Aufgabenerfüllung tunlichst nicht zu wecken gilt, dessen Bellen man jedoch Beachtung schenken muß, beruht, sei dahingestellt. Für beide Seiten befriedigende Ergebnisse waren regelmäßig dann zu erzielen, wenn es gelang, die für technisch-organisatorische Maßnahmen oftmals vorhandene Kongruenz der Anforderungen sowohl des Datenschutzes als auch der speichernden Stelle hinsichtlich Vertraulichkeit, Verfügbarkeit und Integrität der verarbeiteten Daten darzulegen. Einige Problemfelder werden nachfolgend aufgezeigt:

21.4.2 Dienstanweisungen

Hintergrund der in § 9 Absatz 2 LDatG formulierten Verpflichtung zum Festschreiben der getroffenen Datenschutzmaßnahmen in einer Dienstanweisung ist die Absicht, den Mitarbeitern Handlungsanweisungen für ein datenschutzgerechtes Verhalten bei der täglichen Arbeit zu geben. Leider ist festzustellen, daß dieser Verpflichtung nicht in ausreichendem Umfang Rechnung getragen wird, sei es, daß entsprechende Dienstanweisungen nicht vorliegen oder aber, daß sie veraltet sind.

Hinsichtlich des Umfangs der Dienstanweisungen erkennt auch der LfD das Spannungsverhältnis zwischen dem Streben nach Vollständigkeit und einer im Sinne der Handhabbarkeit und Lesbarkeit zu fordernden Beschränkung auf zentrale Punkte. Ein allgemeiner Hinweis auf die „Einhaltung der datenschutzrechtlichen Bestimmungen" als wesentlicher Inhalt einer Dienstanweisung erscheint jedoch auch im Licht der Angemessenheit als unzureichend.

Im Rahmen der Vorgaben des § 9 LDatG sollte eine Dienstanweisung zum Datenschutz insbesondere folgende Bereiche abdecken:

- Ziele der Dienstanweisung,
- Bestehende Maßnahmen zum Datenschutz, ggf. Sicherheitskonzepte,
- Verantwortlichkeiten und Zuständigkeiten im Rahmen des IT-Einsatzes (Ansprechpartner),
- Datenträgerverwaltung (Kennzeichnung, Ausgabe, Rücknahme, Entsorgung, Annahme und Versand, Aufbewahrung),
- Einsatz privater Hard- und Software,
- Besucher, Wartungs- und Reinigungspersonal,
- Verhalten bei Abwesenheit,
- Gestaltung und Verwendung von Paßwörtern,
- Entsorgung von Schriftgut mit personenbezogenen Daten,
- Löschen von Daten,
- Datensicherung.

21.4.3 Paßwortregelungen

Paßwörter sind eine Möglichkeit, sich gegenüber einem IT-System zu legitimieren, in diesem Fall über den Nachweis „geheimen" Wissens. Die Wirksamkeit des Paßworts ist dabei abhängig vom Grad der Geheimhaltung und der Sorgfalt im Umgang, insbesondere im Hinblick auf regelmäßige Änderung. Unter Berücksichtigung des Beharrungsvermögens der Anwender bieten die meisten Paßwortsysteme Mechanismen zur Paßwortverwaltung wie

- Begrenzung der Gültigkeitsdauer,
- Mindeststellenzahl,
- Sperrung der zuletzt benutzten Paßwörter,
- Begrenzung ungültiger Anmeldeversuche,
- Auschluß bestimmer Zeichenfolgen (abcdef, 11111, xxx etc.) als Paßwörter u. ä. m.

Bei Kontrollen war in vielen Fällen feststellbar, daß, obwohl derartige Mechanismen zur Verfügung standen, diese nicht oder nur unzureichend genutzt wurden. Der Wind des Wechsels erfaßt Paßworte nur zögerlich!

Der Einsatz von Benutzerkennungen und Paßworten stellt in vielen Fällen die wirksamste und teilweise einzige Möglichkeit einer Zugangs- und Zugriffskontrolle dar; entsprechend sorgfältig sollte daher der Umgang damit erfolgen. Einige Hinweise zur Gestaltung und zum Einsatz von Paßworten sind in Anlage 11 zusammengefaßt.

21.4.4 Datenträgerverwaltung

Die zunehmende Dezentralisierung des IT-Einsatzes hat Auswirkungen auch auf Art und Zahl der verwendeten Datenträger. Neben Magnetbändern und optischen Datenträgern finden Disketten und Magnetbandkassetten im Rahmen der Datenhaltung und Datensicherung Verwendung. So werden Disketten wegen ihrer Handlichkeit und Speicherkapazität als Informationsträger zunehmend geschätzt und in diesem Zusammenhang u. a. auch verschickt. Als Folge bilden sich in vielen Fällen in Schreibtischschubladen, Aktenschränken und Diskettenboxen Sammelsurien von Musterdisketten, Sicherungsdisketten, „Mal-eben-zwischendurch-gespeichert"-Disketten, beschädigten Disketten, Installationsdisketten, Programmdisketten, „Weiß-nicht-wohin"-Disketten usw. Eine Übersicht über die hierbei gespeicherten Daten ist nur schwer zu behalten und wird, ebenso wie die Entscheidung über die vom Gesetz geforderte Löschung, mit steigendem Umfang der Sammlung nahezu unmöglich.

Bei keiner der kontrollierten Stellen bestanden in diesem Zusammenhang beim dezentralen IT-Einsatz ausreichende Regelungen für eine ordnungsgemäße Datenträgerverwaltung, -nutzung und -entsorgung. Bedauerlich ist dies insoweit, als bereits einfache organisatorische Vorkehrungen einen Schutz vor unabsichtlicher Preisgabe von Daten ermöglichen – erstaunlich auch im Hinblick auf die Tatsache, daß zahlreiche Computerviren ihren Infektionsweg über die Diskettenverarbeitung nehmen.

Die Datenträgerverwaltung kann nicht in das Belieben der Anwender gestellt werden. Für eine ordnungsgemäße Datenträgerverwaltung sind aus der Sicht des Landesbeauftragten u. a. folgende Punkte zu berücksichtigen:

- Eindeutige Kennzeichnung der Datenträger mit Angabe des Eigentümers (z. B. Aufkleber mit Datenträgernummer und Behördenbezeichnung, ggf. Organisationseinheit). Im Falle eines Verlustes ist damit eine Zuordnung möglich, ohne in den Datenbestand Einblick nehmen zu müssen. Durch die Zuordenbarkeit kann ggf. in Verbindung mit einer Empfangsbestätigung, die bei der Ausgabe zu unterschreiben ist, ein erhöhtes Verantwortungsgefühl seitens der Anwender erreicht werden.
- Ausgabe, Rücknahme und Entsorgung von Datenträgern durch eine zentrale Stelle.

  Für nicht mehr benötigte eigene oder zugesandte, defekte und unbrauchbare Disketten/Datenträger muß eine geordnete Form der Rückgabe und ggf. Löschung und Entsorgung festgelegt sein.

- Festgelegte Verfahren für die Annahme und den Versand von Datenträgern (zentrale Annahme, ggf. Virenprüfung, Weiterleitung).
- Festgelegte Verfahren für den Versand von Datenträgern (Kopie der Daten auf physikalisch gelöschte bzw. unbenutzte Datenträger vor dem Versand, Versandnachweise).
- Grundsätzliches Verbot der Verwendung privater Datenträger.

Von gleicher Bedeutung wie Regelungen zur Verwendung und Aufbewahrung von Datenträgern ist die Bereitstellung geeigneter Aufbewahrungsmöglichkeiten. Fälle wie der, daß zwar Geräte für mehrere Tausend DM zur Verfügung standen, die Mittel für einen geeigneten Blechschrank zur Lagerung der Datenträger jedoch erst nach drei Jahren bewilligt wurden, sollten sich nicht wiederholen.

21.4.5 Einsatz von Sicherheitsprodukten

Eine Vielzahl der insbesondere im Bereich der Arbeitsplatzrechner eingesetzten Geräte besitzt systemseitig nur unzureichende Sicherheitsmechanismen. Eine Abschottung der jeweiligen Datenbestände verschiedener Benutzer, ein systemseitiger Schutz vor unbefugter Inbetriebnahme und unbefugtem Datenzugriff sowie die Möglichkeit der Protokollierung sensibler Aktivitäten sind hier nicht oder nur ungenügend ausgebildet. Bei der Verarbeitung personenbezogener Daten muß dieses Defizit daher, abhängig von der Sensitivität der verarbeiteten Daten, gebenenfalls über zusätzliche Hard- oder Softwareerweiterungen ausgeglichen werden. Derartige Produkte werden am Markt mittlerweile in großer Zahl und mit unterschiedlichem Funktionsumfang angeboten, zudem bestehen in verschiedenen Ressorts entsprechende Rahmenverträge.

Wie die Ergebnisse örtlicher Feststellungen zeigen, wird dieser Forderung teilweise nur unzureichend Rechnung getragen. Während in bestimmten Verwaltungszweigen standardmäßig eine Nachrüstung erfolgt bzw. entsprechende Ergänzungen bereits bei der Beschaffung berücksichtigt werden, sind insbesondere im kommunalen Bereich zum Teil erhebliche Defizite zu beklagen. Die Anforderungen des § 9 LDatG insbesondere hinsichtlich der erforderlichen Zugriffs-, Speicher- und Eingabekontrolle werden in vielen Fällen nicht erfüllt. Die Gründe hierfür sind vielfältig und reichen von mangelndem Problembewußtsein oder falsch verstandener Wirtschaftlichkeit bis hin zu schlichter Unkenntnis. Vielen ist nicht bewußt, daß die Verarbeitung personenbezogener Daten in einem automatisierten Verfahren, das keine angemessene Datensicherheit bietet, gegen die Datenschutzgesetze verstößt. In diesem Sinne hat sich auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom 10. Oktober 1988 geäußert.

Soweit eine ausreichende Sicherheit nicht durch vom System bereitgestellte Funktionen erreicht werden kann, sind entsprechende Ergänzungen vorzusehen. Zweckmäßigerweise sollten diese Gesichtspunkte bereits bei der Beschaffung berücksichtigt werden.

21.4.6 Entsorgung von Schriftgut

Die Notwendigkeit der datenschutzgerechten Entsorgung von Schriftgut mit personenbezogenen Daten wird allgemein erkannt, entsprechende Anweisungen sind in der Regel vorhanden. Verschiedene Vorkommnisse im Berichtszeitraum im Bereich der Landesregierung zeigen jedoch einmal mehr, daß Vorgaben, Regelungen, Anweisungen und Vorschriften allein ein datenschutzgerechtes Verhalten nicht garantieren: Es bedarf der ergänzenden Kontrolle, um den Papierkorb nicht zur ergiebigen Datenquelle werden lassen.

In einem Fall landeten Unterlagen statt wie vorgesehen in den verschließbaren Altpapierbehältern im – unverschlossenen – Hausmüllcontainer; in einem anderen fand ein „recherchierender Journalist" in unverschlossenen Papiercontainern mehrerer Ministerien Schriftstücke mit zum Teil sensiblen personenbezogenen Daten (Unterlagen über Leistungen bei Schwerpflegebedürftigkeit, Informationen über Vermögensverhältnisse usw.).

Eine Überprüfung durch den LfD ergab, daß durch die ungenügende Schriftgutentsorgung datenschutzrechtliche Vorschriften, u. a. das Sozial- und Steuergeheimnis, verletzt wurden. Als Konsequenz aus den Vorfällen wurden in den betroffenen Behörden bestehende organisatorische Anweisungen überprüft und geändert. In einem Fall erfolgte kurzfristig die Beschaffung zusätzlicher Aktenvernichter für die dezentrale Aufstellung, in einem anderen ist ergänzend zur Schriftgutvernichtung durch entsprechende Unternehmen die Anschaffung einer zentralen Papiervernichtungsanlage vorgesehen.

Wie leichtfertig bisweilen gehandelt wird, zeigt ein kurz vor Abschluß des Tätigkeitsberichts zutage getretener weiteren Fall: Eine Stadtverwaltung veräußerte alte Büroschränke und beachtete nicht, daß sich in diesen Schänken noch Altakten befanden.

Zwei allgemeine Erkenntnisse aus der Kontrollpraxis seien abschließend noch herausgegriffen:

- Die Höhe der Papierberge in den Arbeitszimmern steht bei dezentraler Sammlung/Vernichtung in proportionalem Verhältnis zur Entfernung des nächsten Sammelbehälters/Aktenvernichters. Soweit die Sammlung oder Vernichtung in der Verantwortung der Beschäftigten liegt, sind hierfür ausreichende Möglichkeiten zu schaffen.
- Die Vernichtung von Schriftgut am Ort der Entstehung kann sicher nicht das Ideal einer Verwaltung sein, an bestimmten neuralgischen Stellen wie Kopierraum, zentralem Schreibdienst, Personalstelle usw. sollten jedoch direkte Möglichkeiten zur Schriftgutvernichtung bestehen.

21.5 Landesdatennetz Rheinland-Pfalz (LDN)

Beim Landesdatennetz Rheinland-Pfalz handelt es sich um ein vom Landesrechenzentrum Mainz betriebenes flächendeckendes Datenkommunikationsnetz auf der Basis überwiegend festgeschalteter Leitungsverbindungen. Angeschlossen sind eine Vielzahl unterschiedlicher Verwaltungen (Melde- und Katasterämter, Ausländerbehörden, KfZ-Zulassungsstellen, Polizeidienststellen, Ministerien, Bezirksregierungen usw.) sowie weitere Rechenzentren. Ein Anschluß erfolgt bislang überwiegend zur Nutzung von im LRZ zentral betriebenen Verfahren.

Entsprechend der Entwicklungen im Bereich der Informationstechnik haben sich im Lauf der Jahre sowohl Änderungen der Struktur des LDN als auch der Anforderungen an ein derartiges Kommunikationsnetz ergeben. Neben „unintelligenten" Endgeräten (Terminals) wurden immer öfter Systeme mit eigener Speicher- und Rechenkapazität entsprechend der Veränderungen der IT-Infrastruktur in der Landes- und Kommunalverwaltung als Netzknoten eingebunden. Da diese ihrerseits mit weiteren Kommunikationsverbindungen ausgestattet sein können, ergibt sich sehr schnell ein hoher Vernetzungsgrad. Damit verbunden sind Bestrebungen, das LDN nicht allein als Zugang zu bestimmten zentralen Anwendungen, sondern darüber hinaus als allgemeines Medium für die Datenkommunikation der angeschlossenen Stellen untereinander zu nutzen.

Das für das Netz vorhandene Instrumentarium der Zugangs- und Zugriffskontrolle hat mit dieser Entwicklung nicht Schritt gehalten und bietet beim heutigen Stand der Informationstechnik keine ausreichende Datensicherheit mehr. Eine lediglich gerätebezogene Zugangs- und Zugriffskontrolle, d. h. die Orientierung der möglichen Datenzugriffe über den Netzwerknamen im wesentlichen am Endgerät und dessen Standort (z. B. Meldeamt) und nicht an den konkreten Befugnissen einzelner Nutzer, entspricht nicht den Anforderungen des § 9 LDatG.

Beim Zugang mehrerer Anwender über die „Geräteadresse" eines lokalen Netzwerkes bzw. eines Behörden- oder Abteilungsrechners, wie er in der Praxis bereits erfolgt, ist die Festlegung gegebenenfalls erforderlicher unterschiedlicher Zugriffsprofile nicht im erforderlichen Umfang möglich.

Der LfD hat demzufolge bereits mehrfach eine dem Stand der Technik entsprechende, die gerätebezogene Kontrolle ergänzende benutzerorientierte Zugangs- und Zugriffskontrolle gefordert (vgl. 12. Tb, Tz. 19.6; 13. Tb, Tz. 20.4).

Aufgrund der heterogenen Zusammensetzung des Kreises der Netzteilnehmer und der erforderlichen Eindeutigkeit der Benutzerkennungen ist hierfür aus der Sicht des Datenschutzbeauftragten eine Systematik erforderlich, welche die angeschlossene Stelle (Behörde, Ort), den funktionalen Bereich sowie den Anwender erkennen läßt. Über die Definition von Benutzergruppen (funktionale Bereiche), Benutzerkennungen (z. B. Namen) und entsprechender Profile muß in Verbindung mit Authentifizierungsmechanismen sichergestellt werden, daß ein Zugang zu bestimmten Verfahren und Verfahrensteilen und deren Nutzung nur möglich ist, wenn hierzu eine explizite Berechtigung besteht.

Eine spürbare Verbesserung der aus Datenschutzsicht unbefriedigenden Situation ist bislang nicht erfolgt. Nach längeren Vorarbeiten wurde vom Ministerium des Innern und für Sport jedoch zwischenzeitlich der Entwurf einer Benutzungsordnung für das LDN vorgelegt, welche die allgemeinen Bedingungen für den Betrieb und die Nutzung festlegt. Die wesentlichen Forderungen einer seinerzeit noch von der DSK angeregten Arbeitsgruppe wurden dabei berücksichtigt, nämlich

- Einrichtung einer benutzer- und gerätebezogenen Zugangskontrolle als Voraussetzung des Netzzugangs,
- Definition von Benutzer- und Gruppenprofilen,
- Differenzierbarkeit der Netzanwender nach Verwaltungen und Verwaltungsteilen auf der Grundlage des funktionalen Behördenbegriffs,
- Festlegung der Zuständigkeiten und Verantwortlichkeiten im Rahmen der verteilten Administration der Netzwerksicherheit,
- Protokollierung und Auswertbarkeit der Netzzugriffe und Datenübermittlungen,
- Geltung der Regelungen des Netzzugangs für alle, d. h. die datenschutzrechtlich relevanten als auch die übrigen Anwendungen.

Die Benutzerordnung soll in Form eines Rundschreibens veröffentlicht werden. Hinsichtlich der praktischen Ausgestaltung der einzelnen Vorgaben soll sie durch ein Benutzerhandbuch ergänzt werden, an dessen Erstellung der LfD beteiligt ist.

Die für die Umsetzung der benutzerorientierten Zugangskontrolle erforderlichen Programmentwicklungen wurden in die Wege geleitet; für die endgültige Einrichtung ist die Beschreibung des funktionalen Behördenaufbaus durch die angeschlossenen Stellen auf der Grundlage einer vom LRZ bereitgestellten Nomenklatur erforderlich. Im Rahmen der verteilten Zuständigkeiten bei der Netzadministration hat das Landesrechenzentrum als Netzbetreiber ein Konzept für ein dezentrales Sicherheitsmanagement im Systemverbund erarbeitet. Durch die Definition entsprechender Schnittstellen und Benutzeroberflächen sollen den lokalen Systemverwaltern damit auf unterschiedlichen Systemplattformen einheitliche und synchronisierte Sicherheitsfunktionen bereitgestellt werden.

Der LfD wird die Umsetzung der beabsichtigten Maßnahmen mit kritischem Interesse verfolgen.

21.6 Sicherheitsmaßnahmen beim Einsatz tragbarer Systeme

Der Einsatz tragbarer Datenverarbeitungssysteme – im Bereich der Privatwirtschaft bei Außendienstmitarbeitern in Form von Laptops, Notebooks, Handhelds usw. schon seit längerem üblich – hat im Bereich der Landesverwaltung mittlerweile ebenfalls eine nennenswerte Größenordnung erreicht.

So finden diese Geräte u. a. in der Finanzverwaltung (Betriebsprüfung, Steuerfahndung), der Gesundheitsverwaltung (Schulärztlicher Dienst) und der Überwachung des ruhenden Verkehrs Verwendung. Hinsichtlich ihrer Leistungsfähigkeit sind sie stationären Systemen oft ebenbürtig. Da die Miniaturisierung auch die für die Kommunikation erforderlichen Komponenten umfaßt (z. B. Funkmodem), ist mittlerweile eine vollständige mobile Datenverarbeitung und -kommunikation möglich. Aufgrund der besonderen Einsatzsituation ergeben sich vermehrt Mißbrauchsmöglichkeiten.

In Umkehrung der seinerzeitigen „Philosophie" der PC-Pioniere „Traue keinem Computer, den Du nicht selbst hochheben kannst!" müssen gerade die unteren Gewichtsklassen unter Datenschutzgesichtspunkten verstärkt Beachtung finden. Naturgemäß sind dabei alle auf die bauliche, räumliche und organisatorische Absicherung ausgerichteten Maßnahmen nicht einsetzbar, die Sicherstellung der Anforderungen des Datenschutzes muß hier vorrangig über technische Lösungen erfolgen.

Eine Prüfung der im Einzelfall getroffenen Maßnahmen durch den Landesbeauftragten ergab unterschiedliche Ergebnisse. Während im Bereich der Finanzverwaltung die Systeme im wesentlichen zufriedenstellend abgesichert waren, waren in anderen Bereichen erhebliche Defizite zu verzeichnen. Datensicherungsvorkehrungen waren nur unzulänglich ausgestaltet und wurden beanstandet. Folgende Maßnahmen sind aus der Sicht des Landesbeauftragten für einen datenschutzgerechten Einsatz mobiler Systeme mindestens erforderlich:

- Schutz vor unbefugter Inbetriebnahme:
  Eine Inbetriebnahme darf erst nach erfolgter Legitimation eines befugten Nutzers möglich sein. Erreichbar ist dies durch entsprechende Software- (Sicherheitsoberfläche mit Paßwortabfrage) oder Hardwarelösungen (Chip-Karte, Token, Erweiterungskarte). Bei neueren Systemen sind derartige Mechanismen in vielen Fällen systemseitig bereits vorhanden (BIOS), oder es besteht die Möglichkeit einer entsprechenden Nachrüstung (PCMCIA-Steckplatz).

  Einige Geräte erlauben einen sogenannten Stand-by-Betrieb, in dem das Gerät in eingeschaltetem Zustand bei verminderter Leistungsaufnahme betriebsbereit gehalten wird und auf Tastendruck hin wieder aktiviert werden kann. Bei den meisten Systemen ist zudem ein Systemstart (Booten) von Diskette möglich. In allen diesen Fällen muß sichergestellt sein, daß das Legitimationsverfahren bei jeder Inbetriebnahme und vor der Herstellung der endgültigen Betriebsbereitschaft durchlaufen wird. Soweit ein Laden von Diskette nicht ausgeschlossen werden kann (z. B. über entsprechende Setup-Einstellungen), muß der Zugriff auf die Daten einer ggf. vorhandenen Festplatte ausgeschlossen sein.

- Verschlüsselung:
  Mobile Systeme unterliegen, weil die immanente Kontrolle einer Büroumgebung fehlt, einem höheren Mißbrauchsrisiko und zudem aufgrund ihrer Abmessungen einem besonderen Diebstahlrisiko. Mehr noch als bei Arbeitsplatzrechnern muß daher ein effektiver Zugriffsschutz gegeben sein. Eine Möglichkeit hierzu bietet die Verschlüsselung. Mittlerweile stehen Lösungen zur Verfügung, die ohne merkbare Geschwindigkeitsverluste eine qualitativ hochwertige Verschlüsselung erlauben.

- Gehäusesicherung:
  Über eine entsprechende Gehäusesicherung sollten Hardwaremanipulationen soweit möglich verhindert, zumindest aber erkennbar gemacht werden (Versiegelung, Verplombung).

- Deaktivierung nicht benötigter Gerätefunktionen:
  Nicht benötigte Systemfunktionen (Diskettenlaufwerk, Kommunikationsschnittstellen, Druckeranschluß usw.) sollten soweit möglich deaktiviert werden. Erfolgen kann dies über ggf. vorhandene Setup-Konfigurationsmöglichkeiten oder entsprechende Funktionen der Sicherheitshard- oder Software.

Weiterhin sind die für stationäre Systeme bestehenden Anforderungen des LfD zugrunde zu legen (vgl. Informationen zum Datenschutz, Heft 2 „Datenschutzrechtliche Sicherungsmaßnahmen"). Insbesondere sind die technischen Maßnahmen durch organisatorische Regelungen zum Einsatz und zur Aufbewahrung der Geräte zu ergänzen (vgl. 13. Tb., Tz. 20.2).

21.7 Projekt „Ressortübergreifende Kommunikation"; Elektronischer Dokumentenaustausch

Im Projekt „Ressortsübergreifende Kommunikation" wird auf der Grundlage internationaler Normen und landesweiter Standards (ODA/ODIF, X.400) unter Beteiligung verschiedener Ministerien der Austausch elektronischer Dokumente, unabhängig von der in den jeweiligen Häusern eingesetzten Systemumgebung, erprobt. Das Projekt ist in mehrere Teile untergliedert, die Phase der Prüfung der technischen Machbarkeit wurde kürzlich abgeschlossen. Die im Rahmen des Projektes gewonnenen Erkenntnisse sollen künftige Grundlage des elektronischen Dokumentenaustauschs zwischen den Ressorts sowie zwischen diesen und den nachgeordneten Bereichen sein.

Die technische Abwicklung der Kommunikation erfolgt über das Datex-P-Netz der DBP-Telekom, der Übergang auf ISDN ist vorgesehen. Hinsichtlich der Realisierung erforderlicher Maßnahmen des technisch-organisatorischen Datenschutzes ist der LfD an die Staatskanzlei und an das Ministerium des Innern und für Sport herangetreten. Neben Fragen der Zugangskontrolle in bezug auf die Netzanschlüsse sind dabei Maßnahmen von Bedeutung, die Vertraulichkeit und Integrität auf dem Kommunikationsweg sicherstellen (z. B. Verschlüsselung und digitale Unterschrift). Weitere Maßnahmen sind Parametrierungsmöglichkeiten. So sollte der Versand von Nachrichten nur für die Stelle möglich sein, von der aus die Verbindung aufgebaut wurde. Weiterhin ist ein besonderer Schutz der Routing-Tabellen (Adressen) erforderlich. Die zugrunde gelegten Normen (X.400/1988) bieten die Möglichkeit der Einbindung von Mechanismen der Authentifizierung und Integritätsprüfung sowie des Vertraulichkeitsschutzes.

Die Bezeichnungen „elektronischer Dokumentenaustausch" oder „elektronische Post" geben den Funktionsumfang nur bedingt wieder. Die Möglichkeit, Notizen, Vermerke, Schreiben usw. elektronisch zu versenden, stellt lediglich einen Ausschnitt aus dem Leistungsspektrum dar; als Anlage oder sogenannte Attachements können einem Dokument Dateien jeglicher Art und damit beispielsweise Ergebnisse einer Datenbankabfrage als maschinell lesbarer Datenbestand oder aber ablauffähige Programme beigefügt werden. In Verbindung mit der bei vielen Postsystemen vorhandenen Möglichkeit, Betriebssystemkommandos abzusetzen oder im Anschluß an eine Übertragung Programme zu starten, ergeben sich u. U. beachtliche Risiken für die Datensicherheit. In einigen in den USA bekanntgewordenen Fällen war aufgrund derartiger Schwachstellen im elektronischen Postsystem ein unbefugtes Eindringen Außenstehender in Rechnernetze möglich.

Der LfD sieht daher die Berücksichtigung entsprechender Sicherungsmöglichkeiten als Voraussetzung eines künftigen Austauschs elektronischer Dokumente an und wird im weiteren Projektverlauf auf die Realisierung derartiger Maßnahmen hinwirken.

21.8 Verfahrensübergreifende Sicherheitskonzepte beim Einsatz der Informationstechnik

Die im Rahmen der Kontrolltätigkeit des Landesbeauftragten für den Datenschutz gewonnenen Erkenntnisse zeigen, daß, entsprechend der in den letzten Jahren erfolgten Entwicklung, die technikunterstützte Informationsverarbeitung zunehmend auf der Basis heterogener, parallel betriebener Lösungen erfolgt (vgl. Tz. 21.1). Neben Terminalanschlüssen an Rechenzentren und dem Betrieb von Anlagen der mittleren Datentechnik sind in rheinland-pfälzischen Behörden in steigendem Maße Systeme unterschiedlicher Funktionalität und Netzeinbindung bis hin zu mobilen Systemen anzutreffen.

Die Beschreibung der zum Datenschutz erforderlichen technisch-organisatorischen Maßnahmen findet sich, soweit vorhanden, entsprechend den Richtlinien zur Planung und Gestaltung von ADV-Verfahren in aller Regel als Bestandteil der jeweiligen verfahrensspezifischen Dokumentation oder in den gemäß § 9 Abs. 2 LDatG erforderlichen, zumeist ebenfalls verfahrensorientierten Dienstanweisungen.

Vor dem Hintergrund eines in der Vergangenheit überwiegend zentralen oder in der Form von Behörden- und Abteilungsrechnern überschaubar dezentralen IT-Einsatzes stellte eine solche isolierte Vorgehensweise einen sinnvollen Ansatz dar. Diese Form des IT-Einsatzes war durch Homogenität der eingesetzten Technik und eine vergleichsweise statische Situation hinsichtlich Änderungen der Funktionalität gekennzeichnet. Damit konnten die im Rahmen der Verfahrensplanung berücksichtigten Sicherheitsmaßnahmen für die Dauer des Verfahrens im wesentlichen unverändert beibehalten werden.

Die zwischenzeitlich erfolgte Entwicklung im Bereich der Informations- und Kommunikationstechnik hat zu einer Veränderung dieser Situation geführt; sie erfordert eine geänderte Betrachtungsweise. Verfahrensübergreifende Vorgaben liegen bislang jedoch nur in Ausnahmefällen vor.

Ansatzpunkt einer offenen Netzkonzeption (vgl. Tz. 21.5.1) ist erklärtermaßen der Zusammenschluß unterschiedlichster Systeme zur gemeinschaftlichen Datenutzung bis hin zur Realisierung verteilter Anwendungen. Daneben werden die beteiligten Systeme lokal ebenfalls für bestimmte Anwendungen genutzt. Insoweit greift eine lediglich verfahrensbezogene Beurteilung der erforderlichen Sicherheitsmaßnahmen zu kurz.

Ein weiterer Aspekt ist die mittlerweile erreichte Leistungsfähigkeit der eingesetzten Software für Arbeitsplatzrechner, welche die komfortable Verwaltung auch größerer Datenbestände erlaubt, was erfahrungsgemäß insbesondere in größeren Verwaltungseinheiten dazu führt, daß ein Überblick über Art und Umfang der Datenverarbeitung nur bedingt vorhanden ist.

Bei der dezentralisierten Nutzungsverantwortung für die Systeme, insbesondere beim Einsatz von Standardsoftware, ist eine verfahrensmäßige, d. h. in die verschiedenen Realisierungsphasen der „Richtlinien zur Gestaltung von ADV-Verfahren in der Landesverwaltung" untergliederte Vorgehensweise im allgemeinen nicht gegeben.

Eine qualifizierte Entscheidung über die Erforderlichkeit von Datensicherungsmaßnahmen ist daher nur bei einem verfahrensübergreifenden Ansatz sichergestellt. Die Bedeutung bisheriger verfahrensorientierter Sicherheitskonzepte wird dadurch nicht geringer; auf der Basis eines allgemeinen Konzeptes müßten diese jedoch künftig verfahrensspezifische Ergänzungen enthalten.

Anzustreben ist eine Situation in der, unabhängig von der Art der eingesetzten Informationstechnik und der Qualität der betroffenen Datenbestände, über die Definition eines behörden- bzw. organisationsspezifischen Mindeststandards ein bestimmtes Sicherheitsniveau festgelegt wird. Aus der Sicht des Datenschutzes ist es nicht hinnehmbar, daß gleiche Datenbestände allein durch die Verlagerung auf andere IT-Systeme einem z. T. deutlich geringeren Sicherheitsstandard unterliegen. Unabhängig von der eingesetzten Hardwareplattform sind vergleichbare Mechanismen der Zugangs- und Zugriffskontrolle sicherzustellen. Auf welche Art und Weise der festgelegte Standard systemspezifisch realisiert wird, bleibt dabei weitgehend offen; Veränderungen bei der Art der eingesetzten Systeme erfordern nicht grundsätzlich eine Anpassung des Sicherheitskonzeptes.

Der LfD hat die Angelegenheit im Interministeriellen Ausschuß für automatisierte Informationsverarbeitung (IMA) thematisiert und wird sie, auch im Hinblick auf die beabsichtigte Neuorganisation der Informationstechnik, weiterverfolgen.

21.9 Datenverarbeitung im Auftrag durch private Dritte

Die in § 4 Landesdatenschutzgesetz beschriebene Datenverarbeitung im Auftrag ist eine auch in Rheinland-Pfalz häufig praktizierte Form. Hinsichtlich automatisierter Verfahren erfolgt dabei die Wahrnehmung von IT-Aufgaben in den meisten Fällen durch Institutionen in öffentlicher Trägerschaft, seltener durch private Auftragnehmer. Insbesondere bei letzteren muß vertraglich sichergestellt sein, daß die für den Auftraggeber geltenden datenschutzrechtlichen Anforderungen Beachtung finden. Unter technisch-organisatorischen Gesichtspunkten waren dabei im Berichtszeitraum zwei Fälle von Bedeutung.

In einem Fall erfolgte die Erfassung von Steuerdaten durch ein privates Datenerfassungsunternehmen (vgl. Tz. 13.3). Bei einer Prüfung der technisch-organisatorischen Maßnahmen durch den LfD haben sich keine Bedenken ergeben, die einer Verlagerung der Erfassungstätigkeiten widersprächen. Es wurden jedoch Empfehlungen ausgesprochen, die aus der Sicht des LfD Voraussetzung einer Auftragsvergabe sind.

- In dem der Auftragsvergabe zugrunde liegenden Vertrag sollten Prüfungsrechte sowohl des Auftraggebers wie auch des LfD vereinbart werden.
- Vor einer Vertragsverlängerung sollte eine Überprüfung der technisch-organisatorischen Maßnahmen durch den Auftraggeber erfolgen und das Ergebnis dokumentiert werden.
- Soweit der Auftragnehmer Dienstleistungen Dritter in Anspruch nimmt, durch die datenschutzrechtliche Belange berührt sein können (z. B. Software-Wartung), sollte die Beachtung der für den Auftraggeber geltenden datenschutzrechtlichen Bestimmungen vertraglich sichergestellt sein.

Die Empfehlungen des Landesbeauftragten für den Datenschutz wurden bei der Neufassung des Vertrages berücksichtigt.

Im einem weiteren Fall (vgl. Tz. 10.3.4) erfolgte keine Datenverarbeitung im eigentlichen Sinne, es wurden lediglich die Aufgaben der Systemverwaltung und Benutzerbetreuung auf eine Privatfirma übertragen. Die Tätigkeit des Systemverwalters unterliegt aus datenschutzrechtlicher Sicht besonderen Anforderungen an die Vertrauenswürdigkeit, da er in der Regel Zugriff auf alle Anwender- und System- und Protokolldaten, Paßworte und kryptografische Schlüssel besitzt. Den erforderlichen vertraglichen Vereinbarungen und Verpflichtungen (vgl. § 4 LDatG) kommt dabei besondere Bedeutung zu. Gerade bei der Verarbeitung besonders sensibler Daten sollten die Aufgaben der Systemverwaltung nicht von privaten Dritten wahrgenommen

werden. Es ist aus der Sicht des Datenschutzes nicht hinnehmbar, daß beispielsweise aufgrund offener Fragen bei der Vertragsverlängerung Probleme hinsichtlich der Wahrnehmung der Systemverwalteraufgaben entstehen.

Der Landesbeauftragte hat daher die oberste Aufsichtsbehörde gebeten zu prüfen, inwieweit eine Systemverwaltung durch eigene Mitarbeiter erfolgen kann.

22 Sonstige Tätigkeitsbereiche

22.1 Mitteilungspflichten nach dem Betäubungsmittelgesetz (BtMG)

Von einer Therapieeinrichtung wurde an den LfD die Frage gerichtet, ob und ggf. unter welchen Voraussetzungen Informationen über einen Therapieabbruch oder über den Nichtantritt eines Verurteilten zur Behandlung an Justizbehörden übermittelt werden dürfen. Ein Kostenträger hatte gegenüber der Einrichtung die Auffassung vertreten, die Vorschriften zum Schutze des Sozialgeheimnisses ließen eine Informationsübermittlung nur mit Einwilligung der Betroffenen zu.

Der LfD wies darauf hin, daß die Therapieeinrichtung nicht Leistungsträger im Sinne des Sozialgesetzbuchs (SGB) und damit auch nicht unmittelbar Normadressat der Vorschriften zum Schutze des Sozialgeheimnisses ist. Die Tatsache, daß der Kostenträger zugleich Sozialleistungsträger ist, rechtfertigt keine andere Beurteilung.

Zu berücksichtigen ist indessen, daß die von dem Leistungsträger offenbarten Daten nach § 78 SGB X der Zweckbindung unterliegen und von den Personen oder Stellen, denen sie offenbart wurden, in demselben Umfang geheimzuhalten sind wie von dem Leistungsträger selbst. Aus der zitierten Vorschrift erwächst für die Therapieeinrichtung also die Verpflichtung, die vom Kostenträger mitgeteilten Daten nur beim Vorliegen der Voraussetzungen der §§ 67 ff. SGB X zu offenbaren.

Daten über Patienten werden indessen nicht nur vom Kostenträger, sondern auch von anderen Stellen übermittelt – z. B. bei einer Zurückstellung der Strafvollstreckung durch Justizbehörden nach § 35 BtMG –. Außerdem werden Daten bei Behandlungsbeginn und im Rahmen der Behandlung beim Patienten unmittelbar erhoben. Solche Daten, zu denen auch die unmittelbar erlangte Kenntnis des Behandlungsabbruchs gehört, unterliegen nicht dem Sozialgeheimnis, weil die Therapieeinrichtung nicht Leistungsträger ist und die Daten auch nicht im Sinne des § 78 SGB X von einem Leistungsträger offenbart werden.

Dies bedeutet selbstverständlich nicht, daß diese Daten ungeschützt sind. Sie unterliegen dem Arztgeheimnis (§ 2 der Berufsordnung für Ärzte, 203 Abs. 1 StGB); außerdem sind allgemeine Datenschutzvorschriften (im wesentlichen das Bundesdatenschutzgesetz) und bereichsspezifische Datenschutzvorschriften (Landeskrankenhausgesetz – LKG –) anzuwenden. § 36 Abs. 3 Nr. 1 LKG, der die allgemeinen Übermittlungsregelungen des Bundesdatenschutzgesetzes verdrängt, läßt eine Übermittlung von Patientendaten an Personen und Stellen außerhalb des Krankenhauses – also auch an Justizbehörden – zu, soweit sie zur Erfüllung einer gesetzlich vorgeschriebenen Mitteilungspflicht erforderlich ist. § 35 Abs. 3 zweiter Halbsatz BtMG begründet für die Therapieeinrichtung eine derartige Mitteilungspflicht; die Unterrichtung der Justizbehörden über den Behandlungsabbruch ist also zulässig.

Eine gesetzliche Mitteilungspflicht bezüglich des Nichtantritts einer Behandlung existiert hingegen nicht. Die Erbringung eines Nachweises über den Behandlungsantritt gehört nach § 35 Abs. 3 erster Halbsatz BtMG zu den Obliegenheiten des Verurteilten.

Eine Anfrage des Ministeriums für Arbeit, Soziales, Familie und Gesundheit betraf die Frage, ob auch aus § 36 Abs. 5 eine Offenbarungsbefugnis in solchen Fällen hergeleitet werden kann, in denen aufgrund gerichtlicher Entscheidung die Vollstreckung zurückgestellt und die in der Einrichtung verbrachte Zeit dem verurteilten Abhängigen auf die Strafe angerechnet werden soll. Nach der zitierten Vorschrift sind die Vollstreckungsbehörde, der Verurteilte und die behandelnden Personen oder Einrichtungen zu hören.

Zwar ist der Vorschrift eine Offenbarungsbefugnis nicht gleichermaßen deutlich zu entnehmen wie § 35 Abs. 3 zweiter Halbsatz BtMG. Sinn und Zweck der Vorschrift lassen aber dennoch den gesetzgeberischen Willen erkennen, daß im Rahmen der Anhörung eine Einschätzung des künftigen Verhaltens vorgetragen wird. Auch Angaben über Therapiedauer sowie eine knappe Schilderung des Therapieverlaufs und der erreichten Verhaltensänderung werden für zulässig gehalten.

22.2 Heimaufsicht

Sowohl die Datenschutzkommission wie auch der LfD hatten sich schon wiederholt mit der Frage zu befassen, welche Ermittlungsbefugnisse der Heimaufsicht zustehen (vgl. 11. Tb. Tz. 12.8; 13. Tb. Tz. 11.4). Nach § 9 Abs. 1 Heimgesetz (HeimG) haben der Träger und der Leiter eines Heims der zuständigen Heimaufsichtsbehörde die für die Durchführung des Heimgesetzes und

der aufgrund dieses Gesetzes erlassenen Rechtsverordnungen erforderlichen mündlichen und schriftlichen Auskünfte innerhalb der gesetzten Frist und unentgeltlich zu erteilen. Nach einer Entscheidung des OVG Koblenz vom 6. Dezember 1988 – 7 A 14/88 – muß für das Auskunftsverlangen nach § 9 Abs. 1 HeimG ein konkreter Anlaß vorhanden sein, der ein Einschreiten der Heimaufsichtsbehörde als möglich erscheinen läßt. An das Vorliegen eines derartigen Anlasses dürfen aber keine hohen Anforderungen gestellt werden.

Vor diesem Hintergrund äußerte sich der LfD zur Anfrage einer Heimbetriebsgesellschaft, ob die Heimaufsichtsbehörde befugt ist, eine Mitgliederliste des Mehrheitsgesellschafters – eines eingetragenen Vereins – und Auskunft darüber zu verlangen, welche Vereinsmitglieder dem Verein Kapital zur Finanzierung seiner Gesellschaftsanteile zur Verfügung gestellt haben. Der LfD vertrat die Auffassung, daß das Auskunftsverlangen nach § 9 Abs. 1 HeimG in vollem Umfange gerechtfertigt und die Auskünfte demnach zu erteilen sind. Zur Schutzbedürftigkeit der begehrten Informationen war anzumerken, daß im Grundsatz keine besondere Geheimhaltungsbedürftigkeit besteht; zum Teil sind sie sogar öffentlich zugänglich. Die Namen der Gründungsmitglieder eines Vereins ergeben sich aus den Unterschriften unter der Gründungssatzung, die bei den Vereinsakten im Amtsgericht für jedermann zur Einsicht vorliegt (§ 79 BGB). Das Amtsgericht kann auch jederzeit ohne besondere Begründung die Zahl der Vereinsmitglieder verlangen (§ 72), die dann ebenfalls jedermann zur Einsicht offenliegt.

Bezüglich der Informationen über die zur Verfügung gestellten Kapitalien durch Vereinsmitglieder an den Verein war zu berücksichtigen, daß nur ein nichtwirtschaftlicher Verein in das Vereinsregister eintragungsfähig ist. Ein Verein, dessen Zweck auf einen wirtschaftlichen Geschäftsbetrieb gerichtet ist, ist nicht eintragungsfähig und erlangt somit keine Rechtsfähigkeit. Wenn ein eingetragener Verein wirtschaftlicher Träger einer Heimbetriebsgesellschaft ist, so ist nicht auszuschließen, daß dieser Verein keine Rechtspersönlichkeit besitzt und daß seine Mitglieder unmittelbar haften oder auch im Rahmen der Beteiligung an der Heimbetriebsgesellschaft unmittelbar berechtigt und verpflichtet sind. Vor diesem Hintergrund war das Verlangen nach der Offenbarung sowohl der Namen der Mitglieder wie der wirtschaftlichen Verhältnisse des Vereins für die Heimaufsicht i. S. des § 9 Abs. 1 HeimG erforderlich und zulässig.

22.3 Liegenschaftskataster

Mit dem Inkrafttreten der Katasterverordnung am 16. Oktober 1992 wurden die Bemühungen um Schaffung bereichsspezifischer Datenschutzregelungen für das Katasterwesen (vgl. 12. Tb. Tz. 17.2; 13. Tb. Tz. 15.3) vorläufig abgeschlossen. Wie zuvor schon beim Katastergesetz hat das Ministerium des Innern und für Sport auch bei der Bearbeitung der Rechtsverordnung die Beratung des LfD in Anspruch genommen und eine erfreuliche Aufgeschlossenheit für die Belange des Datenschutzes gezeigt. Die Verordnung enthält detaillierte Bestimmungen zum Inhalt des Liegenschaftskatasters sowie Bestimmungen über die regelmäßige Übermittlung von Daten aus dem Liegenschaftsbuch unter besonderer Berücksichtigung der automatisierten Datenverarbeitung. Die Aufzählung der Eigenschaften, die im Liegenschaftsbuch nachzuweisen sind (§ 3), darf nicht in dem Sinne verstanden werden, daß hierdurch Übermittlungsbefugnisse für die Behörden und Stellen begründet werden, die die Daten zur Erfüllung ihrer Aufgaben erhoben haben. Soweit derartige Übermittlungsbefugnisse noch nicht existieren, müssen sie im Interesse der Normenklarheit geschaffen werden (entsprechend der Regelung für die Übermittlung von Hinweisen auf Altlasten in § 27 Abs. 4 LAbfWAG).

22.4 Entwicklung des Datenschutzregisters

Das Datenschutzregister wurde bis zum Jahre 1985 im Auftrag der DSK durch das Landesrechenzentrum (LRZ) geführt. Die Anmeldungen wurden nach Prüfung durch die Geschäftsstelle der Datenschutzkommission zur Erfassung und weiteren Verarbeitung an das LRZ weitergeleitet. Da ein Direktzugriff auf das Register nicht möglich war, wurden Auswertungen nur auf schriftliche Anforderung durch das LRZ erstellt. Weil dieses Verfahren sehr zeit- und kostenaufwendig war, wurde es eingestellt. Um indessen der gesetzlichen Verpflichtung weiterhin zu genügen, erstellten Mitarbeiter der Datenschutzkommission eine Software, die die automatisierte Führung des Datenschutzregisters auf einem Personalcomputer ermöglichte. Im Jahr 1992 wurde dieses Verfahren auf das in der Behörde des LfD eingesetzte Bürokommunikationssystem übernommen mit der Folge, daß jetzt jeder Referent unmittelbar an seinem Arbeitsplatz die Möglichkeit hat, auf das Datenschutzregister im Online-Verfahren zuzugreifen und es nach beliebigen Kriterien auszuwerten. Die bestehenden Recherchemöglichkeiten werden vorwiegend genutzt, um örtliche Prüfungen vorzubereiten. Ferner werden Auszüge erstellt und zur Aktualisierung an die betroffenen Behörden versandt. Ebenso kann aufgrund der Meldungen zum Datenschutzregister die Weiterentwicklung der Automatisierung beobachtet werden. In der Vergangenheit gaben Anmeldungen zum Datenschutzregister häufig Veranlassung, örtliche Feststellungen durchzuführen und datenschutzrechtliche Verbesserungen anzuregen.

Die Bedeutung des Datenschutzregisters für die Datenschutzkontrolle wird auch aus der zahlenmäßigen Entwicklung der Anmeldungen erkennbar. Bei der Umstellung im Jahre 1986 waren im Datenschutzregister ca. 3 200 Anwendungen gespeichert, heute sind es bereits 4 800. Insbesondere sind in der ersten Hälfte des Jahres 1993 viele Anmeldungen von Schulen eingegangen, die aufgrund von Hinweisen in einer speziellen Informationsschrift für die Schulen – Heft 6 Datenschutz in der Schule – (vgl. Tz. 8.1.6) erst auf die bestehende Anmeldepflicht aufmerksam wurden.

Für 1993 liegen zur Zeit ca. 170 Anmeldungen vor. Im Durchschnitt werden ca. 200 Verfahren pro Jahr neu angemeldet.

Nähere Überprüfungen vor Ort ergeben immer wieder, daß speichernde Stellen ihrer Anmeldepflicht zum Datenschutzregister nicht in der gesetzlich vorgeschriebenen Weise nachkommen.

Der LfD ist stetig bemüht, den mit dem Anmeldeverfahren verbundenen Verwaltungsaufwand so gering wie möglich zu halten. So wurde beispielsweise zugelassen, daß für zentral entwickelte Verfahren verkürzte Anmeldungen vorgelegt werden. Die Novellierung des Landesdatenschutzgesetzes soll genutzt werden, die Verfahrensregelungen für Anmeldungen zum Datenschutzregister weiter zu vereinfachen.

Auswertungen des Datenschutzregisters (vgl. Anlage 12) zeigen, in welchen Anwendungsgebieten vermehrt Informationstechnik eingesetzt wird und wie sich die Zahl der Anwendungen in repräsentativen Bereichen entwickelt hat.

22.5 Koordinierungstätigkeiten

Der LfD hat an den regelmäßigen Sitzungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder teilgenommen. Dieses Gremium ist durch die Erweiterung um die Datenschutzbeauftragten der jungen Bundesländer nicht nur größer geworden, es hat einen erheblichen Zugewinn an Erfahrungen und neuen Gesichtspunkten erhalten. Die Abstimmung ist allerdings nicht leichter geworden, was sich auch in der bescheidenen Zahl von Beschlüssen niederschlägt.

Die Arbeitskreise der Konferenz bilden nach wie vor ein bedeutsames Instrument des Erfahrungsaustauschs und der Meinungsbildung.

Auf der Ebene des Landes hat der LfD erstmals ein Treffen der datenschutzrechtlichen Koordinationsreferenten der Ressorts organisiert. Neben allgemeinen Fragen des Datenschutzes (insbesondere auch zur Personaldatenverarbeitung) wurde die Funktion der Koordinationsreferenten angesprochen. Nicht in jedem Haus haben diese auch die Aufgabe des hausinternen Datenschutzbeauftragten. Dies wäre aus der Sicht des LfD allerdings grundsätzlich zu begrüßen. Der LfD hat auch auf die Aufgabe dieser Referenten hingewiesen, ihn rechtzeitig und möglichst umfassend auf anstehende Normsetzungsverfahren hinzuweisen. Probleme gab es hier insbesondere, wenn Verwaltungsvorschriften Vorgänge regeln, die zwar Datenschutzrelevanz besitzen, in denen es also um die Erhebung, Speicherung und Übermittlung personenbezogener Informationen geht, in denen aber die automatisierte Datenverarbeitung nicht angesprochen wird. Hier ist – insbesondere bei dem einen oder anderen im Jahr 1991 neu errichteten oder neu zugeschnittenen Ressort – der Datenschutzbezug nicht immer gesehen worden.

Schwierigkeiten haben sich auch im Zusammenhang mit EG-Regelungen ergeben. Nach Kenntnis des LfD werden hier die Landesregierungen durchaus frühzeitig durch die EG unterrichtet. Von den einzelnen Fachreferaten ist der Weg zum Landesbeauftragten über den Koordinierungsreferenten aber wohl häufig zu lang, er wird nur selten beschritten.

23 Schlußbemerkung

In der Schlußbemerkung möchte der LfD an die Beratung des 13. Tätigkeitsberichts in der Sitzung des Landtags am 11. Dezember 1992 anknüpfen. In einem Diskussionsbeitrag wurde darauf hingewiesen, daß der Datenschutzbeauftragte seine Position als „Partei für den Datenschutz" verkenne, wenn er in weichen und diplomatischen Formulierungen einerseits die Interessen des Datenschutzes und andererseits die Verwaltungsinteressen darstelle und abwäge. Wer sich näher mit Datenschutzrecht befaßt, weiß, daß diese Abwägung auch unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes in fast jedem zu bearbeitenden Einzelfall gefordert ist, da schutzwürdige Belange der Betroffenen einerseits und berechtigte Informationsinteressen der Verwaltung andererseits gegeneinander stehen. In diesem Spannungsfeld vollzieht sich die Arbeit des Datenschutzes. Eine einseitige Betonung des Rechts auf informationelle Selbstbestimmung führt nicht zu seiner Stärkung; in Konfliktfällen kann sie bewirken, daß der Datenschutz nicht mehr ernst genommen wird.

Im übrigen hat die intensive Beratung des Tätigkeitsberichts durch den Landtag die Stellung des LfD bei der Wahrnehmung von Kontrollaufgaben unterstützt und seine Bemühungen gefördert, die Öffentlichkeit über die Ergebnisse der Datenschutzarbeit zu informieren. Daß dies nach wie vor notwendig ist, zeigen viele Eingaben, in denen um Rat gebeten und nach staatlichen Maßnahmen zur Gewährleistung des Rechts auf informationelle Selbstbestimmung gefragt wird. Vorwiegend aus aktuellem Anlaß gab der LfD eine Reihe von Presse- und Rundfunkinterviews; in einigen Fällen wurden die Medien durch besondere Erklärungen über wichtige Datenschutzfragen informiert.

Die Bemühungen des LfD um eine personelle Verstärkung seiner Behörde waren leider nur zum Teil erfolgreich. Ansonsten sind die Arbeitsbedingungen als gut zu bezeichnen; die für Sachausgaben zur Verfügung stehenden Haushaltsmittel sind knapp, aber ausreichend bemessen.

Bewährt hat sich die Zusammenarbeit mit der Verwaltung des Landtags in allen Angelegenheiten, die sich auf den inneren Dienstbetrieb beziehen. Diese Zusammenarbeit ermöglicht, die knappen Mittel in der Dienststelle des LfD in vollem Umfange auf die Datenschutzarbeit zu konzentrieren.

Anlage 1

Entschließung
der 43. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 23./24. März 1992
zum
Arbeitnehmerdatenschutz

I.

Im Rahmen des Arbeitsverhältnisses werden personenbezogene Daten aus ganz unterschiedlichen Lebensbereichen des Arbeitnehmers erhoben und gespeichert. Diese Daten verwendet der Arbeitgeber nicht nur für eigene Zwecke. Aus dem Arbeitsverhältnis ergeben sich auch Auskunfts-, Bescheinigungs- und Meldepflichten, die der Arbeitgeber gegenüber öffentlichen Stellen zu erfüllen hat. Durch die Möglichkeit, im Arbeitsverhältnis anfallende personenbezogene Daten miteinander zu verknüpfen und sie – losgelöst vom Erhebungszweck – für andere Verwendungen zu nutzen, entstehen Gefahren für das Persönlichkeitsrecht des Arbeitnehmers. Mit der Intensität der Datenverarbeitung, insbesondere durch Personalinformationssysteme und digitale Telekommunikationsanlagen, nehmen die Kontroll- und Überwachungsmöglichkeiten des Arbeitgebers zu.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb bereits seit 1984 bereichsspezifische und präzise gesetzliche Bestimmungen zum Arbeitnehmerdatenschutz. Bundestag, Bundesrat und Bundesregierung haben ebenfalls eine Regelungsnotwendigkeit bejaht; gleichwohl stehen bundesgesetzliche Regelungen über den allgemeinen Arbeitnehmerdatenschutz immer noch aus.

Die Notwendigkeit zur gesetzlichen Regelung besteht unabhängig davon, ob Arbeitnehmerdaten in automatisierten Dateien, in Akten oder in sonstigen Unterlagen verarbeitet werden. Der erhöhten Gefährdung durch die automatische Datenverarbeitung ist durch spezifische Schutzvorschriften Rechnung zu tragen.

Angesichts der besonderen Abhängigkeit des Arbeitnehmers im Arbeitsverhältnis und während der Phase einer Bewerbung um einen Arbeitsplatz ist durch Gesetz zu untersagen, daß Rechte, die dem Arbeitnehmer nach einschlägigen Datenschutzvorschriften zustehen, durch Rechtsgeschäft, Tarifvertrag und Dienst- oder Betriebsvereinbarung ausgeschlossen werden. Außerdem ist durch Gesetz festzulegen, daß eine Einwilligung des Arbeitnehmers oder Bewerbers nur dann als Grundlage einer Datenerhebung, -verarbeitung oder -nutzung in Frage kommt, wenn die Freiwilligkeit der Einwilligung sichergestellt ist, also die Einwilligung ohne Furcht vor Nachteilen verweigert werden kann. Deshalb dürfen allein aufgrund einer Einwilligung z. B. keine Gesundheitszeugnisse, Ergebnisse von Genomanalysen u. ä. angefordert werden, wenn sie den Rahmen des Fragerechts des Arbeitsgebers überschreiten.

II.

Die gesetzliche Ausgestaltung des Arbeitnehmerdatenschutzes muß insbesondere folgende Grundsätze beachten:

1. Die Datenerhebung muß grundsätzlich beim Arbeitnehmer erfolgen.

2. Der Arbeitgeber darf Daten des Arbeitnehmers – auch durch Befragen des Arbeitnehmers oder Bewerbers – nur erheben, verarbeiten oder nutzen, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Arbeitsverhältnisses erforderlich oder sonst gesetzlich vorgesehen ist. Dabei ist der Grundsatz der Zweckbindung zu beachten. Auch ist zwischen der Bewerbungs- und Einstellungsphase zu unterscheiden.

3. Der Arbeitgeber darf Daten, die er aufgrund gesetzlicher Vorgaben für andere Stellen (z. B. Sozialversicherungsträger) erheben muß, nur für diesen Zweck verwenden.

4. Eine Datenauswertung und -verknüpfung, die zur Herstellung eines umfassenden Persönlichkeitsprofils des Arbeitnehmers führen kann, ist unzulässig.

5. Beurteilungen und Personalauswahlentscheidungen dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen werden.

6. Notwendige Datenübermittlungen zwischen Arzt und dem Arbeitgeber sind eindeutig zu regeln. Dem Arbeitgeber darf grundsätzlich nur das Ergebnis der ärztlichen Untersuchung zugänglich gemacht werden. Darüber hinaus dürfen ihm – soweit erforderlich – nur tätigkeitsbezogene Risikofaktoren mitgeteilt werden. Medizinische und psychologische Befunde sind getrennt von den übrigen Personalunterlagen aufzubewahren. Die Ergebnisse medizinischer oder psycholo-

gischer Untersuchungen und Tests der Beschäftigten dürfen nur verarbeitet werden, wenn dies dem Schutz des Beschäftigten dient.

7. Dem Arbeitnehmer sind umfassende Auskunfts- und Einsichtsrechte in die Unterlagen einzuräumen, die sein Arbeitsverhältnis betreffen. Diese Rechte müssen sich auch auf Herkunft, Verarbeitungszwecke und Empfänger der Daten sowie die Art und Weise ihrer Auswertung erstrecken.

8. Dem Personal-/Betriebsrat muß ein Mitbestimmungsrecht bei der Einführung, Anwendung und der wesentlichen Änderung von automatisierten Dateien mit personenbezogenen Daten der Arbeitnehmer für Zwecke der Personalverwaltung zustehen. Das gilt auch bei sonstigen technischen Einrichtungen, mit denen das Verhalten und die Leistung der Beschäftigten überwacht werden kann.

9. Gesetzlich festzulegen ist, welche Daten der Arbeitnehmervertretung für ihre Aufgabenerfüllung zugänglich sein müssen und wie der Datenschutz bei der Verarbeitung von Arbeitnehmerdaten im Bereich der Arbeitnehmervertretung gewährleistet wird. Regelungsbedürftig ist auch das Verhältnis zwischen dem Personal-/Betriebsrat und dem behördlichen Datenschutzbeauftragten.

10. Die Befugnis des Personal-/Betriebsrats, sich unmittelbar an die Datenschutzkontrollinstanzen zu wenden, ist gesetzlich klarzustellen.

11. Arbeitnehmerdaten dürfen nur dann ins Ausland übermittelt werden, wenn dort ein dem deutschen Recht vergleichbarer Datenschutzstandard gewährleistet ist oder wenn der Betroffene nach den oben genannten Grundsätzen (vgl. Abschnitt I Abs. 4) eingewilligt hat.

Anlage 2

Entschließung
der Sonderkonferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 28. April 1992
– gegen die Stimme Bayerns in Abwesenheit Sachsens –
zur Neuregelung des Asylverfahrens
(Bundestagsdrucksache 12/2062)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält Änderungen des Gesetzentwurfs zur Neuregelung des Asylverfahrens für erforderlich, insbesondere der geplanten Regelungen

1. über die erkennungsdienstliche Behandlung von Asylbewerbern zur Sicherung der Identität (§ 16 Abs. 1) und
2. über die Nutzung der dabei gewonnenen erkennungsdienstlichen Unterlagen zur Strafverfolgung und zur Gefahrenabwehr (§ 16 Abs. 5).

Zu 1.:

Nach dem geltenden Recht sind Lichtbilder und Fingerabdrücke bei Asylbewerbern nur dann zu fertigen, wenn deren Identität nicht eindeutig bekannt ist. Demgegenüber sieht der Gesetzentwurf zur Neuregelung des Asylverfahrens vor, daß von sämtlichen Asylbewerbern – bis auf wenige Ausnahmen – Lichtbilder und Fingerabdrücke zu fertigen sind. Dies ist mit dem Verfahrensgrundsatz der Verhältnismäßigkeit nicht vereinbar.

Der Staat hat selbstverständlich das Recht zu wissen, mit wem er es zu tun hat. Jeder – gleichgültig ob Deutscher oder Ausländer – muß sich deshalb durch Dokumente ausweisen können; nur wenn Zweifel an der Identität bestehen, kommen erkennungsdienstliche Maßnahmen in Betracht. Dieser Grundsatz unserer Rechtsordnung muß auch im Rahmen der Neuregelung des Asylverfahrens beachtet werden. Nur wenn feststeht, daß die Identität eines hohen Anteils der Asylbewerber – also nicht bloß einzelner oder bestimmter Gruppen – zweifelhaft ist, wäre eine erkennungsdienstliche Behandlung aller Asylbewerber gerechtfertigt. Gerade dies aber ist bisher nicht hinreichend belegt: In der amtlichen Begründung des Gesetzentwurfs ist allein davon die Rede, daß nach Feststellung niederländischer Behörden 20 % der Asylbewerber unter falschem Namen einen weiteren Asylantrag stellen. Aussagekräftige Angaben, in welchem Umfang in der Bundesrepublik Deutschland Asylbewerber unter Täuschung über ihre Identität gleich bei der ersten Antragstellung oder nach dessen Ablehnung erneut versuchen, Asyl zu erhalten, fehlen bislang.

Zu 2.:

Bei der zentralen Auswertung der Fingerabdrücke von Asylbewerbern durch das Bundeskriminalamt muß – ungeachtet dessen, ob das Bundeskriminalamt dabei in eigener Zuständigkeit oder für das Bundesamt für die Anerkennung ausländischer Flüchtlinge tätig wird – unbedingt folgendes sichergestellt sein:

- Fingerabdrücke von Asylbwerbern, die unter Beachtung des zur Nr. 1 Gesagten gefertigt wurden, dürfen nur gespeichert werden, soweit dies zur Sicherung der Identität unbedingt erforderlich ist. Dazu reicht die bisher vom Bundeskriminalamt angewandte Methode der sogenannten Kurzsatzverformelung der Fingerabdrücke aus. Gerade aber dabei soll es nicht bleiben: Mit der bevorstehenden Einführung der AFIS – einem neuen automatisierten Fingerabdruckverfahren – sollen künftig auch die Fingerabdrücke von Asylbewerbern, die allein zur Feststellung deren Identität gefertigt wurden, genauso erfaßt und ausgewertet werden, wie die Fingerabdrücke mutmaßlicher oder tatsächlicher Straftäter. Asylbewerber würden damit von vornherein wie Straftäter behandelt. Eine solche Verfahrensweise wird dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot, nicht gerecht. Zudem unterläuft sie die in § 16 Abs. 4 des Gesetzentwurfs vorgesehene Trennung der erkennungsdienstlichen Unterlagen von Asylbewerbern und Straftätern. Um die gebotene Differenzierung sicherzustellen, sollte – über das Trennungsgebot des § 16 Abs. 4 hinaus – die Verformelung auf den Abdruck eines Fingers des Asylbewerbers beschränkt werden, da dies zur eindeutigen Feststellung seiner Identität genügt.

- Die Datenschutzbeauftragten verkennen nicht, daß es unter Umständen im vorwiegenden Allgemeininteresse notwendig sein kann, im Rahmen asylrechtlicher Identitätsfeststellung gefertigte Fingerabdrücke für Zwecke der Stafverfolgung zu nutzen. Weil eine solche Verwendung einen neuen und zudem erheblichen Eingriff in das Grundrecht auf Datenschutz darstellt, darf sie nicht – wie es der Gesetzentwurf aber vorsieht – praktisch voraussetzungslos erfolgen. Notwendig ist vielmehr, die Voraussetzungen in einem abschließenden Straftatenkatalog aufzuführen; darin könnten auch die in der amtlichen Begründung des Gesetzentwurfs erwähnten Fälle des Sozialhilfebetrugs enthalten sein.

– Ein entsprechender Maßstab ist an die Regelung anzulegen, wann zur Indentitätssicherung gefertigte Fingerabdrücke zur polizeilichen Gefahrenabwehr genutzt werden dürfen. Eine solche Nutzung sollte nur zugelassen werden, soweit dies zur Abwehr einer gegenwärtigen erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist.

Anlage 3

Entschließung
der Sonderkonferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 28. April 1992
– gegen die Stimme Bayerns –
zum Grundrecht auf Datenschutz

1. Seit dem Volkszählungsurteil des Bundesverfassungsgerichts im Jahre 1983 ist allgemein anerkannt, daß die Grundrechte auch die Befugnis des einzelnen umfassen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu entscheiden. Die Datenschutzbeauftragten treten dafür ein, dieses Recht ausdrücklich im Grundgesetz zu verankern. Damit würde

   - für die Bürger deutlicher erkennbar, daß unsere Verfassung ihr Recht auf Datenschutz in gleicher Weise garantiert wie die traditionellen Grundrechte,
   - der wachsenden Bedeutung des Datenschutzes für das Funktionieren der freiheitlichen Demokratie Rechnung getragen und auf die negativen Erfahrungen der DDR-Geschichte reagiert,
   - der Grundrechtskatalog dem technologischen Wandel angepaßt und
   - die Konsequenz aus den positiven Erfahrungen gezogen, die in mehreren Ländern des Bundes und im Ausland mit ähnlichen Verfassungsbestimmungen gemacht wurden.

   Die Konferenz begrüßt deshalb die Vorstellungen, die in der Verfassungskommission des Bundesrates entwickelt worden sind.

   Die Datenschutzbeauftragten empfehlen der Gemeinsamen Verfassungskommission des Bundestages und Bundesrates im Zusammenhang mit Artikel 1 und Artikel 2 GG den nachfolgenden Text zur Beratung:

   „Jeder hat das Recht, über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen. Dazu gehört das Recht auf Auskunft und Einsicht in amtliche Unterlagen. Dieses Recht darf nur durch Gesetz oder aufgrund eines Gesetzes eingeschränkt werden, soweit überwiegende Interessen der Allgemeinheit es erfordern."

2. Darüber hinaus empfiehlt die Konferenz, die unabhängige Datenschutzkontrolle, die für die Verwirklichung des Grundrechts auf Datenschutz im Alltag von entscheidender Bedeutung ist, in der Verfassung zu verankern.

3. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es zusätzlich für erforderlich, in die Verfassungsdiskussion folgende Punkte mit einzubeziehen, die sich aus der Entwicklung der Informationstechnik ergeben:

   - Stärkung der Grundrechte aus Artikel 10 und 13 im Hinblick auf neue Überwachungstechniken,
   - Recht auf Zugang zu den Daten der Verwaltung (Aktenöffentlichkeit, Informationsfreiheit),
   - Instrumente zur Technikfolgenabschätzung.

Anlage 4

Entschließung der 44. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum Datenschutz bei internen Telekommunikationsanlagen

Der zunehmende Einsatz von digitalen Telekommunikationsanlagen (TK-Anlagen) in Wirtschaft und Verwaltung birgt Datenschutzrisiken in sich, denen durch eine datenschutzfreundliche Ausgestaltung der Technik und durch geeignete bereichsspezifische Regelungen entgegengewirkt werden muß. Telefongespräche stehen – auch wenn sie von einem Dienstapparat aus geführt werden – unter dem Schutz des Grundgesetzes.

Dies hat das Bundesverfassungsgericht in seiner neueren Rechtsprechung hervorgehoben.

Der Schutz des Fernmeldegeheimnisses und des nichtöffentlich gesprochenen Wortes ist gerade bei Arbeitnehmern bedeutsam, da diese sich in einem besonderen Abhängigkeitsverhältnis befinden; aber auch das informationelle Selbstbestimmungsrecht Dritter, die anrufen oder angerufen werden, muß gewahrt werden.

Entsprechende bundesrechtliche Regelungen für interne TK-Anlagen sind überfällig, da in diesen Anlagen – insbesondere wenn sie digital an das öffentliche ISDN angeschlossen sind – umfangreiche Sammlungen sensibler personenbezogener Daten entstehen können, die sich auch zur Verhaltens- und Leistungskontrolle eignen und zudem Hinweise auf das Kommunikationsverhalten aller Gesprächsteilnehmer geben. Die Regelungen sollten verbindliche Vorgaben für die technische Ausgestaltung von TK-Anlagen geben und den Umfang der zulässigen Datenverarbeitung festlegen:

- Es muß technisch möglich sein, daß Anrufer und Angerufene die Rufnummernanzeige fallweise abschalten können.
- Die automatische Speicherung der Rufnummern von externen Anrufern nach Beendigung des Telefongesprächs ist auszuschließen, soweit hierfür keine sachliche Notwendigkeit besteht.
- Die Weiterleitung eines Anrufs an einen anderen als den gewählten Anschluß sollte dem Anrufer so rechtzeitig signalisiert werden, daß dieser den Verbindungsaufbau abbrechen kann.
- Das Mithören und Mitsprechen weiterer Personen bei bestehenden Verbindungen sollte nur nach eindeutiger und rechtzeitiger Ankündigung möglich sein.
- Verbindungsdaten, einschließlich der angerufenen Telefonnummern, sollten nach Beendigung der Gespräche nur insoweit gespeichert werden, als dies für Abrechnungszwecke und zulässige Kontrollzwecke erforderlich ist. Die Nummern der Gesprächspartner von Arbeitnehmervertretungen, internen Beratungseinrichtungen und sonstigen auf Vertraulichkeit angewiesenen Stellen dürfen nicht registriert werden.
- Die TK-Anlagen müssen durch geeignete technische Maßnahmen gegen unberechtigte Veränderungen der Systemkonfiguration und unberechtigte Zugriffe auf Verbindungs- und Inhaltsdaten geschützt werden. Da TK-Anlagen geeignet sind, das Verhalten und die Leistung der Arbeitnehmer zu kontrollieren, und sie überdies häufig die Arbeitsplatzgestaltung beeinflussen, löst ihre Einführung in Betrieben und Behörden Mitbestimmungsrechte der Betriebsräte und überwiegend auch der Personalräte aus. Sie dürfen daher nur betrieben werden, wenn unter Beteiligung der Arbeitnehmervertretungen verbindlich festgelegt wurde, welche Leistungsmerkmale aktiviert und unter welchen Bedingungen sie genutzt werden, welche Daten gespeichert, wie und von wem sie ausgewertet werden. Die Nutzer der TK-Anlage sind über den Umfang der Datenverarbeitung umfassend zu unterrichten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, daß umgehend datenschutzrechtliche Regelungen für den Einsatz und die Nutzung von internen TK-Anlagen mit einer bereichsspezifischen Rechtsgrundlage für die Verarbeitung von Arbeitnehmerdaten geschaffen werden.

Anlage 5

Entschließung
der 44. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 1./2. Oktober 1992
zum Entwurf eines Gesetzes zur
Sicherung und Strukturverbesserung der gesetzlichen Krankenversicherung
– Gesundheits-Strukturgesetz 1993 –
(Bundesratsdrucksache 560/92)

Die Bundesregierung will mit dem Gesundheits-Strukturgesetz dem Kostenanstieg in der gesetzlichen Krankenversicherung entgegenwirken. Dieses begrüßenswerte Ziel soll nach dem vorgelegten Gesetzentwurf u. a. auch durch eine verstärkte automatische Datenverarbeitung erreicht werden. Die damit verbundenen Eingriffe in die Persönlichkeitsrechte der Versicherten und in die sie schützende ärztliche Schweigepflicht müssen auf das unbedingt Notwendige beschränkt werden. Die Datenschutzkonferenz hält vor allem folgende Verbesserungen für notwendig:

- Der Gesetzentwurf sieht vor, daß die Krankenhäuser den Krankenkassen mehr Versichertendaten zur Verfügung stellen müssen als bisher. Es sollte deshalb eingehend geprüft werden, ob die Krankenkassen tatsächlich alle geforderten Angaben benötigen; die Aufgabenteilung zwischen Krankenkassen und Medizinischem Dienst muß aufrechterhalten bleiben.

- Für das Modellvorhaben zur Überprüfung des Krankenhausaufenthaltes müssen die Erhebung, Verwendung und Löschung von Versichertendaten durch den Medizinischen Dienst präziser als bisher vorgesehen geregelt werden.

- Beim Einzug der Vergütung der Krankenhausärzte für Wahlleistungen durch Krankenhäuser sollte die Einschaltung privater Abrechnungsstellen ohne Einwilligung der Patienten nicht zugelassen werden, da dabei Abrechnungsdaten an Dritte offenbart werden. Die Daten sind gegen unbefugte Offenbarung und Beschlagnahme rechtlich besser geschützt, wenn sie – auch zur Abrechnung – im Krankenhaus verbleiben. Die Krankenhäuser sind zudem in der Lage, die Vergütung einzuziehen.

- Für die neu vorgesehenen Patienten-Erhebungsbogen zur Ermittlung des Bedarfs an Pflegepersonal im Krankenhaus sollte eine strikte Zweckbindung sowie eine frühestmögliche Löschungs- oder Anonymisierungspflicht festgelegt werden. Eine Überlassung der Patienten-Erhebungsbogen in der im Gesetzentwurf vorgesehenen Fassung an die Krankenkassen ist abzulehnen.

Anlage 6

Entschließung
der 44. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zur Krankenversichertenkarte als Chipkarte

Die Konferenz der Datenschutzbeauftragten stellt fest, daß wegen der wachsenden Automatisierung bei allen Institutionen des Gesundheitswesens und der Erweiterung des Anteils maschinenlesbarer Datenträger eine Speicherung auf einer Chipkarte als elektronische Krankenversicherungskarte auf die gesetzlich festgelegten Grunddaten beschränkt bleiben muß und nicht auf Gesundheitsdaten ausgedehnt werden darf. Eine technische Sicherung dieser Beschränkung ist zu gewährleisten.

Anlage 7

Entschließung
der 44. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 1./2. Oktober 1992
– gegen die Stimme Bayerns –
zum „Lauschangriff"

Die Datenschutzbeauftragten des Bundes und der Länder erklären:

Nachdem erst vor kurzem mit dem Gesetz zur Bekämpfung der organisierten Kriminalität die Befugnisse der Strafverfolgungsbehörden erheblich erweitert worden sind und obwohl über den Erfolg dieser Maßnahmen noch keine Erfahrungen gesammelt werden konnten, wird gegenwärtig parteiübergreifend vielfach die Forderung erhoben, der Polizei in bestimmten Fällen das heimliche Abhören und Herstellen von Bild- und Tonaufzeichnungen in und aus Wohnungen (sog. „Lauschangriff") zu ermöglichen.

1. Das Grundgesetz gewährt jedem einen unantastbaren Bereich privater Lebensgestaltung, der der Einwirkung der öffentlichen Gewalt entzogen ist. Dem einzelnen muß um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein „Innenraum" verbleiben, in dem er „sich selbst besitzt" und „in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt" (BVerfGE 27,1 ff.). Jedem muß ein privates Refugium, ein persönlicher Bereich bleiben, der obrigkeitlicher Ausforschung – insbesondere heimlicher – entzogen ist. Dies gilt gegenüber Maßnahmen der Strafverfolgung vor allem deshalb, weil davon auch unverdächtige oder unschuldige Bürger betroffen sind. Auch strafprozessuale Maßnahmen dürfen nicht den Wesensgehalt eines Grundrechts, insbesondere nicht das Menschenbild des Grundgesetzes verletzen.

2. Die Datenschutzbeauftragten nehmen die Gefahren, die das organisierte Verbrechen für die Opfer und auch für die Demokratie und den Rechtsstaat heraufbeschwört, sehr ernst. Sie sind allerdings der Meinung, daß eine angemessene Abwägung zwischen der Verfolgung der organisierten Kriminalität und dem Schutz der Persönlichkeitsrechte der Bürger geboten und möglich ist und es eine Wahrheitserforschung um jeden Preis auch künftig im Strafprozeßrecht nicht geben darf. Daraus folgt, daß der Lauschangriff auf Privatwohnungen für Zwecke der Strafverfolgung auch in Zukunft nicht erlaubt werden darf.

3. Eine andere Frage ist, ob und unter welchen Voraussetzungen der Gesetzgeber für Räume, die allgemein zugänglich sind oder beruflichen oder geschäftlichen Tätigkeiten dienen (z. B. Hinterzimmer von Gaststätten, Spielcasinos, Saunaclubs, Bordelle), einen Lauschangriff zulassen kann. Hierfür sind Mindestvoraussetzungen ein eng begrenzter abschließender Straftatenkatalog, die Verwendung der gewonnen Erkenntnisse ausschließlich zur Verfolgung dieser Straftaten, ein strikter Richtervorbehalt sowie die Wahrung besonderer Amts- und Berufsgeheimnisse.

Anlage 8

Entschließung
der 45. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 16./17. Februar 1993
zur Richtlinie des Rates vom 7. Juni 1990
über den freien Zugang zu Informationen über die Umwelt (330/313/EWG)

Im Interesse eines wirksamen Umweltschutzes hat der Ministerrat der Europäischen Gemeinschaften die Umweltinformationsrichtlinie erlassen, die jedem Bürger ein Recht auf Zugang zu den bei Behörden vorhandenen Informationen über die Umwelt gewährt. Da es nicht gelungen ist, die Richtlinie innerhalb der vorgesehenen Frist bis Ende 1992 in deutsches Recht umzusetzen, herrscht gegenwärtig Rechtsunsicherheit bei Bürgern und Behörden über den Zugang zu Umweltinformationen.

Die Konferenz der Datenschutzbeauftragten sieht in der Gewährung eines freien Zugangs zu Umweltinformationen einen wesentlichen Beitrag zu größerer Transparenz des Verwaltungshandelns. Informationsfreiheit und Datenschutz bilden dabei keinen unlösbaren Gegensatz. Die Konferenz hält es für geboten, die Arbeit am Entwurf des Umweltinformationsgesetzes (UIG) zügig zum Abschluß zu bringen. Sie begrüßt entsprechende Initiativen auf Landesebene.

In den Gesetzen sind folgende datenschutzrechtliche Grundsätze zu berücksichtigen:

Soweit Umweltinformationen auf Personen beziehbar sind, ist das Grundrecht auf informationelle Selbstbestimmung zu beachten. Deshalb sind Informationen grundsätzlich in anonymisierter oder aggregierter Form zu geben. Wenn damit das Informationsinteresse nicht erfüllt werden kann, sind Eingriffe in das Persönlichkeitsrecht nur unter klaren gesetzlichen Voraussetzungen zulässig, welche die Rechte, insbesondere die Verfahrensrechte, der Betroffenen wahren.

Anlage 9

Datenschutz bei TELEFAX

1. Sie tragen die Verantwortung für die durch Sie übermittelten personenbezogenen Daten; prüfen Sie daher genau deren Sensibilität.

2. Beachten Sie die für Ihre Behörde/Dienststelle geltenden Anweisungen für die Nutzung des Telefax-Dienstes.

3. Nutzen Sie nach Möglichkeit alle der Sicherheit dienenden Einrichtungen des Gerätes, insbesondere die Anzeige des erreichten Gerätes.

4. Vergewissern Sie sich vor einer Sendung, ob der Adressat noch unter der Ihnen bekannten Anschlußnummer erreichbar ist.

5. Verständigen Sie sich vor der Absendung besonders sensibler Daten mit dem Adressaten über den konkreten Zeitpunkt der Übermittlung.

6. Gewährleisten Sie – möglichst durch persönliche Anwesenheit am Gerät – während der Übertragung von Dokumenten mit personenbezogenen Daten, daß kein Unbefugter in diese Einsicht nehmen kann.

7. Verständigen Sie sich nach Empfang einer Sendung mit Ihrem Partner über aufgetretene Mängel und ggf. deren Behebung.

8. Erleichtern Sie sich und Ihren Partnern die Nachweisführung:
   - Vorblatt der Behörde/Dienststelle benutzen,
   - Blattnumerierung der Kopien,
   - Originale mit Verifikationsstempel versehen,
   - Journalfunktion nutzen.

9. Faxübertragungen sind „abhörbar": Was am Telefon nicht gesagt werden darf, darf auch nicht gefaxt werden.

10. Beachten Sie bei der Nutzung von Fernkopierern auf PC-Basis (z. B. Fax-Karten) auch die damit verbundenen Risiken; verständigen Sie sich darüber mit Ihrem Datenschutzbeauftragten.

Anlage 10

ISDN-Merkblatt des Landesbeauftragten für den Datenschutz

I.

Allgemeines

Der Einsatz und die Nutzung von internen Telekommunikations-Anlagen, die zunehmend ISDN-fähig sind, beeinflussen häufig die Arbeitsplatzgestaltung. Aber auch Rechte Dritter, die anrufen oder angerufen werden, können durch die Verarbeitung personenbezogener Daten in automatisierter Form betroffen sein. ISDN-Anlagen sind Computersysteme; sie werden durch Programme gesteuert. Der zur Datensicherung Verpflichtete hat daher in eigener Verantwortung diejenigen Maßnahmen gemäß § 9 LDatG zu bestimmen, die den gesetzlich geforderten Datenschutz gewährleisten. Durch die rechnergestützte Kommunikation ist eine Vielzahl von Leistungsmerkmalen realisierbar. Die neuen technischen Möglichkeiten bergen aber auch Gefahren für das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung.

II.

„Die empfindlichsten" Leistungsmerkmale im Überblick:

- Rufnummeranzeige (die vollständige Rufnummer des Anrufers wird im Display angezeigt).
  Die fehlende Anonymität kann die Vertraulichkeit voraussetzende Funktionsfähigkeit bestimmter Einrichtungen beeinträchtigen (Beratungsstellen, Personalrat, behördlicher Datenschutzbeauftragter usw.).
- Aufschalten (Teilnehmer können sich in bestehende Verbindungen einschalten).
  Es besteht das Risiko des unbemerkten Mithörens von Gesprächen.
- Anrufumleitung (ankommende Gespräche werden zu einem bestimmten Ziel umgeleitet).
  Hier können Regelungen zur innerbehördlichen Abschottung durchbrochen und vertrauliche Gesprächskontakte Dritten bekannt werden. Es besteht auch die Möglichkeit, daß sich der Anrufer plötzlich ohne sein Wissen in einer Konferenzschaltung befindet.
- Automatischer Rückruf (im Besetztfall oder während der Abwesenheit des Angerufenen kann die Rückruffunktion aktiviert werden; nach Beendigung des Gesprächs oder nach Rückkehr des Angerufenen stellt die Anlage durch automatische Wahl die Verbindung her).
  Diese Funktion kann zu einer Kette von Rückruftelefonaten gegen den Willen des erfolglos Angerufenen führen. Es besteht die Gefahr der mißbräuchlichen Kontrolle des Kommunikationsverhaltens und der unbefugten Anwesenheitskontrolle.
- Konferenzschaltung (zu einer bestehenden Verbindung werden weitere Teilnehmer hinzugeschaltet).
  Derjenige, der die Liste der Teilnehmer festlegt und die Konferenz einberuft (Konferenzleiter) kann einen „Spion" zuschalten, der dann, ohne echter Konferenzteilnehmer zu sein, in der Lage ist, den Gesprächsablauf zu verfolgen. Die Vertraulichkeit der Kommunikation ist dadurch gefährdet.

III.

Vorschläge für die datenschutzverträgliche Gestaltung von ISDN-Anlagen:

- Eine vollständige Auflistung erstellen, über welche Leistungsmerkmale jede einzelne Nebenstelle verfügt und wer für die Vergabe der Leistungsmerkmale zuständig ist.
- Hersteller über die Möglichkeit der Anlagen-Konfigurierung befragen. Bei sehr empfindlichen Leistungsmerkmalen deren Sperrung in Erwägung ziehen, wenn kein ausreichender Datenschutz realisierbar ist.
- In Dienstanweisungen festlegen, welche Leistungsmerkmale wie zu nutzen sind.
- Abschluß einer Dienstvereinbarung im Hinblick auf die Freigabe und Nutzung von Leistungsmerkmalen sowie die Gebührendatenerfassung mit einer Regelung bzgl. Dienst- und Privatgesprächen.
- Mitbestimmungsrecht des Personalrats bei Einführung und Betrieb beachten.
- Vorsicht bei Fernwartung.
  Zunächst abwägen, ob sie erforderlich und vertretbar ist. Wenn Fernwartung danach unumgänglich, die Risiken möglichst effektiv minimieren und durch Kontrollen flankieren. Also: Auftragnehmer sorgfältig auswählen. Umfang der Fernwartung vertraglich genau festlegen. Zum Beispiel Online-Zugriffe auf personenbezogene Daten ausschließen; Protokollierung der Vorgänge und übertragenen Daten.

IV.

Einschlägige Rechtsprechung mit Fundstellen

- Mithören eines Dienstgesprächs; Beschluß des BVerfG vom 19. Dezember 91, 1 BvR 382/85 in CR 1992, 498 ff.
- Telefondatenerfassung und Psychologengeheimnis; Urteil des BAG vom 13. Januar 1987, 1 AZR 267/85 in NJW 1987, 1509 ff.
- Erfassung und Speicherung von Daten dienstlicher Ferngespräche; Urteil des VGH Mannheim vom 29. Januar 1991, 4 S 1912/90 in NJW 1991, 2721 ff.

Anlage 11

Hinweise
für die Gestaltung und den Einsatz von Paßwörtern

Für den Benutzer:

1. Ihr Paßwort sollte für Sie leicht zu merken, für andere jedoch schwer zu erraten sein. Sie sollten daher keine Trivialpaßworte wie Namen, Geburtstage, Telefonnummern, Urlaubsziele usw. verwenden. Auch gängige Zeichenfolgen (123456, abcdef, 08/15, 4711, sesam) bieten keinen wirksamen Schutz. Vermeiden Sie Systematiken (sesam1, sesam2, sesam3 . . .).

2. Nutzen Sie Gestaltungsmöglichkeiten wie Zeichenmischung und Verfremdung (z. B. zerberus wird zu z§rb§r§s oder z1rb2r3s) oder die Mnemotechnik (Einmal ist keinmal! wird zu 1x=k1x!).

3. Notieren oder speichern Sie keine Paßworte!
   Ausnahme: Systemverwalter- oder selten benutzte Paßworte.
   Hinterlegen Sie diese im versiegelten Umschlag an einem sicheren Ort.

4. Geben Sie Paßworte grundsätzlich nicht an andere weiter!
   Soweit dies im Einzelfall unvermeidlich ist, ändern Sie anschließend Ihr Paßwort.

5. Ändern Sie Ihr Paßwort in angemessenen Zeitabständen, wenn Ihr System Ihnen das nicht automatisch vorgibt. Ändern Sie es nicht zu oft, aber ändern Sie es!

6. Wenn Sie mit mehreren Paßworten arbeiten (müssen), versuchen Sie, diese zu synchronisieren. Ein Paßwort im Kopf ist günstiger als drei auf Papier.

Für den Systemverwalter:

7. Versehen Sie jede Benutzerkennung mit einem Paßwort!

8. Begrenzen Sie die Gültigkeitsdauer von Paßworten; der Zeitraum sollte Abwesenheiten (Urlaub, Krankheit) abdecken, 90 Tage jedoch nicht überschreiten.

9. Paßworte sollten verschlüsselt abgelegt werden und der Zugriff soweit wie möglich beschränkt sein.

10. Nutzen Sie systemseitige Möglichkeiten, die Gestaltung von Paßworten zu beeinflussen (Nr. 1, 2). Soweit möglich, setzen Sie Stoplisten ein, um Trivialpaßworte zu verhindern.

11. Begrenzen Sie die Zahl erfolgloser Anmeldeversuche, und sperren Sie die Benutzerkennung nach Erreichen der zulässigen Anzahl.

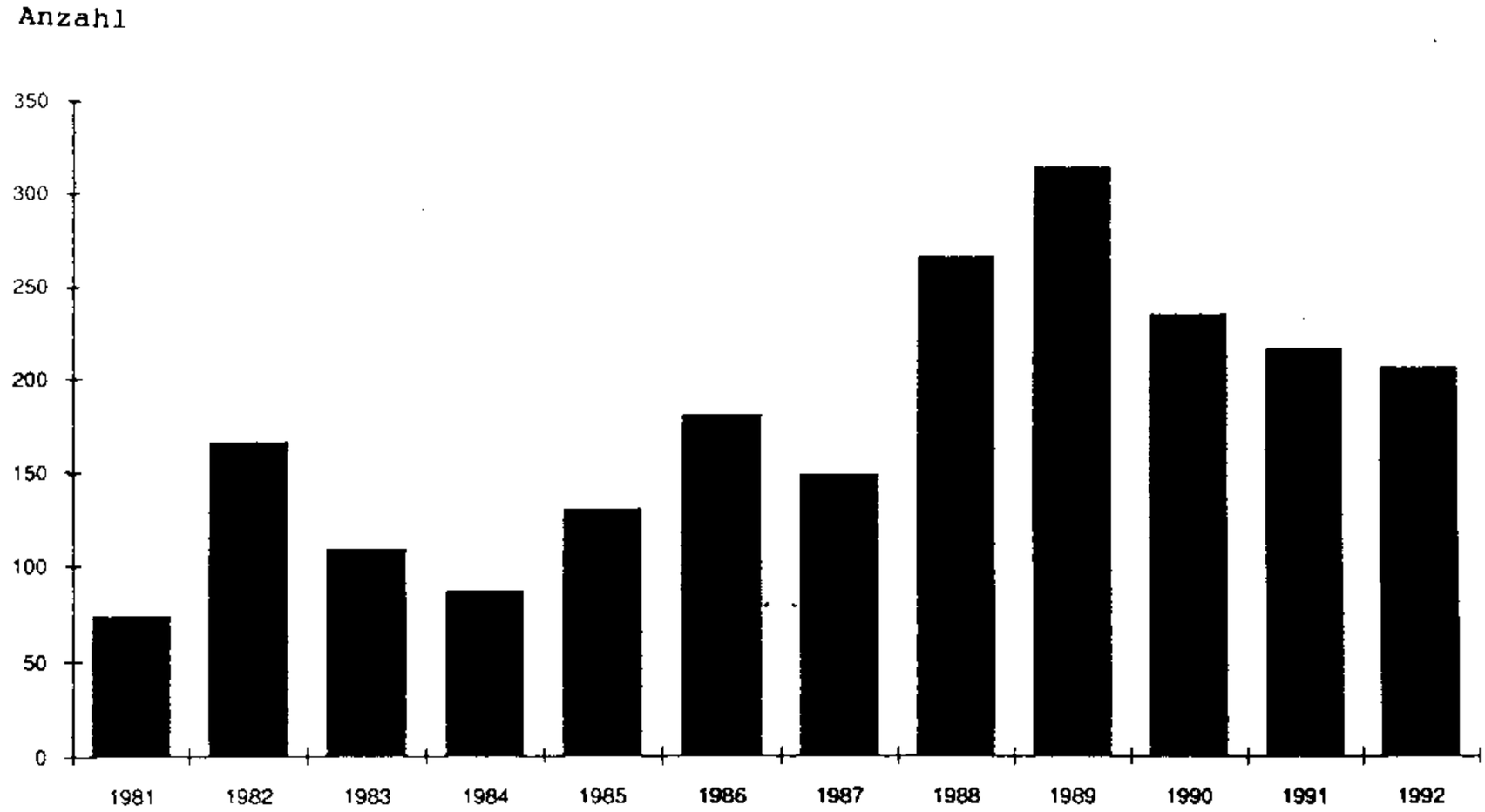
12. Richten Sie das System so ein, daß die Benutzer ihr Paßwort selbständig ändern können. Von Ihnen sollte lediglich ein Anfangspaßwort vergeben werden, das nur für die erstmalige Anmeldung gilt und anschließend geändert werden muß.

Anlage 12

Einsatz der automatisierten Datenverarbeitung in der Landes- und Kommunalverwaltung

Die folgenden Übersichten beruhen auf Auswertungen des Datenschutzregisters. Sie zeigen die Entwicklung der Anwendungszahlen bei einzelnen ausgewählten speichernden Stellen und die Verteilung von Anwendungen auf die Anwendungsgebiete.

a) Anmeldungen zum Datenschutzregister 1981 bis 1992

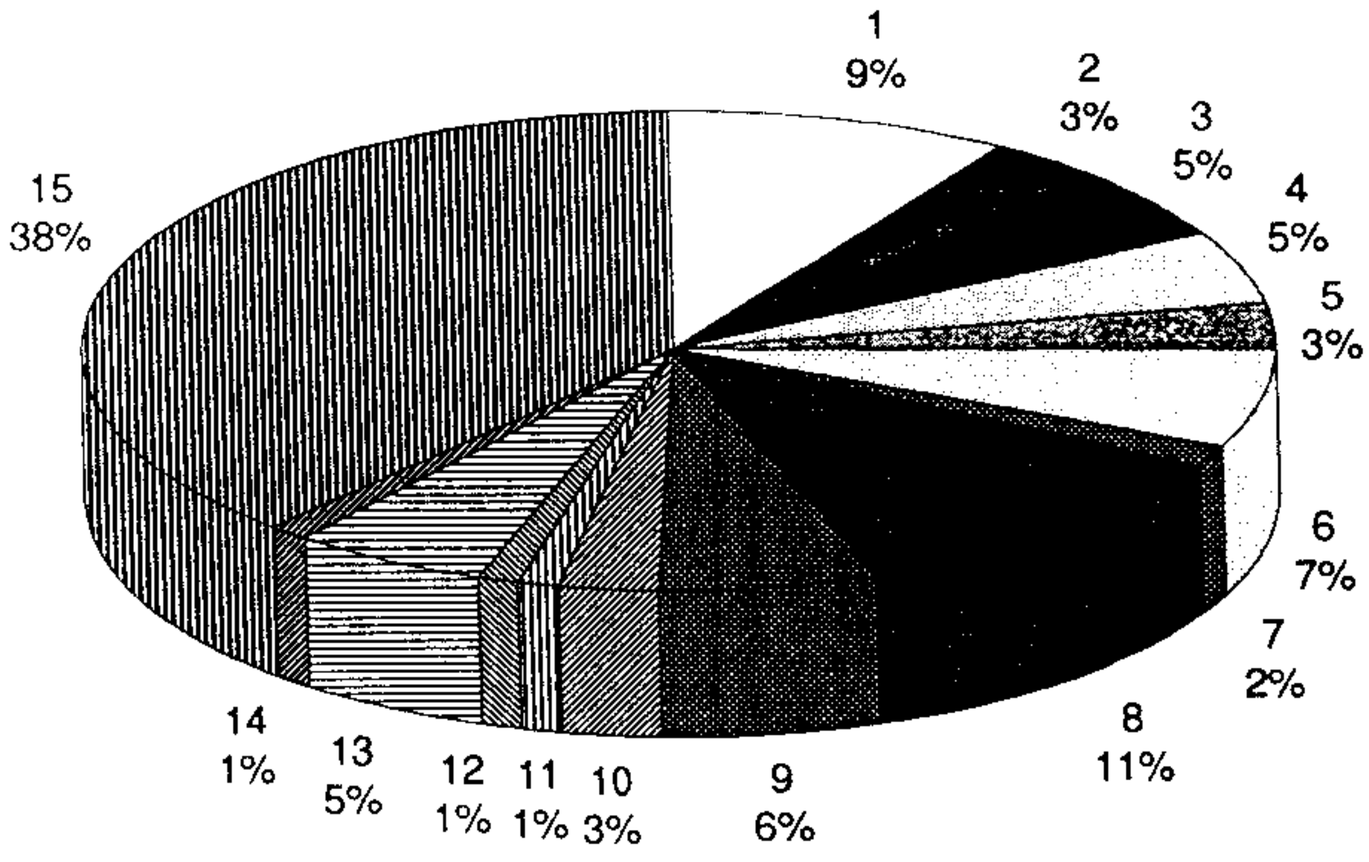


Zentral entwickelte Verfahren (z. B. Einwohnerinformationssystem, Ordnungswidrigkeitenverfahren usw.) sind nicht berücksichtigt.

b) Übersicht über die Anmeldungen zum Datenschutzregister

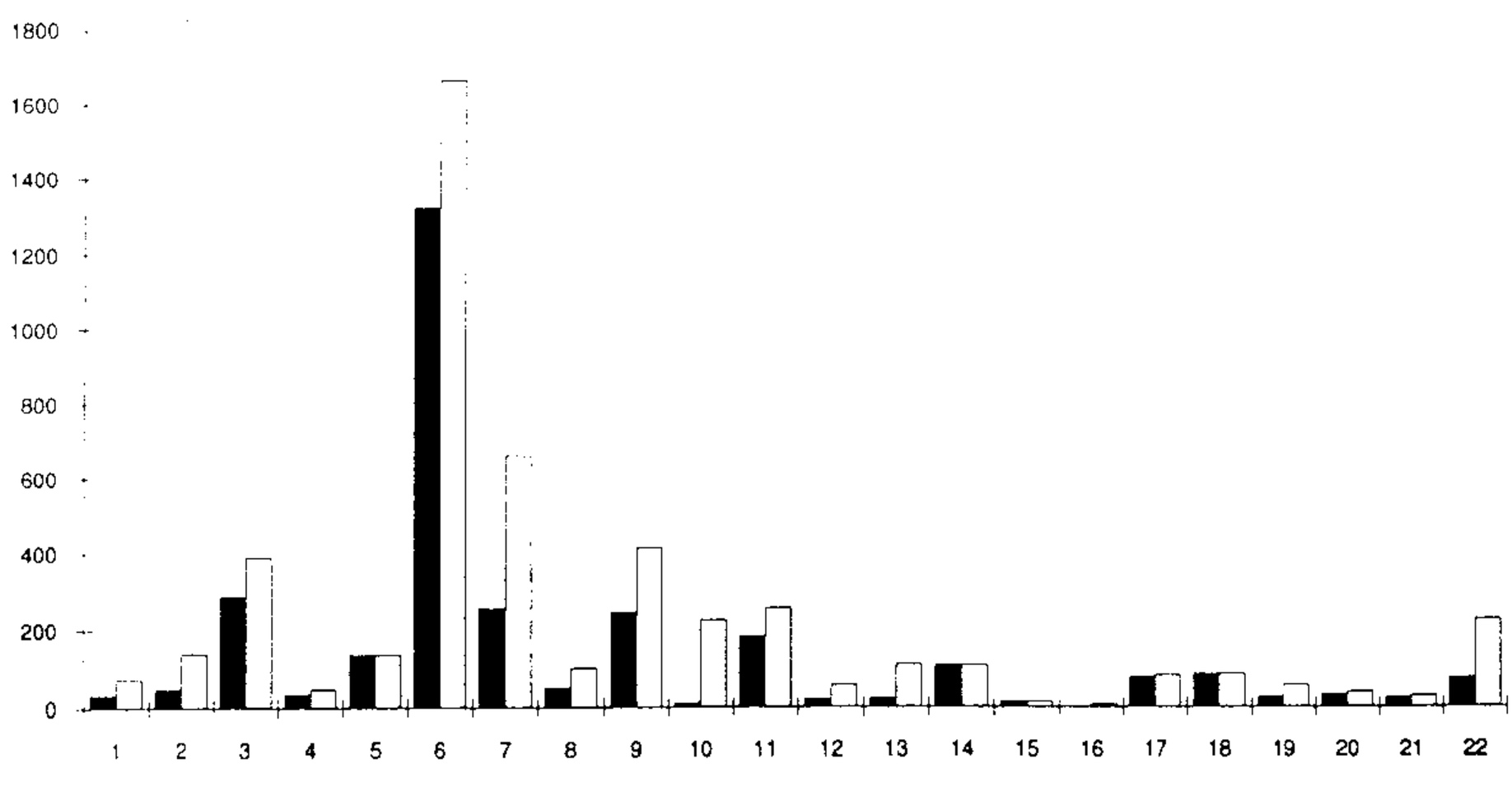
nach ausgewählten Anwendungsgebieten in %
(Gesamtzahl der Anmeldungen 4 887)

		%
1	Abgaben (Steuern, Gebühren und Beiträge)	9
2	Adreßdateien	3
3	Einwohnerwesen	5
4	Gesundheitswesen	5
5	Haushalts-, Kassen-, Rechnungswesen	3
6	Justiz (inklusiv Gerichtsvollzieher und Notare)	7
7	Landwirtschaft und Weinbau	2
8	Personaldatenverarbeitung	11
	– Besoldung und Vergütung 7	
	– Personalwesen 3	
	– Personenstandswesen 1	
9	Schulwesen	6
10	Sozialhilfe	3
11	Statistik (Bundes-, Landes-, Kommunalstatistik)	< 1
12	Umweltschutz	< 1
13	Verkehrswesen/Bußgeldverfahren	5
14	Wahlen	< 1
15	Sonstige	38

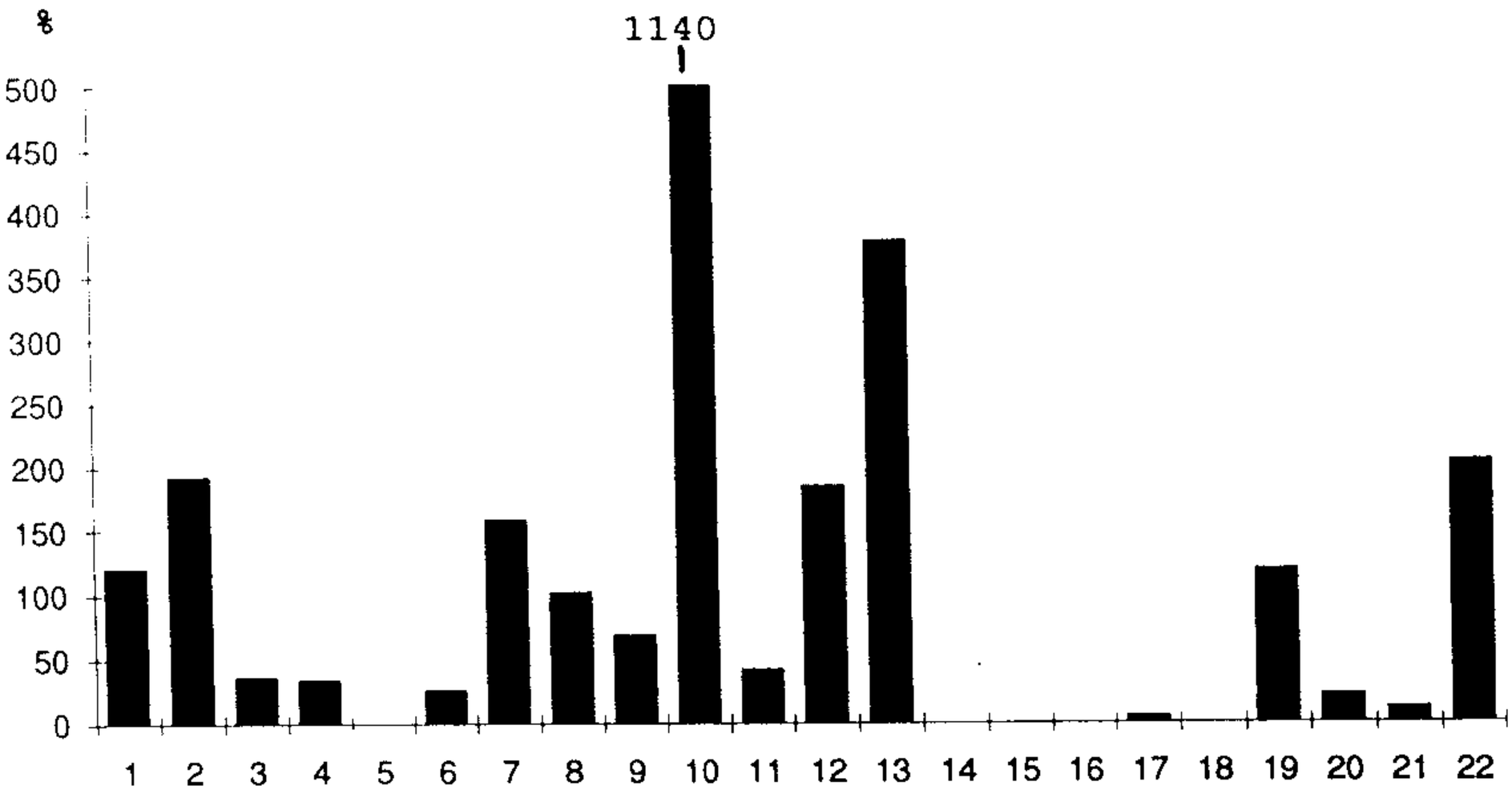


nach ausgewählten zusammengefaßten speichernden Stellen im Vergleich zu den Anmeldungen bis zum Jahr 1987

		1987	1993	Steigerung in %
1	Staatskanzlei, Landtag, Ministerien	33	73	121
2	Bezirksregierungen	47	138	193
3	Kreisverwaltungen	287	390	36
4	Polizeipräsidien, -direktionen, -ämter	35	47	34
5	Kataster- und Vermessungsämter	135	135	0
6	Städte, Gemeinde, Verbandsgemeinden	1 323	1 666	26
7	Schulen	255	660	159
8	Kreiskrankenhäuser	50	101	102
9	Krankenkassen	245	415	69
10	Oberfinanzdirektion, Finanzämter	10	224	1 140
11	Gerichte, Staatsanwaltschaften inklusive Justizvollzugsanstalten und Landesjustizkasse	180	256	42
12	Notare	20	57	185
13	Gerichtsvollzieher	23	110	378
14	Forstämter	107	107	0
15	Kulturämter	13	13	0
16	Gesundheitsämter	0	7	.
17	Landesversicherungsanstalten	77	81	5
18	Bezirksschornsteinfegermeister	86	86	0
19	Universitäten, Hochschulen	26	57	119
20	Alters- und Krankenkassen	32	39	22
21	Standesorganisationen, Berufsverbände	25	28	12
22	Sonstige	74	225	204



prozentuale Steigerung der Anmeldungen bezogen auf die Anmeldungen bis 1987



1 = Staatskanzlei, Landtag, Ministerien
2 = Bezirksregierungen
3 = Kreisverwaltungen
4 = Polizeipräsidien, -direktionen, -ämter
5 = Kataster- und Vermessungsämter
6 = Städte, Gemeinde, Verbandsgemeinden
7 = Schulen
8 = Kreiskrankenhäuser
9 = Krankenkassen
10 = Oberfinanzdirektion, Finanzämter
11 = Gerichte, Staatsanwaltschaften inklusive Justizvollzugsanstalten und Landesjustizkasse
12 = Notare
13 = Gerichtsvollzieher
14 = Forstämter
15 = Kulturämter
16 = Gesundheitsämter
17 = Landesversicherungsanstalten
18 = Bezirksschornsteinfegermeister
19 = Universitäten, Hochschulen
20 = Alters- und Krankenkassen
21 = Standesorganisationen, Berufsverbände
22 = Sonstige