

1. Vorwort

Der Jahresbericht enthält nur einen Teil des gesamten Spektrums der Tätigkeiten der Dienststelle. Viele Projekte aus den vergangenen Berichten werden noch betreut, ohne dass sie Erwähnung finden, andere sind noch nicht so weit gediehen, eine Darstellung würde noch zu rudimentär wirken. Die im Bericht aufgegriffenen Themen sind nicht nur Schwerpunktbereiche, sondern zum Teil sollen sie die Facetten und Bandbreite der Arbeit wiedergegeben. Der der Bürgerschaft und dem Senat vorzulegende Bericht enthält zugleich auch immer Elemente der Darstellung für die Bürger. Sie fordern regelmäßig nach Erscheinen den Bericht bei mir an. Die Leser sind angesichts des Berichtsumfangs wie in den vergangenen Jahren gehalten, sich das herauszusuchen, was sie interessiert und sollten die Artikel lesen, deren Themen in ihren Lebensbereichen zum Tragen kommen.

Als Trost für die berufstätigen Leser sei angemerkt, dass die eingereichten Beiträge um rund ein Drittel gekürzt oder gestrichen wurden. Gleichwohl wünschte ich mir an der einen oder anderen Stelle eine noch konzentriertere Darstellung. Zur Verbesserung beabsichtige ich in Abstimmung mit Bürgerschaft und Senat im Rahmen der gesetzlichen Bestimmungen ein neues Modell zu entwickeln.

Das vergangene Jahr ist noch von einem schwerpunktmäßigen Einsatz der Kapazitäten im öffentlichen Sektor geprägt. Diese Gewichte werden sich mit der Novellierung des BDSG in Richtung Privatwirtschaft verschieben. Der Bericht lässt erkennen, dass neben den Beratungen zur Gestaltung technischer Systeme auch eine verstärkte Prüftätigkeit im technischen Bereich z. T. durch Online-Prüfungen zu verzeichnen ist. Alle, auch die nichttechnischen Prüfungen machen deutlich, dass in nicht unerheblichem Umfang noch Maßnahmen zur Verbesserung des Datenschutzes zu ergreifen sind. Im Wesentlichen kann positiv festgestellt werden, dass im Gegensatz zu früheren Zeiten die Energien der geprüften Stellen nicht mehr darauf verwandt werden den Datenschutz möglichst fernzuhalten, sondern darauf gerichtet sind den Empfehlungen zur Verbesserung des Datenschutzes Rechnung zutragen.

1.1. I love you-Virus

Im Frühjahr 2000 verbreitete sich binnen kürzester Zeit — von den Philippinen kommend nach Europa und schließlich weltweit — das „I love you-Virus“ und blockierte die Netze und Rechner. Ein immenser wirtschaftlicher Schaden wurde verursacht. Auch die Bremer Verwaltung war in erheblichem Maße betroffen. Noch Tage, nachdem der Angriff erkannt und bekannt war, tauchte das als Anhang an eine E-Mail versandte Virus immer wieder neu in bereits „gereinigten“ Verwaltungsnetzen auf. Einzelne Mail-Server wurden mehrere Wochen vom Netz genommen.

Der Vorfall macht deutlich, wie verletzlich die Informationsgesellschaft ist. Die Reaktion der Politik nach dem Vorfall mit erhöhtem Strafrechtsschutz (vgl. BR-Drs. 275/00) dürfte eher von fragwürdigem Erfolg sein. Besser wäre es, den Datenschutz zu erhöhen. Nur mit hohen Sicherheitsstandards kann ein ausreichendes Schutzniveau erreicht werden. Datenschutz ist auch Datensicherheit, ist der Schutz vor nicht erlaubten Einwirkungen. Wenn nicht rechtzeitig in Datenschutz und -sicherheit investiert wird, können die Versäumnisse in Folge weit mehr Kosten verursachen oder gar den wirtschaftlichen Ruin bedeuten.

1.2. Neue Trends und die Bedrohungen des informationellen Selbstbestimmungsrechts

Die Entwicklung auf dem Gebiet der Medien und der IuK-Technik (Informations- und Kommunikationstechnik) ist rasant. Dies machen einige Zahlen deutlich, die ich diesem Bericht beifüge (vgl. Ziff. 16.8.). Unterstützt wird dieser weltweite Prozess auch durch verschiedene Initiativen der EU (vgl. Ziff. 16.8.). Es mag sich der Leser fragen, was hat diese Entwicklung mit dem Land Bremen zu tun. Nun, ich betrachte es als meine Aufgabe, die in Bremen lebenden Bürgerinnen und Bürger in ihrem Bestreben zu unterstützen, ihr informationelles Selbstbestimmungsrecht zu wahren und zu schützen. Daher muss der Landesbeauftragte für den Datenschutz für die „global villages“ Bremen und Bremerhaven den Blick über die Landesgrenzen hinaus und in die Zukunft richten, um diesem Anspruch gerecht werden zu können. Einige Schlaglichter des Jahres 2000 seien an dieser Stelle eingefangen, einige bevorstehende Entwicklungen angesprochen.

Computerprotagonisten sehen bereits jetzt, dass mit der Vernetzung von Computern durch das Internet nur ein erster Schritt getan ist. So sagte Bill Gates, „99 Prozent der großen Internet-Applikationen müssen noch geschrieben werden“. Sie sollen PC, größere Server und mobile Endgeräte miteinander umfassend verbinden. Einige sehen im XML-Standard, eine Universalsprache für Datenaustausch, den Schlüssel zur universellen Vernetzung unterschiedlichster Quellen mit PC, Fernseher, Mobiltelefon und Taschencomputer.

Gewaltigen Datenmengen, die durchs Internet transportiert werden, stellen alles bisher Dagewesene in den Schatten. Was hier mittlerweile von E-Commerce-Unternehmen bewältigt werden muss, sei einmal anhand eines der größten Online-Buchhändler dargestellt: Die Web-Site wurde im letzten Jahr monatlich von 15 Millionen Surfern besucht. Von diesen Besuchern werden Nutzerprofile angelegt, um ihren Weg durch die Site und ihr Kaufverhalten zu verfolgen und zu speichern, damit ihnen beim nächsten Besuch gleich auf der ersten Seite maßgeschneiderte Angebote präsentiert werden können. Zu diesen enormen Datenmengen kommen noch die herkömmlichen Transaktionsdaten wie Bestellungen, Stornierungen, Reklamationen und Passwortänderungen hinzu. Welche Dimensionen das Datenvolumen insgesamt bei allen E-Commerce- Unternehmen in den nächsten Jahren annehmen wird, ist kaum vorstellbar, gehen doch konservative Schätzungen davon aus, dass in diesem Jahrzehnt jährlich 50 Millionen neue Internetnutzer hinzukommen werden. Zugleich muss gesehen werden, dass spätestens im Moment einer Bestellung die gespeicherten Verbraucherprofile personenbezogen zugeordnet werden können. Diese Informationen selbst lassen sich weiter vermarkten. So ist bekannt, dass Kreditkartenunternehmen in den USA die äußerst informativen Datenspuren ihrer Kunden verkaufen. Berichten zufolge soll es branchenüblich sein, dass große Unternehmen sich über Bewerber für einen höheren Posten bereits im Vorfeld aussagekräftige Persönlichkeitsprofile von namhaften Kreditkartenunternehmen besorgen. Gebranntmarkt quasi mit einem geheimen Stempel tritt ein solcher Bewerber seinen Weg an. Nicht viel anders ergeht es dem Verbraucher, wenn er bei einem Versandhaus bestellt oder um einen Kredit nachsucht; die wenig durchschaubaren „Scorewerte“ begleiten ihn (vgl. auch Ziff. 16.4. des Berichts).

Auch das WAP (Wireless Application Protokoll) verdient ein Augenmerk des Datenschutzes. Allerdings ist im Moment noch keine Euphorie auszumachen. WAP ist zur Enttäuschung vieler nicht das angekündigte mobile farbenfrohe Internet, sondern die Datendienste fürs Handy wurden schon mit dem Videotext im Fernsehenkanal verglichen. Bisher sollen in Deutschland rund 2000 Seiten abrufbar sein, wovon zahlreiche Seiten bisher nur aus der Überschrift bestehen. Auch der Zugang ist sehr mühsam und von Provider zu Provider verschieden; komplizierte Eingaben bei E-Commerce-Anwendungen werden ebenso beklagt wie hohe Gebühren. Auf eine systematische Prüfung habe ich daher verzichtet. Die diesjährige Cebit wird allerdings voraussichtlich einen neuen Anlauf nehmen und neue WAP-Dienste anbieten, die mit der Ortsbestimmung des Nutzers (z. T. Meter genau) verbunden ist. Hier ist aus Sicht des Datenschutzes sicherzustellen, dass der Handy-Nutzer selbst entscheiden kann, ob und wann das Handy seinen Standort an Provider und Dienstanbieter übermittelt. WAP kommt allerdings auch geschäftlich zum Einsatz. So werden Unternehmensdaten außerhalb der sicheren Unternehmensumgebung erstellt. Mitarbeiter übertragen von ausgelagerten Arbeitsplätzen z. B. Kundendaten von Laptops via Handy an die Firmenrechner. Hier empfiehlt es sich, eine WAP-fähige Anti-Virensoftware für WAP-Gateways einzusetzen.

Eine weitere schnurlose Technik bahnt sich unter dem Namen „Bluetooth“ an, eine Entwicklung des so genannten Mobile-Computing, die es ermöglicht, mittels Radiowellen mit kurzer Reichweite verschiedene Endgeräte mit drahtloser Übertragungstechnik zu verbinden. Angriffspunkt ist hier die eventuelle Abhörmöglichkeit. Ähnliche Technik wird z. Zt. laut Zeitungsberichten an der Uni Bremen durch das Technologiezentrum Informatik (TZI) getestet. In zwei bis drei Jahren sollen Funkstrecken den gesamten Campus miteinander verbinden. Mit 10 Megabit können die Daten übertragen werden, eine Verbindungsqualität, die selbst für Videokonferenzen ausreicht.

Ein weiterer neuer Berufszweig hat sich entwickelt, der sog. „Infobroker“. Hierbei handelt es sich um Rechercheprofis, die im Auftrag Dritter in Archiven und Datenbanken Jagd auf Daten im Web machen. Die Aufgabe scheint dabei eher einem Spitzel zu gleichen, der heimlich in die Privatheit eindringt. Dass es dabei häufig um personenbezogene Daten geht, liegt auf der Hand. Auch hier zeigt sich, dass das Datenschutzprinzip der Datenvermeidung die beste Antwort ist.

Eine zur Einschränkung für Kinder entwickelte nicht abschaltbare Internet-Software auf dem Familien-PC entwickelte sich zum Boomerang, erlaubte sie doch nicht nur das Verhalten der Kinder im Internet, sondern auch das Verhalten der Eltern zu überwachen.

Eine absolute Sicherheit gibt es nicht, das machte im letzten Jahr ein Hackereintritt deutlich. Trotz aller Sicherheits- und Verschlüsselungstechniken, die seit Jahren mit großem Aufwand eingesetzt werden, gelang es ins Rechenzentrum von Microsoft einzubrechen und geheimgehaltene Quellcodes auszuspionieren. Der Einbrecher schickte einen so genannten Wurm oder Trojaner in die Firma. Das Programm baut eine Verbindung des infizierten Rechners ins Internet auf und ermöglicht so den Export von Daten. Auch wenn in diesem Falle nur technische Daten ausgelesen wurden, wird doch deutlich, dass Unternehmen mit personenbezogenen Daten ebenso getroffen werden können.

Im März 2000 startete ein Fernsehsender unter dem Titel „Big Brother“ ein Medienspektakel, bei dem zehn Männer und Frauen in eine gemeinsame Wohnung eingesperrt dem Voyeurismus vieler Fernseh- und Internetnutzer preisgegeben wurden. Mit der unverantwortlichen Inszenierung wurden die Schamgrenzen beim Eindringen in den sensiblen Bereich der Wohnung bagatellisiert. Mit der Sendung wird ein gesellschaftliches Bewusstsein gefördert, wonach die Persönlichkeitssphäre nur noch wenig wert ist. Indirekt wird zugleich suggeriert, das durch Art. 13 GG geschützte Grundrecht auf Unverletzlichkeit der Wohnung sei überholt. Mit der Sendung wurde zugleich Anschauungsunterricht nachgeliefert, warum Datenschutzbeauftragte gegen den „Großen Lauschangriff“ erbitterten Widerstand geleistet haben und weshalb sie sich der Zulassung von polizeilichen Videokameras in Privatwohnungen widersetzt haben. Zum Glück machen neuere Meinungsumfragen deutlich, dass der überwiegende Teil der Bevölkerung im Persönlichkeitsschutz ein sehr hohes Gut sieht.

Das Thema „Videoüberwachung“ nahm auch in 2000 wieder breiten Raum ein (vgl. Ziff. 6.1.3., 15.1.3., 15.1.5. und 17.1. dieses Berichts) und wird noch an Brisanz zunehmen. Mit der Videoüberwachung (Video- und Webcams) sind besondere Risiken für das Recht auf informationelle Selbstbestimmung verbunden. Weil eine Kamera alle Personen erfasst, die in ihren Bereich kommen, werden von der Videoüberwachung unvermeidbar völlig unverdächtige Menschen mit ihren individuellen Verhaltensweisen betroffen. Erfassung, Aufzeichnung und Übertragung der Bilder sind für die Einzelnen in aller Regel nicht durchschaubar. Schon gar nicht können sie die Bearbeitungs- und Verwendungsmöglichkeiten abschätzen. Die daraus resultierende Ungewissheit, ob und von wem sie beobachtet werden und zu welchen Zwecken dies geschieht, erzeugt einen latenten Anpassungsdruck. Dies beeinträchtigt nicht nur die grundrechtlich garantierten individuellen Entfaltungsmöglichkeiten, sondern auch das gesellschaftliche Klima in unserem freiheitlichen und demokratischen Gemeinwesen insgesamt. Alle Menschen haben grundsätzlich das Recht, sich in der Öffentlichkeit zu bewegen, ohne dass ihr Verhalten durch Kameras beobachtet, aufgezeichnet oder ins Internet übertragen wird.

Zusammenfassend lässt sich feststellen: Der Einsatz automatisierter Datenverarbeitung birgt weiterhin ein erhebliches Gefahrenpotential für die Privatsphäre der Bürgerinnen und Bürger. Mehr denn je haben sich Datennetze und Computer in allen Bereichen des Lebens ausgebreitet. Die Entwicklung geht dabei so dramatisch schnell voran, dass wir kaum noch wirklich beurteilen können, wie abhängig unsere Gesellschaft mittlerweile von der IuK-Technik ist. Dabei ist die Entwicklung so vielfältig und vielschichtig, dass wir immer häufiger an die Grenzen der Beeinflussbarkeit der verschiedenen Entwicklungen stoßen. Darüber hinaus sind die Grenzen so fließend, dass zum Teil schon nicht mehr genau zwischen realer und virtueller Welt unterschieden werden kann. Längst sind bei der Datenverarbeitung auch die Grenzen zwischen öffentlicher Verwaltung und Privatwirtschaft verwischt. Weder sind die Daten im privaten Bereich weniger sensibel als im staatlichen Bereich, noch sind die in der Wirtschaft eingesetzten DV-Anlagen moderner, als die der Verwaltung. Häufig bedienen sich beide Bereiche der gleichen Hard- und Software und der gleichen Instrumente und Methoden. Der Zwang zur Kostenreduzierung und Modernisierung hat gleichzeitig zum massiven Einsatz der automatisierten Datenverarbeitung in der Verwaltung beigetragen.

Die Computertechnologie ist in alle Lebensbereiche eingedrungen. Beim Einkaufen, Bezahlen, Reservieren mittels Chip- und Magnetstreifenkarten, in digitalen Netzen, durch Teilnahme an Online-Diensten, national und international, überall

fällt eine Fülle personenbezogener Daten an. Diese elektronischen Spuren sind geeignet, Persönlichkeitsprofile über den Einzelnen zu bilden. Die moderne IuK-Technik ermöglicht es, Daten in weltweit verteilten Rechnersystemen zu verarbeiten. Weltumspannende Datennetze schaffen die Voraussetzungen, um verschiedene Datensammlungen zusammenzuführen, nach unterschiedlichsten Gesichtspunkten zu durchsuchen und das Verhalten einzelner zu analysieren.

Auch wenn die eine oder andere Neuentwicklung auf dem Computermarkt neue Chancen für den Schutz der Privatheit bieten, so bleibt doch unter dem Strich richtig, dass mit der beschriebenen Entwicklung auch die Risiken für das informationelle Selbstbestimmungsrecht beständig gewachsen sind. Der Datenschutz bleibt daher die notwendige Antwort auf die Risiken der Computertechnik für das EU- und verfassungsrechtlich garantierte Recht auf informationelle Selbstbestimmung.

1.3. Vorbereiteter Internet-Auftritt

Die Arbeiten zur Erstellung einer eigenen Homepage sind weitestgehend abgeschlossen. Die Seite wird künftig unter www.bremen.datenschutz.de sowie www.datenschutz.bremen.de abrufbar sein. Das Layout orientiert sich an der Seite bremen.de. Das Angebot wird technisch gesehen aus einem Frame bestehen, auf dem sämtliche Steuerungsfunktionen untergebracht sind und es wird XML-fähig sein, ein Format, das die Volltextsuche erleichtert. Das Angebot wird in einigen Bereichen aus dynamisch erzeugten Webseiten bestehen, die tagesaktuell gepflegt werden können und z. B. besonders für Presseerklärungen geeignet sind. Die inhaltliche Struktur der Homepage wird u. a. die Bereiche „Tipps für Bürger“, „Informationen — Jahresberichte“, „Recht“, „Technik“, „Datenschutzausschuss der Bremischen Bürgerschaft“ und „Aktuelles“ enthalten. Für die Bürger werden u. a. Formulare zum Download und Ausdruck bereitgestellt. Die Seite ist mit den Angeboten anderer Datenschutzbeauftragte, insbesondere dem „Virtuellen Datenschutzbüro“ verlinkt.

Ich habe dem Datenschutzausschuss das Projekt im Oktober 2000 vorgestellt; er ist mit dem Konzept und Präsentation einverstanden.

1.4. Serviceorientierte Verwaltung

Verwaltungsreform, Bürgerämter, Bürgerbüros, Bürgerkommune, Service-Center und Call-Center sowie Internet-basierte Verwaltungsdienstleistungen sind die neuen Stichworte, unter die sich die Umgestaltung der Verwaltung zusammenfassen lässt. Eine Arbeitsgruppe der Datenschutzbeauftragten der Länder — an der ich mich beteiligt habe — hat für diesen Bereich ihre Vorschläge für einen sicheren Datenschutz zusammengetragen und in einer Broschüre veröffentlicht, die in meiner Dienststelle angefordert werden kann. Der Inhalt der Broschüre ist auch im Internet abrufbar. Folgende Themen werden dort behandelt:

- Multifunktionaler Service (Bürgeramt, Bürgerbüro, Bürgerladen und Kundencenter),
- Call-Center,
- Informationsangebote öffentlicher Stellen im Internet,
- Interaktive Verwaltung,
- Bürgerkarte,
- Elektronische Auskunft, Akteneinsicht und Bürgerbeteiligung,
- Auslagerung von Verwaltungsfunktionen.

1.5. Zur Situation der Dienststelle

Der amtierende Landesbeauftragte für den Datenschutz hatte sich am 31. Dezember 1999 aus seinem Amt verabschiedet, die Wiederbesetzung der Stelle konnte im Berichtszeitraum nicht abgeschlossen werden. Mit der Entscheidung des Senats vom 6. Februar 2001 zeichnet sich in dieser Frage ein Ende ab. (Nach Redaktionsschluss wurde ich am 21. Februar 2001 von der Bremischen Bürgerschaft gewählt.) Bedingt durch die Unsicherheit der Entscheidung des Senats konnten längst über-

fällige Umstrukturierungsmaßnahmen im Berichtsjahr nicht getroffen werden. Hinzu traten weitere personelle Abgänge. Damit sind zwar die Zielzahlen des PEP (Personalentwicklungsprogramm) erreicht, da aber die Anforderungen an die Dienststelle nicht geringer wurden, konnten die Arbeitsergebnisse nur gehalten werden, indem die einzelnen Beschäftigten zum Teil in erheblichem Umfang Mehrarbeit leisteten, die noch im kommenden Jahr abzubauen sein wird. Ich denke, der Bericht macht die Leistungsfähigkeit der Dienststelle sowie die Vielfalt und Bandbreite des Tätigkeitsspektrums deutlich, auch wenn gerade die Erledigung der vielen, den Landesbeauftragten für den Datenschutz erreichenden Bürgeranfragen und Beschwerden, die oft auch eine Aufklärung vor Ort — häufig daher verbunden mit Fahrten nach Bremen — erfordern, nicht so deutlich zum Ausdruck kommen.

Ich habe das letzte Jahr genutzt, alle Haushaltspositionen auf Einsparmöglichkeiten hin zu untersuchen. Durch harte Verhandlungen oder Wechsel des Vertragspartners konnte ich in einer Reihe von Positionen günstigere Bedingungen oder sogar rückwirkend eine Gutschrift erreichen. Auf der anderen Seite ist absehbar, will sich der Landesbeauftragte für den Datenschutz nicht aus dem Verbund der Bremer Verwaltung verabschieden, dass sich bereits im kommenden Jahr — auch wegen des Standortes — Kostensteigerungen in einzelnen Haushaltsbereichen abzeichnen. So wird es unbedingt erforderlich sein, eine Standleitung für die Datenübertragung nach Bremen einzurichten. Auch die neuen Bahntarife und erhöhte Heizölkosten werden zu Buche schlagen. Im Berichtsjahr konnten in nur sehr eingeschränktem Umfang technische Fortbildungsmaßnahmen genehmigt werden, um die Haushaltsansätze nicht zu überschreiten. Angesichts der raschen technischen Entwicklung und der Vielzahl der mit technischem Sachverstand von der Dienststelle zu beratenden Projekte und zu kontrollierenden Verfahren ist eine permanente Fortbildung eine notwendige Voraussetzung für die Aufgabenerfüllung.

1.6. Eingabenschwerpunkte und Öffentlichkeitsarbeit

Ein bedeutender Teil der von mir zu erfüllenden Aufgaben ist die Bearbeitung von Bürgereingaben. Sie bezogen sich zu ungefähr gleichen Teilen auf die Verarbeitung personenbezogener Daten im öffentlichen und im nicht-öffentlichen Bereich. Während die Eingaben im öffentlichen Bereich insbesondere die Verarbeitung personenbezogener Daten durch die Polizei, die Sozialverwaltung und Einrichtungen des öffentlichen Gesundheitsdienstes betrafen, bezogen sie sich im nicht-öffentlichen Bereich insbesondere auf Fragen des Arbeitnehmerdatenschutzes und die Datenverarbeitung von Kreditinstituten, Versicherungsgesellschaften, Auskunftseien und in zunehmendem Maße auf Internet-Provider.

Die Eingaben waren nicht selten Anlass für umfangreiche Datenschutzüberprüfungen, deren Zahl — trotz der geringeren Personaldecke — notwendigerweise im Berichtszeitraum ebenfalls zunahm.

Mehrere Fortbildungsveranstaltungen und Vorträge zu aktuellen Themen des Datenschutzes wurden außerdem wieder in Wirtschaft und Verwaltung durchgeführt. Ein Schwerpunkt hierbei waren Veranstaltungen bei Einrichtungen im Sozialbereich und des öffentlichen Gesundheitswesens. Auch die Presse griff — oft nach Pressemitteilungen — aktuelle Datenschutzthemen auf. Exemplarisch genannt seien Berichte der Bremer Presse wie „Abgehört wird auch im Internet“, „Der gläserne Mensch“, „Keine Weitergabe von Daten an rechtsradikale Parteien“, „Datenschützer warnt vor Kunden-Observationen“, „Menschen werden Objekt fremder Einflussnahme“, „Big Brother auf dem Weg zum Sielwall“, „Lauschangriff: Keine Wanzen in der guten Stube“, „Videoüberwachung: Allheilmittel oder Gift für Freiheitsrechte“, „Webcams, Datenschützer besorgt“ oder „Der gläserne Student“.

1.7. Kooperation mit anderen Datenschutzbehörden

Die Zusammenarbeit und der Erfahrungsaustausch findet für den öffentlichen Bereich unter den Datenschutzbeauftragten von Bund und Ländern statt und für den privaten Bereich unter den Datenschutzaufsichtsbehörden.

Die Konferenz der Datenschutzbeauftragten tagte in Hannover und Braunschweig unter Vorsitz des Niedersächsischen Datenschutzbeauftragten. Die wichtigsten Themen finden sich in den Konferenzbeschlüssen wieder (vgl. Ziff. 17. dieses Berichts). Die obersten Datenschutzaufsichtsbehörden der Länder trafen sich zweimal in Düsseldorf. Die hier erzielten Ergebnisse werden jeweils in einem Protokoll fest-

gehalten, das nicht veröffentlicht wird, die Beschlüsse des „Düsseldorfer Kreises“ schaffen aber für die Datenschutzkontrollen der Aufsichtsbehörden eine einheitliche Grundlage für die Anwendung der Vorschriften des Bundesdatenschutzgesetzes (BDSG) im nicht-öffentlichen Bereich. Einige der Themen finden sich unter Ziff. 16. dieses Berichts. Auf der Ebene der Aufsichtsbehörden findet in der Regel einmal im Jahr ein Workshop statt, wo alle Teilnehmer einen Themenbereich vorbereiten. In beiden Bereichen (öffentlich und nicht-öffentlich) findet die Zusammenarbeit auch auf der Ebene von fachspezifischen Arbeitskreisen statt, an denen sich i. d. R. jeweils nur ein Teil der Länder beteiligen.

1.8. Ausblick

Die Anpassung der Vorschriften des BDSG an die EU-Datenschutzrichtlinie wird höchste Zeit, wird doch seit Ende des Berichtsjahrs die Einleitung eines Vertragsverletzungsverfahrens durch die Europäische Kommission geprüft. Nunmehr wird für Ende Mai 2001 das Inkrafttreten des neuen BDSG erwartet. Daraus resultierend kann spätestens dann auch zügig mit der Novellierung des Bremischen Datenschutzgesetzes (BrDSG) begonnen werden. Die Entwicklungen in Bezug auf Polizeigesetz und Meldegesetz sind in 2000 nicht so schnell vorangekommen, wie ich noch im letzten Bericht gemutmaßt habe die parlamentarischen Beratungen werden in 2001 aufgenommen werden.

Des weiteren ist demnächst vom Bund der Entwurf eines Arbeitnehmerdatenschutzgesetzes zu erwarten. Der dafür zuständige Referatsleiter im Bundesarbeitsministerium hatte im Berichtsjahr dem Arbeitskreis Personalwesen der Datenschutzbeauftragten des Bundes und der Länder die Grundzüge des Entwurfs dargelegt und erklärt, neben bereichsspezifischen Regelungen über die Verarbeitung von Arbeitnehmerdaten werde der Gesetzentwurf im Hinblick auf die Informations- und Kommunikationsfreiheit Regelungen zur Nutzung von E-Mail und Internet am Arbeitsplatz vorsehen. Die nähere Ausgestaltung dieser Regelungen bleibe Betriebsvereinbarungen vorbehalten.

Die Präsenz des Landesbeauftragten für den Datenschutz mit einer Homepage im Internet (vgl. Ziff. 1.3. dieses Berichtes) wird ebenso wie die vom BDSG übertragenen neuen Aufgaben weitere Arbeit (z. B. Bürgereingaben zu Videoüberwachung und Chip-Karten) nach sich ziehen und zu Schwerpunktverlagerungen führen. Die Vielzahl der Automatisationsprojekte der Verwaltung in Bremen und Bremerhaven ist dem Bericht zu entnehmen, die meisten sind noch nicht abgeschlossen und bedürfen weiterer Begleitung. Hinzu kommen neue Projekte. Schon jetzt ist absehbar, dass die völlige Neustrukturierung der DV der Polizei (Vorgangsbearbeitung und INPOL-neu) umfangreiche Datenschutzberatung und -begleitung verlangen wird.

Auf dem Weg zu einer Informations- und Kommunikationsgesellschaft werden zunehmend auch technische Aspekte des Datenschutzes eine entscheidende Rolle spielen. Überall wo IuK-Technologie zur Verarbeitung personenbezogener Daten eingesetzt wird, sind technische, organisatorische und personelle Maßnahmen erforderlich, um eine missbräuchliche oder zweckentfremdete Nutzung der Daten zu vermeiden. Eine wichtige Aufgabe kann dabei von der Technik selbst übernommen werden, wenn es gelingt, in größerem Rahmen technische Systeme auch im Interesse des Datenschutzes zu entwickeln und einzusetzen. Verschlüsselungs- und Anonymisierungstechniken oder so genannte Webwasher, (z. B. Filter gegen Bugs, Banner, Privacyverletzungen oder Cookies) sind nur Beispiele für diese Entwicklung, die letztlich noch weiter gehen wird, wenn erst erkannt wird, dass der Datenschutz selbst auch ein Zukunftsmarkt sein wird. Jedenfalls belegen die Meinungsumfragen zum Datenschutz u. a. auch, dass alle Generationen dem Datenschutz einen hohen Stellenwert einräumen. Datenschutz wird damit zu einem Qualitätsmerkmal. Diesen Prozess gilt es aktiv zu unterstützen.