

9. Inneres

9.1 Unberechtigter Zugriff auf Online-Melderegister war möglich

Wenige Stunden vor Ausstrahlung eines Fernsehberichts über eine Sicherheitslücke einer Internetkomponente einer Einwohnermeldeamtssoftware, die auch im Land Bremen zum Einsatz kommt, wurde ich von Kollegen aus einem anderen Bundesland darüber in Kenntnis gesetzt. Ich setzte mich umgehend mit den Einwohnermeldeämtern in Bremen und Bremerhaven in Verbindung. Für Bremen konnte sofort Entwarnung gegeben werden, da nach Auskunft des Stadtamtes das entsprechende Softwaremodul noch nicht zum Einsatz gekommen war. Anders in Bremerhaven, wo die Online-Melderegisterauskunft bereits im Einsatz war. Beim dortigen Bürger- und Ordnungsamt führte ich umgehend eine Datenschutzprüfung des betroffenen Moduls durch. Sowohl das Amt als auch die b.i.t. (technischer Betreiber) zeigten sich bei der Prüfung sehr kooperativ. Im Rahmen der Prüfung konnte ich feststellen, dass die Sicherheitslücke in Bremerhaven tatsächlich bestand: Ein Standardpasswort eines Benutzerkontos, mit dem die Software immer ausgeliefert wird, war nicht in geeigneter Form geändert worden. Protokolldaten gaben Auskunft darüber, dass es seit 2005 Zugriffe aus dem Internet unter der besagten Benutzerkennung gegeben hatte, die aber fast immer eindeutig im Rahmen von Wartungsarbeiten dem Softwarehersteller oder der b.i.t zuzuordnen waren. Allerdings gab es im Mai 2008 einmalig Zugriffe, die nicht Wartungsarbeiten oder, das hat eine Rückfrage beim Fernsehsender ergeben, den Recherchen im Zusammenhang mit dem Fernsehbericht zuzuordnen waren; ich musste daher von einer unberechtigten Nutzung ausgehen. Bei diesen Zugriffen wurden verschiedene Bereiche des Software-Moduls aufgerufen. Aus den Protokolldaten ist jedoch ersichtlich, dass keine Daten Bremerhavener Bürger eingesehen wurden. Eine Benachrichtigung betroffener Bürger durch das Bürger- und Ordnungsamt war somit nicht notwendig.

Die Herstellerfirma handelte grob fahrlässig, indem sie die Software mit einem Standardpasswort ausgeliefert und dieses Standardpasswort auf einer ihrer Web-Seiten versehentlich veröffentlicht hatte. Ich habe das Bürger- und Ordnungsamt aufgefordert, die Mängel abzustellen und erst nach deren Beseitigung die Online-Melderegisterauskunft wieder in Betrieb zu nehmen.

9.2 Übermittlung von Meldedaten an Adresshändler

Bedingt durch die Datenskandale geriet der Adresshandel in das Blickfeld der Öffentlichkeit. In diesem Zusammenhang wurde auch die Rolle der Melderegister von den Medien, so auch von Radio Bremen, ins Visier genommen.

Nach den melderechtlichen Bestimmungen dürfen die Meldebehörden in Bremen und Bremerhaven Auskünfte über im Melderegister gespeicherte Einwohnerinnen und Einwohner auch an Privatpersonen erteilen. Voraussetzung für die Erteilung einer sogenannten einfachen Melderegisterauskunft nach § 32 Abs. 1 des bremischen Meldegesetzes (BremMeldG), bei der die Meldebehörde Auskunft über Vor- und Familiennamen, Doktorgrade und Anschriften erteilt, ist, dass die auskunftersuchende Person oder Stelle den Betroffenen hinreichend bestimmt. Soweit ein berechtigtes Interesse glaubhaft gemacht wird, dürfen die Meldebehörden gem. § 32 Abs. 2 BremMeldG eine erweiterte Melderegisterauskunft u. a. auch über frühere Vor- und Familiennamen, Tag und Ort der Geburt, Staatsangehörigkeiten, den Familienstand, gesetzliche Vertreterinnen und

Vertreter sowie Anschriften von Ehegatten erteilen. Melderegisterauskünfte über eine Vielzahl nicht namentlich bezeichneter Einwohnerinnen und Einwohner mit einem § 32 Abs. 2 BremMeldG vergleichbaren Datenumfang dürfen die Meldebehörden im Rahmen einer sogenannten Gruppenauskunft nach § 32 Abs. 3 BremMeldG an den genannten Empfängerkreis übermitteln. Die Entscheidung über die Erteilung einer Auskunft nach § 32 BremMeldG liegt jeweils im Ermessen der Meldebehörde.

Nicht selten werden von den Meldebehörden in Bremen und Bremerhaven Melderegisterauskünfte nach § 32 BremMeldG auch an Adresshandelsunternehmen übermittelt, die im Auftrag eines Unternehmens oder einer Privatperson als Adressermittler tätig werden. Hintergrund des Auftrags kann z. B. die Geltendmachung einer finanziellen Forderung gegenüber einem Schuldner sein, wenn dessen Anschrift dem Gläubiger nicht bekannt ist. Häufig werden die über den Adressermittlungsauftrag von den Adresshandelsunternehmen bei den Meldebehörden erhobenen Daten über den Auftrag hinaus in eigenen Datenbanken fortgespeichert, um danach Auskünfte hieraus oder durch den listenmäßigen Verkauf von Daten weitere Einnahmen erzielen zu können. Auf diesem Wege entstehen im privaten Bereich weitere partielle Einwohnermelderegister. Dies stellt eine Zweckänderung dar und ist mit den datenschutzrechtlichen Anforderungen an den Adresserhebungsauftrag und den Vorgaben des Melderechts nicht vereinbar. Die Melderegister dienen vorrangig der staatlichen Aufgabenerfüllung. Sie bieten daneben nicht öffentlichen Stellen und Privatpersonen auf der Grundlage der gesetzlichen Bestimmungen auch Unterstützung an. Da die Bürgerinnen und Bürger zur Abgabe der in den Melderegistern zu speichernden Daten verpflichtet sind, bedürfen sie eines weitergehenden Schutzes. Die Führung von Datenbanken durch Adresshandelsunternehmen mit von ihnen bei den Meldebehörden erhobenen Daten widerspricht den Intentionen des Melderechts. Die nach den melderechtlichen Bestimmungen zu beachtenden schutzwürdigen Interessen der Betroffenen finden bei den Privaten keine Berücksichtigung mehr.

Den Meldebehörden ist daher nahegelegt, im Rahmen ihrer Ermessensentscheidung zumindest keine Meldedaten mehr an die betreffenden Adresshandelsunternehmen herauszugeben, bei denen eine zweckwidrige Verwendung der Meldedaten festgestellt wurde. Darüber hinaus ist die Regelung zur Herausgabe von Meldedaten an Adressbuchverlage ohne Einwilligung der Betroffenen zur Erstellung von Adressbüchern zu überprüfen. Da das Melderecht dem Bund übertragen wurde, sind diese Überlegungen bei der Schaffung eines einheitlichen Bundesmeldegesetzes (vgl. Ziff. 9.4 dieses Berichts) anzustellen.

9.3 Direktzugriff auf Meldedaten durch Behörden

Nach § 30 Abs. 4 Bremisches Meldegesetz (BremMG) erhalten Behörden nur aufgrund einer Rechtsverordnung einen Direktzugriff auf Meldedaten, d. h., diese Stellen können Daten online unmittelbar aus dem Melderegister abrufen. Der Senator für Inneres und Sport hat jedoch Anfang 2007 per Erlass verfügt, dass dieser Vorbehalt einer Rechtsverordnung nicht für Datenabrufe durch Behörden innerhalb einer Gemeinde gilt, der die Meldebehörde angehört. Begründet wird dies damit, § 30 Abs. 5 BremMG enthalte eine entsprechende Ermächtigung. Vielmehr soll nunmehr eine Prüfung ausreichen, ob die angeforderten Daten von der empfangenden Behörde regelmäßig zur Aufgabenerfüllung benötigt werden. Auch sei zu untersuchen, ob und ggf. in welchem Umfang mit der Nutzung des Abrufverfahrens Gefahren für die Rechte der Betroffenen verbunden sind. Der benötigte Datenumfang sei nachprüfbar festzulegen.

Von diesem Erlass habe ich erst im Frühjahr 2008 erfahren. Ich halte den Erlass nicht für rechtskonform und habe der senatorischen Behörde mitgeteilt, die Regelung des § 30 Abs. 5 BremMG besagt ausschließlich, dass derartige Behörden mehr Meldedaten (z. B. Religionszugehörigkeit, Angaben über Ehepartner bzw. Lebenspartner) erhalten können als Behörden, die nicht der Gemeinde der Meldebehörde angehören. Diese Regelung bezieht weder die regelmäßige Datenübermittlung noch den automatisierten Datenabruf ausdrücklich ein. Seit Bestehen des bremischen Meldegesetzes und der technischen Möglichkeit eines automatisierten Abrufs sind viele Regelungen in der Meldedatenübermittlungsverordnung geschaffen worden.

Auch datenschutzpolitisch vermag ich im Übrigen ein Absehen von einer Rechtsverordnung, die die Informationsaustauschwege bei Meldedaten offen legt, nicht nachvollziehen. In weiten Bereichen der Verwaltung sollen die Bürgerinnen und Bürger möglichst umfassend über das Verwaltungshandeln informiert und dadurch Transparenz hergestellt werden. Aber hier, wo eine „Datenautobahn“ eingerichtet werden soll, sollen die betroffenen Bürgerinnen und Bürger nicht einmal erfahren, welche Datenpakete sich darauf bewegen dürfen. Der Wegfall der datenschutzrechtlichen Überprüfung der Zulässigkeit der Datenübermittlung bzw. -weitergabe an eine andere Stelle muss kompensiert werden. Dies geschieht in einer Rechtsverordnung, die für jedermann erkennbar offenlegt, welche Daten aus welchem Anlass zu welchem Zweck an wen übermittelt bzw. weitergegeben werden dürfen.

Der Senator für Inneres und Sport hält die bisherige datenschutzkonforme Praxis nach wie vor unter Hinweis auf die Strukturierung des § 30 BremMG nicht mehr für angezeigt. Er beharrt auf seiner Position, obwohl ich ihn auch nach einer Umfrage unter den Datenschutzbeauftragten des Bundes und der Länder, die meine Rechtsauffassung teilen, aufgefordert habe, den Erlass aufzuheben und an der bisherigen Praxis festzuhalten.

9.4 Entwurf eines Bundesmeldegesetzes

Mit dem Gesetz zur Änderung des Grundgesetzes vom 28. August 2006 (BGBl. I S. 2034) wurde dem Bund gem. Art. 73 Abs. 1 Nr. 3 Grundgesetz die ausschließliche Gesetzgebung für das Melde- und Ausweiswesen übertragen. Hierzu hat der Bundesminister des Innern nun im Berichtsjahr den Referentenentwurf eines Gesetzes zur Fortentwicklung des Meldewesens (Bundesmeldegesetz) vorgelegt. Mit dem Gesetz sollen die Grundlagen für ein einheitliches Melderecht und die Errichtung zentraler Registerstrukturen für einen effektiveren und effizienteren Vollzug des Melderechts geschaffen werden. Der Entwurf aus dem Bundesministerium des Innern entspricht in zahlreichen Punkten nicht den Forderungen des von den Datenschutzbeauftragten des Bundes und der Länder erarbeiteten Eckpunktepapiers. Ich habe den Senator für Inneres und Sport hierüber unterrichtet und ihn um Unterstützung der datenschutzrechtlichen Forderungen gebeten.

Im Einzelnen sieht der Referentenentwurf ein zusätzliches zentrales Bundesmelderegister und damit eine doppelte Datenhaltung vor. Das Vorhaben widerspricht dem Grundsatz der Datenvermeidung, der Vermeidung einer doppelten Datenstruktur und dem Erforderlichkeitsprinzip. Die bisherige dezentrale Struktur hat sich bewährt und entspricht den Anforderungen, um die mit dem Bundesmeldegesetz beabsichtigten politischen Ziele (u. a. funktionierendes Rückmeldeverfahren, Konsolidierung der Daten, Aktualität der Daten, Nutzung der Meldedaten durch öffentliche Stellen, Online-Melderegisterauskunft und zeitnaher Zugriff auf Meldedaten durch Polizeibehörden) zu

erreichen. Der Aufbau eines zentralen Bundesmelderegisters und die damit verbundene problematische, mehrfache Datenhaltung ist daher nicht erforderlich.

Nach dem Entwurf sollen die in den Melderegistern gespeicherten die Identifikation des Betroffenen ermöglichenden Ordnungsmerkmale auch an andere Behörden und öffentlich-rechtliche Religionsgesellschaften übermittelt werden dürfen. Die Ordnungsmerkmale sollen von den Meldebehörden aus den zur jeweiligen Person gespeicherten Meldedaten erstellt werden dürfen und die Führung der automatisierten Melderegister vereinfachen. Im Bundesmelderegister wird zudem ein weiteres Ordnungsmerkmal kreiert, das dem bundesweiten Datenaustausch dienen soll. So entstehen ein oder sogar mehrere verknüpfte einheitliche Personenkennzeichen. Die vorgesehene Schaffung und Verwendung von Ordnungsmerkmalen ist mit den Anforderungen des BVerfG im sog. Volkszählungsurteil nicht zu vereinbaren und daher ebenfalls abzulehnen.

Der Referentenentwurf sieht im Vergleich zu den bislang geltenden Bestimmungen des Melderechtsrahmengesetzes des Bundes und auch denen des bremischen Meldegesetzes eine Ausweitung des Umfangs der von den Meldebehörden zu speichernden Daten und der möglichen Datenübermittlungen vor, die nicht akzeptabel ist. So sollen die Meldebehörden nach dem Referentenentwurf künftig wesentlich mehr Angaben zu ihren Annexkompetenzen, wie z. B. die Mitwirkung bei Steuerverfahren, speichern. Angaben zu Sterbetag und Sterbeort sollen bereits im Rahmen der „einfachen Melderegisterauskunft“, bei der es ausreicht, den Betroffenen hinreichend zu bestimmen, erteilt werden dürfen. War z. B. bei der Erteilung von Melderegisterauskünften über eine Vielzahl nicht namentlich bezeichneter Einwohnerinnen und Einwohner (Gruppenauskunft) die für die Zusammensetzung der Personengruppe heranziehbar Angabe „Familienstand“ beschränkt darauf, ob verheiratet oder eine Lebenspartnerschaft führend, so sollen nach dem Gesetzesentwurf auch die Kriterien „ledig“, „verwitwet“ oder „geschieden“ maßgeblich sein können. Wie bislang schon nach den Bestimmungen des Melderechtsrahmengesetzes und des bremischen Meldegesetzes soll auch die Übermittlung besonderer Arten personenbezogener Daten, insbesondere von Staatsangehörigkeiten, an Personen, die nicht Betroffene sind, und nicht öffentliche Stellen erlaubt sein, wenn lediglich ein berechtigtes Interesse beim Datenempfänger vorliegt. Dies ist mit den einzuhaltenden datenschutzrechtlichen Anforderungen nicht zu vereinbaren.

Die Rechte der Betroffenen werden mit den Regelungen des Gesetzesentwurfs nicht im erforderlichen Umfang gestärkt. An der Widerspruchslösung bei Datenübermittlungen wird festgehalten anstatt diese durch Einwilligungslösungen zu ersetzen. Auf diese Weise könnte z. B. die Weitergabe von Daten zu Marketingzwecken unterbunden bzw. restriktiv geregelt und Missbräuchen entgegengewirkt werden. Auch die Möglichkeit, Firmen von Datenübermittlungen auszuschließen, wenn sie die ihnen übermittelten Daten missbräuchlich verarbeitet oder genutzt haben, sieht der Gesetzesentwurf nicht vor. Die von Datenschutzbeauftragten schon seit längerem erhobene Forderung, Melderegisterauskünfte in besonderen Fällen, also z. B. im Zusammenhang mit Alters- oder Ehejubiläen oder für die Herausgabe eines Adressbuchs, nur noch mit der Einwilligung der Betroffenen zu erlauben, bleibt im Entwurf ebenfalls unberücksichtigt.

Für die regelmäßige Übermittlung personenbezogener Daten, insbesondere in Form automatisierter Datenabrufe, bedarf es präziser Festlegungen des Anlasses und des Zwecks der Übermittlungen, der Datenempfänger und der zu übermittelnden Daten, was durch Bundes- oder Landesrecht (z. B. durch Meldedatenübermittlungsverordnung) bestimmt sein muss. Mit der Einrichtung regelmäßiger

Datenübermittlungen sind erheblich mehr Risiken verbunden als bei einzelnen nicht regelmäßigen Übermittlungen. Dies gilt auch für die Weitergabe von Daten innerhalb derselben Verwaltungseinheit, z. B. der Kommune. Der Gesetzesentwurf entspricht auch diesen Anforderungen nicht ausreichend.

Im Entwurf fehlen außerdem insbesondere Vorschriften zur wirksamen Protokollierung und Revision. Internetzugänge dürfen nur eingerichtet werden, wenn durch geeignete technische Maßnahmen ein Datenmissbrauch ausgeschlossen ist. Das ist nach den bisherigen Regelungen nicht gewährleistet.

Auch die nach dem Entwurf geplanten Einschränkungen der Prüfkompetenz der Landesdatenschutzbeauftragten aus Gründen der inneren Sicherheit sind absurd und widersprechen der vom Bundesverfassungsgericht immer wieder geforderten effektiven unabhängigen Kontrollmöglichkeit jeglicher personenbezogener Datenverarbeitung.

9.5 Videoüberwachung auf der „Discomeile“

Im Juli 2008 habe ich eine Kontrolle der polizeilichen Videoüberwachung der „Discomeile“ durchgeführt (vgl. 30. JB, Ziff. 9.2). Meine Prüfung ergab, dass die Kennzeichnung des videoüberwachten Bereichs nicht ausreichend ist. Auf dem Weg vom Herdentorsteinweg zur Fußgängerzone „Auf der Brake“ fehlt ein erkennbarer Hinweis auf eine Videoüberwachung. Hier wurde gegen § 29 Abs. 3 Satz 1 Bremisches Polizeigesetz (BremPolG) verstoßen. Es ist hier noch ein weiteres Schild für den Bereich der Kamera „Auf der Brake“ aufzustellen, wie schon aus dem Beschilderungskonzept hervorgeht. Die Polizei holte diesbezüglich eine Erlaubnis des Gebäudeeigentümers ein, um am Überbau des Hauses beim Durchgang Herdentorsteinweg/Auf der Brake ein Schild anbringen zu dürfen. Die Beschilderung soll nun unverzüglich erfolgen. Weiterhin stellte ich fest, dass die Kamera auf dem Rembertiring (in der Nähe der Schilderbrücke, auf der Höhe des Stubu) die Straßenseite des Tivolihochhauses und damit hilfeschende Drogenabhängige, die das Kontakt- und Beratungszentrum „Tivoli“ aufgesucht haben, filmen konnte. Auch hier lag ein Verstoß gegen § 29 Abs. 3 Satz 1 BremPolG vor. Nach meinem Hinweis wurde dieser Straßenabschnitt von der Kameraüberwachung sofort ausgenommen. Des Weiteren war aufgrund einer fehlerhaften Konfiguration im Zusammenhang mit einem Software-Update das Netz zur Übertragung der Videodaten mit dem bremischen Verwaltungsnetz (BVN) und darüber auch mit dem Internet verbunden. Zwar war es nicht möglich, aus dem BVN oder Internet auf die Kameras und das Netz zur Übertragung der Videodaten zuzugreifen, die Kopplung mit dem BVN widerspricht allerdings dem Sicherheitskonzept für die Videoüberwachung der „Discomeile“. Dieser Fehler wurde nach meinem Hinweis unverzüglich von der Brekom als technischem Betreiber des Netzes beseitigt.

Im Zusammenhang mit der „Discomeile“ erreichten mich Beschwerden betreffend die private Videoüberwachung innerhalb einer Diskothek auf der „Discomeile“. In dieser Diskothek wird auch eine private Videoüberwachung der Notausgänge und des mit den Notausgängen verbundenen Treppenhauses eines privaten Wohngebäudes betrieben. Im Rahmen meiner Prüfung hat es Gespräche mit dem Diskothekenbetreiber, dem Wohnhauseigentümer und dem Stadtamt gegeben, und es wurden Lösungen erarbeitet.

9.6 Aktualisierte KpS-Richtlinien

In meinem 28. Jahresbericht (vgl. Ziff. 9.7) hatte ich die Überarbeitung der aus dem Jahre 1981 stammenden Richtlinien für die Führung Kriminalpolizeilicher Sammlungen (KpS-Richtlinien)

gefordert. Diese legen allgemein für typische Sachverhalte der polizeilichen Arbeit fest, welche personenbezogenen Daten erhoben und gespeichert werden dürfen. Darüber hinaus enthalten die KpS-Richtlinien grundlegende Regelungen u. a. zur Übermittlung personenbezogener Daten, zur Auskunft an Betroffene und zur Speicherdauer. Die Rechtsgrundlagen für die KpS-Richtlinien finden sich im Bremischen Polizeigesetz (BremPolG), im Bremischen Datenschutzgesetz (BremDSG) und in der Strafprozessordnung (StPO).

Im Mai 2008 wurde mir ein überarbeiteter Entwurf der KpS-Richtlinien vorgelegt, zu dem ich abschließend Stellung nahm. Die neuen KpS-Richtlinien wurden vom Senator für Inneres und Sport zum 1. November 2008 in Kraft gesetzt. Für die Betroffenen konnten einige Vorteile erreicht werden. So wurden die Löschfristen verkürzt. Zum Beispiel bei den Delikten von Jugendlichen mit geringer Bedeutung wurde die Löschfrist von fünf auf zweieinhalb Jahre und bei Kindern von zwei auf ein Jahr halbiert. Die Schadensgrenze bei Sachbeschädigung (§ 303 StGB), Diebstahl (§ 242 StGB), Unterschlagung (§ 246 StGB), Betrug (§ 263 StGB), Erschleichen von Leistungen (§ 265 a StGB) wurde von 100 € auf 1000 € erhöht. Der Grund für diese Heraufsetzung der Schadensgrenze liegt darin, den Bereich der Kleinkriminalität unterhalb dieser Grenze herauszunehmen. Die personenbezogenen Hinweise (PHW) werden grundsätzlich nach fünf Jahren gelöscht.

Während die anderen Punkte abgestimmt werden konnten, konnte keine inhaltliche Einigung bei dem PHW „psychisch auffällig“ erzielt werden. Die PHW dienen vor allem der Eigensicherung der Polizei (vgl. 30. JB, Ziff. 9.19) und werden im Rahmen der Einsatztaktik der Polizei berücksichtigt. PHW sind beispielsweise Attribute wie „gewalttätig“, „bewaffnet“ oder „psychisch auffällig“. Der letztgenannte PHW wird bundesweit nur im Land Bremen nach der Dienstanweisung über polizeiliche Maßnahmen gegenüber psychisch auffälligen Personen aus dem Jahre 2003 vergeben. In dieser Dienstanweisung wird geregelt, dass der PHW „psychisch auffällig“ im Vorfeld der Feststellung einer psychischen Krankheit vergeben werden kann. Somit bedarf es für diesen Eintrag in dem polizeilichen Informationssystem keiner Feststellung einer psychischen Erkrankung durch den Arzt.

Beschwerden von Betroffenen führten dazu, dass die Vergabe des PHW „psychisch auffällig“ im jeweiligen Einzelfall nicht genau verifizierbar war (vgl. 30. JB, Ziff. 9.5 und Ziff. 9.19). Mit Blick auf die bundesweit durchaus übliche Vergabe eines PHW „psychisch krank“ nach ärztlicher Feststellung regte ich an, den PHW „psychisch auffällig“ abzuschaffen und den PHW „psychisch krank“ einzuführen. Inwieweit darüber hinaus noch eine weitere Kategorie erforderlich ist, die den Kreis der Eigen- und Fremdgefährder ohne ärztliche Feststellung umfasst, bedarf noch weiterer Erörterung.

9.7 Internetnutzung bei der Polizei Bremen

Vor vier Jahren habe ich die Internetnutzung bei der Polizei Bremen geprüft und aufgrund der vorgefundenen Mängel ein entsprechendes Datenschutzkonzept gefordert, das den Einsatz von Rechnern mit Internetanschlüssen in den Revieren regelt (vgl. 27. JB Ziffer 6.1). Da bei der Polizei Bremen der Zugriff auf das Programm Fundinfo über eine Internetverbindung geplant ist (vgl. 29. JB Ziffer 9.21), habe ich es für erforderlich gehalten, die Umsetzung der von der Polizei Bremen seinerzeit angekündigten Maßnahmen zu überprüfen. Dazu habe ich die Internetnutzung in zwei Polizeirevieren sowie in zwei Abteilungen des Polizeipräsidiums geprüft.

Polizeiinterne Vorgaben für die Mitarbeiter zur Nutzung des Internets ergeben sich aus der „Dienstanweisung für die Nutzung des Internet bei der Polizei Bremen“. Danach ist die private

Nutzung des Internets untersagt. Weiterhin ist es nicht zulässig, Daten mit dienstlichem Bezug auf den Internetrechnern zu speichern. Die Dienstanweisung sowie ein weiteres Merkblatt zur Internetnutzung wurden auf dem Desktop eines jeden Internetrechners sichtbar für die Mitarbeiter zur Verfügung gestellt. Die Revier- und Abteilungsleiter vor Ort haben mir bestätigt, dass allen Mitarbeitern die Regelungen zur Internetnutzung bekannt seien.

Die seinerzeit bestehende Standalone-PC-Lösung für die Internetnutzung wurde inzwischen abgelöst. Die eingesetzten Internetrechner werden jetzt zentral administriert und automatisiert gewartet. Es wurde ein zweistufiges Anmeldeverfahren implementiert. Die Mitarbeiter haben keine Administrationsrechte mehr. Entgegen meiner Empfehlung, externe Medien, wie z.B. CD-Laufwerke, zu deaktivieren und USB-Schnittstellen zu sperren, sind diese allerdings weiterhin uneingeschränkt zur Nutzung freigegeben worden.

Meine Prüfung der Festplatteninhalte hat ergeben, dass aufgrund der vorgefundenen Dateien und Cookies auf eine private Nutzung zu schließen ist. So sind beispielsweise PC-Spiele, ein Programm zur Musikbearbeitung, Kirchengemeindebriefe und Dokumentationen zu Ausbildungsberufen vorgefunden worden, wie auch zahlreiche Bilddateien mit Familienfotos, Tierfotos, Grundrisse von Häusern, Skulpturen, Rasenmähern, Grillbauten, Motorrädern, Angeln, Fußballveranstaltungen sowie Cookies von Urlaubsgebieten, Videoportalen, Mitfahrzentralen, Veranstaltungsportalen und Interneteinkaufsshops.

Bei einigen Programmen ist derzeit noch unklar, ob diese in Kenntnis und mit Zustimmung der Abteilung Informations- und Kommunikationstechnik heruntergeladen worden sind. Hierbei handelt es sich u. a. um Google Earth, einen freien Virenschanner, Bildbetrachtungsprogramme, Tools für den Einsatz von Festplatten und USB-Sticks sowie Software zum Brennen von CDs.

An unzulässigen dienstlichen Daten habe ich Bilder einer Überwachungskamera vorgefunden. Außerdem sind auf einem Rechner Personalstatistiken der Polizei Bremen bearbeitet worden.

Die private Nutzung des Internets stellt einen klaren Verstoß gegen die Dienstanweisung dar. Nach Ziffer 3.5 ist eine private Nutzung unzulässig. Aber selbst, wenn in Zukunft die private Nutzung bei der Polizei Bremen gestattet werden sollte, ist zu beachten, dass nach Ziffer 4 Absatz 3 der Richtlinie für die Bereitstellung und Nutzung von Internet-/Intranetzugängen vom 1. Februar 2004 (BremABI. Nr. 20 vom 10. Februar 2004) das Handeln der Mitarbeiter der Polizei Bremen insofern unzulässig wäre, als dass hier Dateien, wie z. B. PC-Spiele, und andere ausführbare Dateien heruntergeladen worden sind.

Die Installation bzw. das Herunterladen von nicht zugelassen Programmen und Dateien kann die Sicherheit des Systems gefährden. Der geplante Einsatz des Programms Fundinfo bei der Polizei Bremen ist so lange datenschutzrechtlich bedenklich, wie nicht sichergestellt ist, dass eine solche Nutzung der Rechner unterbleibt. Die Mitarbeiter müssen daher nochmals im Hinblick auf den Umgang mit dem Internet und den damit verbundenen Gefahren sensibilisiert werden.

Bereits bei der letzten Prüfung der Internetrechner habe ich darauf gedrungen, dass keine dienstlichen personenbezogenen Daten auf den Internetrechnern gespeichert werden. Wegen der besonderen Risiken bei der Nutzung des Internets (z. B. Verlust der Vertraulichkeit und der Integrität) ist nach Ziffer 6. der Dienstanweisung für die Nutzung des Internets der Polizei Bremen das Speichern von Daten mit dienstlichem Bezug auf Internetrechnern nicht gestattet. Es sollte daher nochmals

darauf hingewirkt werden, zukünftig eine Speicherung personenbezogener dienstlicher Daten auf diesen Rechnern zu verhindern.

Da in keinem Fall eine Begründung für eine Nutzung externer Medien genannt werden konnte, empfehle ich, die Medien zu deaktivieren und nur in konkreten Einzelfällen eine dedizierte Nutzung der USB-Schnittstelle zu erlauben.

Meine Prüfberichte habe ich der Polizei Bremen übersandt. Eine Stellungnahme steht aus.

9.8 PIER

PIER steht für Polizeiliche Information Ermittlung Recherche. Dieses Verfahren soll der Polizei Bremen bei komplexen Ermittlungen zur Seite stehen und insbesondere Beziehungen zwischen verschiedenen Personengruppen visualisieren.

Das System PIER ist mandantenfähig. Geplant sind zwei Mandanten. Wie unter Ziffer 9.9 dieses Jahresberichts beschrieben, werden die Sexualstraftäter aus dem Verfahren HEADS (Haft-Entlassenen-Auskunfts-Datei-Sexualstraftäter) als ein Bestandteil in PIER gespeichert. Dies soll in dem einen Mandanten erfolgen, in dem auch weitere Daten, z. B. vom Staatsschutz, bearbeitet werden. Insofern ist datenschutztechnisch durch Berechtigungen eine strikte Abgrenzung erforderlich, die sicherstellt, dass nur auf die erforderlichen Daten in dem jeweiligen Verfahren zugegriffen werden kann. Aus dem Berechtigungskonzept geht hervor, dass es unterschiedliche Rollen (z. B. Administrator, Sachbearbeiter, Dolmetscher) gibt. Es ist zurzeit unklar, ob diese strikte Trennung innerhalb eines Mandanten eingehalten werden kann bzw. wie groß das Risiko ist, dass durch fehlerhafte Berechtigungsvergabe auf sensible Daten eines anderen Moduls innerhalb eines Mandanten zugegriffen werden kann. Eine klare Trennung zwischen den Modulen Staatsschutz und HEADS wäre aus datenschutzrechtlicher Sicht die bessere Lösung.

Eine besondere Funktion dieses Programms ist die Meldungskonfiguration. Sollte in einem Verfahren ein Täter in PIER erfasst werden, der bereits in einem anderen Verfahren in PIER erfasst worden ist, so werden grundsätzlich Meldungen an die beteiligten Verfahren (auch zwischen den beiden Mandanten) generiert. In dem Mandanten, in dem die Daten von HEADS und dem Staatsschutz gespeichert sind, ist durch geeignete Konfiguration sicherzustellen, dass keine Meldungen aus diesem Mandanten in den anderen Mandanten erfolgen.

Zu einer ersten Version der Verfahrensbeschreibung von PIER hatte ich bereits im Juli 2008 Stellung genommen. Aus technischer Sicht habe ich angemerkt, dass noch Angaben zur Zugangs- und Zugriffskontrolle, zur Eingabekontrolle und der Verfügbarkeitskontrolle zu machen sind. Die Verfahrensbeschreibung, die Erfassungsrichtlinien und das Berechtigungskonzept wurden mir Ende September 2008 in aktualisierter Form vorgelegt und werden derzeit durch mich geprüft. Die Inhalte der Protokollierung sowie die Protokollierungsfristen befinden sich noch in der Abstimmung mit mir.

9.9 HEADS

HEADS ist eine Kurzbezeichnung für Haft-Entlassenen-Auskunfts-Datei-Sexualstraftäter. Sinn und Zweck dieser Datei ist die Überwachung rückfallgefährdeter Sexualstraftäter. HEADS zielt auf den Schutz der Bevölkerung durch eine Minimierung des Risikos einer erneuten Begehung von Straftaten von als besonders rückfallgefährdet eingestuften Sexualstraftätern. Dies soll durch eine Verbesserung

des Informationsaustausches zwischen Polizei und Justiz erreicht werden. Beispielsweise soll die Zusammenarbeit zwischen Vollstreckungsbehörde, Justiz-/Maßregelvollzug, Führungsaufsichtsstelle und Bewährungshilfe sowie Polizeibehörden optimiert werden. Dieser Informationsaustausch zwischen Polizei und Justiz beruht auf einem Datenübermittlungs- und Datenverarbeitungsprozess. Zum Konzept dieser Datei habe ich gegenüber dem Senator für Inneres und Sport Stellung genommen. Grundsätzliche rechtliche Bedenken gegen die Einführung dieser Datei habe ich nicht. HEADS wird in PIER (Polizeiliche Informationen Ermittlung Recherche (vgl. Ziff. 9.8 dieses Berichts) geführt.

9.10 ZAKS

Die Zentrale Antikorruptionsstelle (ZAKS) beim Senator für Inneres und Sport ist eine Stelle, bei der jeder Verdacht auf Korruption gemeldet werden kann.

Die Homepage der ZAKS bietet die Möglichkeit, Mitteilungen an die ZAKS per Kontaktformular auf dem E-Mail-Weg zu senden. Hierbei handelt es sich um einen unverschlüsselten Übertragungsweg. Die Hinweisgeberin oder der Hinweisgeber wird nicht darüber informiert, dass es sich um eine unsichere Verbindung handelt, die nicht gegen unbefugte Lesezugriffe auf dem Übertragungsweg geschützt ist. Ich habe nachdrücklich eine Verschlüsselung empfohlen.

9.11 Keine Ermittlungen von Polizeibeamten in eigener Sache

Im Jahr 2008 beschäftigte ich mich weiterhin mit der Thematik unbefugter Abrufe von Polizeibeamten aus dem polizeilichen Informationssystem (ISA-Web) sowie unzulässiger Ermittlungen von Polizeibeamten (vgl. 30. JB, Ziff. 9.5). Abfragen aus dem polizeilichen Informationssystem und Ermittlungen dürfen gemäß § 20 Bremisches Verwaltungsverfahrensgesetz (BremVwVfG) nicht von einem Polizisten vorgenommen werden, der selbst betroffen oder beteiligt ist oder ein Angehöriger eines Beteiligten ist. Betroffen ist ein Polizeibeamter, wenn er außerhalb seiner amtlichen Eigenschaft als Polizist auf sonstige Art und Weise eine Beziehung zur Sache hat. Hierzu zählt z. B. auch die ehrenamtliche Tätigkeit oder Mitgliedschaft in einem Verein. Gründe für die Unzulässigkeit von Abfragen aus ISA-Web oder von Ermittlungen liegen in der Befangenheit und Parteilichkeit des Polizeibeamten. Abfragen aus dem polizeilichen Informationssystem oder Ermittlungen zur Ahndung einer Ordnungswidrigkeit oder Verfolgung einer Straftat, die ein befangener Polizeibeamter durchführt, sind daher unzulässig. Ich habe mich daher mit dem Polizeipräsidenten darauf geeinigt, dass dieser alle Polizeibeamten in Bremen noch einmal auf diese Rechtslage hinweist. Dies ist mit Anweisung vom November 2008 geschehen. Entsprechend habe ich auch die Polizei in Bremerhaven informiert.

9.12 Eingaben im Bereich der Polizei von Bremen und Bremerhaven

Die Eingaben von Bürgern über die Verarbeitung ihrer Daten im polizeilichen Informationssystem haben in den vergangenen Jahren zugenommen. Ich konnte verschiedenen Bürgern helfen, ihre Rechte auf Auskunft, Berichtigung oder Löschung durchzusetzen.

In einem Fall kam es zu einer Verwechslung von Familienangehörigen aufgrund der Namensähnlichkeit. Der Sohn wurde trotz unterschiedlichen Alters und unterschiedlichen Geburtsnamens mit seinem Vater verwechselt. Daten, die den Vater betrafen, wurden beim Sohn

gespeichert; sie waren in dem polizeilichen Informationssystem zu löschen. Hier wurde eine Löschung bzw. Berichtigung dieser Einträge durch mich erreicht.

In einem anderen Fall kam ein Petent zu mir und bat um die Löschung kriminalpolizeilicher Daten aus dem polizeilichen Informationssystem ISA-Web. Die Polizei Bremerhaven sah den Zeitpunkt der Verurteilung als für die Fristberechnung maßgeblich an. Fristbeginn ist aber der Tatzeitpunkt und damit die Erfassung bei der Polizei und nicht die Verurteilung, denn die Strafverfahrensdauer darf dem Betroffenen nicht zum Nachteil gereichen. Eine Stellungnahme steht noch aus.

Einer weiteren Beschwerde lag ein Wortgefecht zwischen Bürgern auf offener Straße zugrunde. In dieser Auseinandersetzung behauptete eine Bürgerin, alles über den anderen Bürger zu wissen, denn sie arbeite schließlich bei der Polizei. Ich ging dessen Beschwerde nach. Meine Prüfung ergab, dass die Bürgerin zwar in den Räumen der Polizei arbeitet, es wurde aber keine unbefugte Abfrage in der kriminalpolizeilichen Sammlung vorgenommen.

9.13 Rechtewahrung in gemeinsam genutzten Laufwerken bei der Polizei

Bremen

Im Berichtsjahr 2004 bin ich im Rahmen von datenschutzrechtlichen Prüfungen bei der Polizei Bremen auf ein sogenanntes öffentliches Laufwerk aufmerksam geworden, das zum Datenaustausch und zur organisationsübergreifenden Sachbearbeitung betrieben worden ist. Meine datenschutzrechtliche Auffassung habe ich im 27. Jahresbericht unter Ziffer 6.2 dargestellt. Seinerzeit wurde ein öffentliches Laufwerk genutzt, für das es kein Datenschutzkonzept gab. Die Daten konnten von der gesamten Polizei Bremen eingesehen werden, und es gab keine Regelung zur Löschung der dort gespeicherten Dateien. Die danach durch die Polizei Bremen neu geschaffenen Regelungen habe ich in diesem Jahr geprüft.

Die Polizei Bremen hat zwei zentrale Laufwerke eingerichtet. Zum einen steht für Dateien, die aufgrund der Größe nicht über das E-Mail-System ausgetauscht werden sollen, ein öffentliches Laufwerk zur Verfügung. Um zu verhindern, dass Daten über einen längeren Zeitraum ungelöscht gespeichert bleiben, soll wöchentlich automatisiert die Löschung aller hier noch verbliebenen Dateien erfolgen. In diesem Speicherbereich befanden sich zum Zeitpunkt der Prüfung nur wenige Dateien, die jünger waren als das Datum des letzten Löschvorgangs. Die vorgeschriebene Löschung wurde eingehalten.

Zum anderen ist ein Laufwerk eingerichtet worden für Datenzugriffe, die organisationsübergreifend von Mitarbeitern aus mehreren Sachgebieten erfolgen müssen und auf dem jeder Direktion ein eigenes Verzeichnis zugeordnet worden ist.

Die Vergabe von Berechtigungen für diese Unterverzeichnisse ist auf die Direktionen delegiert worden. Jede Direktion hat für diese Aufgabe einen oder mehrere Verantwortliche bestimmt. Die Verantwortlichen haben Vollzugriff und können weitere Unterverzeichnisse anlegen sowie Mitarbeiter zur Nutzung zuordnen.

In der von der Abteilung IuK erstellten Dokumentation wird darauf hingewiesen, dass die Verantwortlichen für ihre Arbeit dokumentationspflichtig sind, dass diese Dokumentation Bestandteil der IT-Revision sein kann und auch aus Datenschutzgründen erforderlich ist.

Ich habe bzgl. der Berechtigungsvergabe kritisiert, dass es keine technischen Möglichkeiten einer reversionssicheren Protokollierung gibt. Die Überprüfung der Dokumentation über die Vergabe der Zugriffsberechtigung auf Verzeichnisse in einer Fachdirektion hat ergeben, dass es keine vollständigen Unterlagen darüber gab, wie die Berechtigungen vergeben worden sind.

Ich habe der Polizei Bremen bereits in 2007 empfohlen, ein Werkzeug zur Dokumentation des Istzustands für die Berechtigungseinstellungen zu nutzen. Auf diese Weise können zunächst einmal grundsätzliche Überprüfungen kritischer Zustände (Vergabe Vollzugriff, Zugriff für Jedermann) durchgeführt werden.

Weiterhin besteht die Möglichkeit, dass anhand dieser Dokumentation die Direktionen zu einer regelmäßigen Überprüfung der aktuellen Berechtigungen angehalten werden. Unklare Berechtigungsvergaben sollen anhand der vollständigen Aufbewahrung der Anträge geklärt werden.

Die Polizei Bremen hat mitgeteilt, dass sie mittlerweile den Istzustand über ein Snapshotverfahren rudimentär speichert. Diese Dokumentation ist allerdings auch für einen Soll-/Istvergleich der Berechtigungen nur sehr eingeschränkt verwendbar. Daher ist die Polizei Bremen in Kontakt mit dem Hersteller ihres proprietären Betriebssystems getreten, um eine brauchbare Dokumentationslösung zu erhalten.

Diese Vorgehensweise stellt insgesamt eine schwächere Form gegenüber einer automatisierten Protokollierung dar.

9.14 Das normenverdeutlichende Gespräch mit Kindern und Jugendlichen

Die Polizei Bremen möchte Gespräche mit Kindern und jugendlichen Ersttätern führen, um den Minderjährigen das Unrecht der Tat vor Augen zu führen. Auch deren Erziehungsberechtigte sollen mit einbezogen werden, um diese auf ihre Verantwortung im Sozialisierungsprozess hinzuweisen und sie zur Wahrnehmung ihrer Pflichten gemäß Art. 6 Grundgesetz (GG), § 171 Strafgesetzbuch (StGB) und §§ 52 bis 58 Bremisches Schulgesetz (BremSchulG) anzuhalten. Vor den Gesprächen möchte die Polizei die kriminalpolizeilichen Informationssysteme abfragen und dabei neben den Kindern und jugendlichen Ersttätern auch die Eltern überprüfen. Über Art und Ausgestaltung des Verfahrens finden derzeit Gespräche mit der Polizei statt.

9.15 ViCLAS-Datenbank des Bundeskriminalamtes

Auch in diesem Jahr ist mir vom Bundesministerium des Innern die Errichtungsanordnung „ViCLAS“ zur automatisierten Datei mit personenbezogenen Daten beim Bundeskriminalamt (§ 34 BKAG) zur Stellungnahme gegenüber dem Senator für Inneres und Sport übersandt worden. Derzeit findet grundsätzlich eine lokale Speicherung von Daten über Straftaten von Kindern in der kriminalpolizeilichen Sammlung statt, die das 7. Lebensjahr vollendet haben. Die ViCLAS-Datenbank ist ein Instrument zur Abbildung von Straftaten und Täterverhalten im Bereich der sexuell motivierten Gewaltkriminalität (Tötungs- und Sexualdelikte). In dieser bundesweiten Verbunddatei sollen Kinder als Täter gespeichert werden. Ich habe Bedenken gegen die Eröffnung einer bundesweiten Zugriffsmöglichkeit auf die dort gespeicherten Daten von Kindern, weil bisher nicht hinreichend nachgewiesen ist, dass die in Rede stehenden Kinder überörtlich tätig werden. Ich habe mich daher mangels rechtlicher Erforderlichkeit gegen die Erweiterung der Speicherung von Daten über strafunmündigen Kindern auf Bundesebene ausgesprochen.

9.16 Bericht aus dem Arbeitskreis Sicherheit

Der Arbeitskreis Sicherheit der Datenschutzbeauftragten des Bundes und der Länder dient dem Erfahrungs- und Informationsaustausch. Aus der Fülle der Themen seien folgende exemplarisch genannt: HEADS (Haft-Entlassenen-Auskunfts-Datei-rückfallgefährdeter-Sexualstraftäter, [vgl. Ziff. 9.9 dieses Berichts]), die Zuverlässigkeitsüberprüfungen, die polizeiliche Überwachung von Internetknotenpunkten, der Datenschutz in der polizeilichen und justiziellen Zusammenarbeit auf europäischer Ebene, das Bundeskriminalamtgesetz (vgl. Ziff. 20.1), die Antiterrordatei (vgl. Ziff. 9.18) , die Praxis der Auskunftserteilung durch die Polizei und die Auskunftspraxis bei den Verfassungsschutzbehörden.

9.17 Onlinedurchsuchung privater Computer

Bahnbrechend ist die Entscheidung des Bundesverfassungsgerichts (BVerfG) vom 27. Februar 2008 (Az. 1 BvR 370/07; 1 BvR 595/07) zur Onlinedurchsuchung. Gegenstand des Verfahrens vor dem BVerfG waren Verfassungsbeschwerden gegen das Gesetz über den Verfassungsschutz in Nordrhein-Westfalen, welches zum einen Befugnisse der Verfassungsschutzbehörde zu verschiedenen Datenerhebungen aus informationstechnischen Systemen, gemeint sind insbesondere private Computer, zum anderen den Umgang mit den erhobenen Daten vorsah. Im Fokus ist eine Vorschrift, die zum heimlichen Zugriff auf informationstechnische Systeme ermächtigt, die sogenannte Onlinedurchsuchung.

Das BVerfG hat diese Vorschrift für „verfassungswidrig und nichtig“ (Rn. 165) erklärt. Die Vorschrift zur Onlinedurchsuchung verletze das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz [GG]) in seiner besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Rn. 166). Diese Ausprägung des allgemeinen Persönlichkeitsrechts schützt vor Eingriffen in informationstechnische Systeme, soweit der Schutz nicht durch andere Grundrechte wie Art. 10 GG (Telekommunikationsgeheimnis), Art. 13 GG (Unverletzlichkeit der Wohnung) oder durch das Recht auf informationelle Selbstbestimmung gewährleistet ist (Rn. 167). Das BVerfG stellt fest, dass die Vorschrift zur Onlinedurchsuchung nicht dem Gebot der Normenklarheit genügt (Rn. 208), die Anforderungen des Verhältnismäßigkeitsgrundsatzes nicht gewahrt sind (Rn. 218) und die Norm keine hinreichenden Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung enthält (Rn. 167). Das BVerfG entwickelte damit ein neues Grundrecht auf Gewährleistung und Integrität informationstechnischer Systeme (Rn. 201), um den neuartigen Gefährdungen im Zuge des informationstechnischen Fortschritts und gewandelter Lebensverhältnisse Rechnung zu tragen (Rn. 169 und 187). Es dient dem Schutz der Privatsphäre. Die Anforderungen, die das BVerfG aufstellt, wie zum Beispiel die Verfahrensvorkehrungen, der Vorbehalt richterlicher Anordnung, haben auch Geltung für den Gesetzentwurf zur Abwehr des internationalen Terrorismus (vgl. Ziff. 9.19 dieses Berichts).

9.18 Prüfung der Antiterrordatei

Im September und Oktober 2008 habe ich eine Ergänzungsprüfung der Antiterrordatei beim Landeskriminalamt (LKA) und beim Landesamt für Verfassungsschutz (LfV) durchgeführt (vgl. 30. JB, Ziff. 9.6). Eine Aktualisierung der Antiterrordatei findet wöchentlich statt. Ich habe stichprobenartig verschiedene Datensätze überprüft. Des Weiteren habe ich das Verfahren bei Abrufen und Eilabrufen

von Bundesbehörden hinsichtlich erweiterter Grunddaten im Sinne des Antiterrordateigesetzes (ATDG) vom 22. Dezember 2006 kontrolliert. Von der Einhaltung der Vorgaben des ATDG habe ich mich vor Ort überzeugt. Eine Kontrolle der Protokolldaten steht noch aus.

9.19 Abwehr des internationalen Terrorismus

Der Gesetzentwurf zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt (BKAG-E; BT-Drs. 16/9588, 16/10121 und 16/10822) führte zu heftigen Diskussionen. Wesentliche Kritikpunkte, die u. a. auch vom Deutschen Anwaltverein, der Bundesrechtsanwaltskammer und vom Deutschen Journalisten-Verband vorgebracht werden, bestehen in der Ausweitung der präventiven Befugnisse des Bundeskriminalamts (BKA). Ermächtigungen, wie zum Beispiel die Rasterfahndung (vgl. 29. JB, Ziff. 9.2), die Onlinedurchsuchung von privaten PC (vgl. Ziff. 9.17 dieses Berichts), der Spähangriff in Wohnungen oder die Herausgabepflicht von Daten der Informanten durch Journalisten, sind unangemessen. Bedenken bestehen darüber hinaus hinsichtlich der Datenvorsorge zur Verfolgung künftiger Straftaten. Der Schutz von Daten aus dem Kernbereich privater Lebensgestaltung wird faktisch, beispielsweise durch die Regelung über Lausch- und Spähangriffe gemäß § 20 h Abs. 5 BKAG-E, unterlaufen.

Als weiterer grundsätzlicher Kritikpunkt wird die Verschiebung der Sicherheitsarchitektur genannt. Die Grenzen zwischen nachrichtendienstlichen Erkenntnissen und kriminalpolizeilichen Prognosen und Handlungsgrundlagen werden verwischt. Dies wird auch als sogenannte Vernachrichtlichung bezeichnet. An dieser Stelle wird gegen das verfassungsrechtliche, rechtsstaatliche Trennungsgebot verstoßen. Kritik muss auch an der Unbestimmtheit und damit der mangelnden Normenklarheit geübt werden. Der Begriff des internationalen Terrorismus wird nicht gesetzlich definiert. Die Zuständigkeiten von BKA und LKA können nicht klar abgegrenzt werden. Parallelzuständigkeiten und damit einhergehende Ermittlungsspannen sind zu befürchten. Die Evaluierung von fünf Jahren ist zu lang. Stattdessen ist eine Befristung der Befugnisse anzustreben. Abgeordnete von Oppositionsparteien haben Verfassungsbeschwerden gegen diesen Gesetzentwurf angekündigt.

9.20 Unfalldatenschreiber bei der Feuerwehr

Bei der Feuerwehr in Bremen und Bremerhaven werden sogenannte Unfalldatenspeicher (UDS) eingesetzt. Ein Unfalldatenspeicher ist ein Gerät, welches bei Inbetriebnahme des Rettungsfahrzeugs permanent und uhrzeitgenau Fahrzeugbewegungen, Stellung bzw. Bedienung angeschlossener Bedienelemente erfasst und interne Vorgänge überwacht.

Die Einführung dieser Geräte habe ich in 2005 bei der Feuerwehr in Bremen begleitet (vgl. 28. JB, Ziff. 9.13). Nach einem Probetrieb habe ich Ende 2006 die Überprüfung der technischen und organisatorischen Maßnahmen bei der Feuerwehr Bremen vorgenommen. Daraus ergaben sich einige Forderungen zur Verbesserung des Datenschutzes, beispielsweise eine Festplattenverschlüsselung für das Notebook, Vorgaben zur Protokollierung und zum Anmeldeverfahren, dessen Umsetzung die Feuerwehr Bremen nachträglich vornahm. Eine Überprüfung der Ereignisdaten des UDS konnte seinerzeit nicht vorgenommen werden, da diese inkonsistent waren. Eine nachträgliche Kontrolle dieser Ereignisdaten bei der Feuerwehr in Bremen fand im Juli 2008 statt. Der zum Auslesen eines UDS erforderliche Laptop wurde verschlossen aufbewahrt und enthielt die ausgelesenen Daten sowie die erforderliche Software. Die Auswertung der

Ereignisdaten, wie zum Beispiel Blaulicht, Blinker rechts/links, Bremse und Sirene im Statistikspeicher, automatischen Speicher und Stillstandspeicher, ergab, dass bisher kein Auslesen stattfand und die Daten konsistent waren.

Ein besonderes Augenmerk richtete ich auf rechtliche Fragen des Arbeitnehmerdatenschutzes. Durch das Auslesen der Daten eines UDS können Verhaltensanalysen hinsichtlich der im Rettungsdienst tätigen Fahrerinnen und Fahrer durchgeführt werden. Ein Auslesen zu diesem Zweck ist nicht erlaubt. Durch Dienstvereinbarungen bei den Feuerwehren in Bremen und Bremerhaven sowie bei den verschiedenen Rettungsdiensten Arbeiter-Samariter-Bund, Deutsches Rotes Kreuz und Malteser wird gewährleistet, dass ein Auslesen des UDS nicht ohne Kenntnis der Fahrerin bzw. des Fahrers des Rettungsfahrzeugs vorgenommen wird. Insofern wird dem Datenschutz für den Bereich der Arbeitnehmerinnen und Arbeitnehmer ausreichend Rechnung getragen.

9.21 Elektronischer Personalausweis kommt 2010

Der neue elektronische Personalausweis soll 2010 im Scheckkartenformat eingeführt werden. Die gesetzliche Grundlage ist das Gesetz über Personalausweise und den elektronischen Identitätsnachweis (PAG, BT-Drs. 16/10489 vom 7. Oktober 2008). Er vereint drei Funktionen in einem. Neben der bisher gebräuchlichen Ausweisfunktion, zum Beispiel für die Reise, treten die Identitätsfunktion für das E-Government und E-Business sowie optional die Signaturfunktion als elektronisches Pendant zur eigenhändigen Unterschrift. Der neue elektronische Personalausweis wird mit einem RFID-Chip versehen sein, auf dem die persönlichen Daten des Ausweisinhabers inklusive Lichtbild und auf Wunsch zwei Fingerabdrücke gespeichert werden. Es sind aber noch eine Reihe datenschutzrechtlicher Fragestellungen offen.

Aus dem Grobkonzept des Bundesministeriums des Innern (BMI) zum elektronischen Personalausweis (Version 2.0) geht hinsichtlich der Sicherheit der Biometriedaten nicht klar hervor, wie diese auf dem Chip gegen unberechtigtes Auslesen gesichert werden sollen. Hinsichtlich der Verwendung der Identitätsfunktion im Internet bestehen Gefahren durch Schadsoftware auf dem PC des Bürgers. Hier ist ein Abhören des Datenflusses oder ein Auslesen der PIN möglich. Zur Schadensminimierung darf die Kommunikation nur über eine gesicherte Datenleitung (Datenkanal) betrieben werden. Nicht geklärt ist, wer im Schadensfall haftet. Ein weiterer Kritikpunkt wird im Grobkonzept hinsichtlich der Integration von Zertifikaten und Schlüsseln beschrieben, die als eindeutige Personenkennzeichen für die Gültigkeitsdauer des Personalausweises verwendet werden können. Es sind Regelungen zur Seriennummer und äquivalente Vorkehrungen zum Schutz des allgemeinen Persönlichkeitsrechts zu treffen. Diese Vorkehrungen müssen näher bezeichnet werden. Des Weiteren muss geregelt sein, wie verfahren werden soll, wenn der RFID-Chip defekt ist. Die drei Funktionen des neuen Ausweises müssen datenschutztechnisch getrennt zur Verfügung gestellt werden. Gefahren bestehen im Hinblick auf die Manipulation von sehr sensiblen Daten, wie zum Beispiel das biometrische Lichtbild, und den Diebstahl von Identitäten. Des Weiteren habe ich zusammen mit den anderen Datenschutzbeauftragten des Bundes und der Länder datenschutzrechtliche Bedenken gegen die Speicherung der Fingerabdrücke auf dem RFID-Chip geäußert. Nach den Verhandlungen der Datenschutzbeauftragten mit dem BMI wurde diese Wahlmöglichkeit hinsichtlich der Speicherung von Fingerabdrücken erreicht.

9.22 Projekt „Unbarer Zahlungsverkehr“ für die Verwaltung

In der gesamten bremischen Verwaltung ist die Möglichkeit eines unbaren Zahlungsverkehrs geplant. Dabei soll mit externen Diensteanbietern zusammengearbeitet werden. Seit 2007 wird dieses Projekt (früher „Bargeldloser Zahlungsverkehr für Verwarnungen“) durch mich beraten.

Von besonderem Interesse ist, dass ein externer Provider beauftragt werden soll, sich um die Zahlungseingänge zu kümmern und bestimmte Zahlungsdaten zu archivieren. Diese Beauftragung zur Abwicklung des unbaren Zahlungsverkehrs stellt eine Auftragsdatenverarbeitung nach § 9 Bremisches Datenschutzgesetz (BremDSG) dar, dessen Vorgaben zu berücksichtigen sind. Die datenschutzrechtliche Verantwortlichkeit verbleibt gemäß §§ 9 Abs. 1 Satz 1, 2 Abs. 3 Nr. 1 BremDSG beim Auftraggeber. Konkret haben Auftragnehmer also mit den Auftragsunterlagen schriftlich darzustellen:

- die Datenverarbeitung (Geschäftsprozessmodellierung nebst Datenübermittlungen),
- ggf. die Unterauftragsverhältnisse (Einschaltung Dritter zur Auftragsabwicklung),
- die technischen und organisatorischen Maßnahmen nach § 7 BremDSG (z. B. in Gestalt eines IT-Sicherheitskonzepts oder Datenschutzkonzepts) und
- ggf. meine Kontrollmöglichkeiten sicherzustellen.

Die sichere Zahlungsabwicklung setzt verschiedene technische und organisatorische Maßnahmen des Auftragnehmers voraus. Hierzu gehören etwa die sichere Authentifizierung an Geräten und Software, eine verschlüsselte Übertragung der Zahlungsdaten sowie Plausibilitätsprüfungen und Protokollierungen. Zur Routine gehört es sicherzustellen, dass beim Auftragnehmer nur Befugte Zugang und Zutritt zu den Datenverarbeitungsanlagen und Zugriff auf die Abrechnungsdaten besitzen und dass Zugriffe revisionssicher protokolliert werden. Im Rahmen der Verfügbarkeitskontrolle ist zu gewährleisten, dass beispielsweise die Belege für die Speicherdauer zum Zwecke der Rechnungsprüfung lesbar bleiben.

Es ist durch geeignete Maßnahmen sicherzustellen, dass bei unbarer Zahlung zum Beispiel die Art der Verwarnung nicht elektronisch übermittelt wird oder gar auf dem Konto- oder Kreditkartenbeleg der Überweisenden erscheint. Der Zahlungsbeleg muss einem konkreten Vorgang zuordenbar bleiben, zum Beispiel bei Nachfragen des Bürgers oder zum Nachvollziehen der Verbuchung.

Es besteht ein schutzwürdiges Interesse der Betroffenen, nicht unter Verwendung unbarer Zahlungsmethoden bezahlen zu müssen, die weitere, möglicherweise ungewollte Datenspuren, zum Beispiel auf dem Konto oder der Kreditkartenabrechnung, auslösen. Den betroffenen Bürgern muss daneben eine bare und damit anonyme Zahlungsmöglichkeit verbleiben. Auf die Freiwilligkeit der unbaren Zahlung, die dann nur mit Einwilligung gemäß § 3 Abs. 3 und 4 BremDSG der Betroffenen erfolgen darf, ist in geeigneter Form hinzuweisen; dies geschieht in der Verwaltung regelmäßig per Dienstanweisung.