

9. Inneres

9.1 Videoüberwachung in Polizeifahrzeugen

Die Polizei Bremen hat derzeit 12 von 45 Fahrzeugen mit Videogeräten ausgestattet, die das Vorgehen der Beamten bei Anhalte- und Kontrollvorgängen im öffentlichen Verkehrsraum aufzeichnen. Ich wurde darüber im September diesen Jahres informiert. Es handelt sich hier um Videodaten zur Eigensicherung nach § 29 Abs. 5 Bremisches Polizeigesetz (BremPolG), d. h. um Leib und Leben der Polizeibeamten zu sichern.

Die Polizei Bremen legte mir eine entsprechende Dienstanweisung vor, die die Einzelheiten zur Ausführung des § 29 Abs. 5 BremPolG regelt. Ich habe mir die Datenverarbeitung vor Ort angesehen.

Die Aufzeichnung beginnt bei Einschalten der Anhaltebrücke mit dem „Stopp Polizei“-Signal oder durch manuelle Betätigung einer Bedientaste. Die Aufzeichnung endet nicht automatisch, sondern erst wieder bei Betätigung einer Bedientaste. Der Aufnahmebetrieb im Fahrzeug wird durch ein optisches Signal (rote Kontrollleuchte) angezeigt.

Der Betroffene soll, da es sich um eine Maßnahme mit Präventionscharakter handelt, die Angriffe verhindern soll, zusätzlich auf die Aufzeichnung hingewiesen werden. Auf Nachfrage soll Betroffenen und Dritten mitgeteilt werden, dass eine unverzügliche Löschung der Daten stattfindet, wie sie auch das Bremische Polizeigesetz vorsieht. Tatsächlich aber werden die Daten erst nach zwölf Stunden gelöscht bzw. überschrieben.

Eine Auswertung der Speicherkarten und Speicherung der Videodaten auf CD erfolgt ausschließlich auf schriftlichen Antrag. Das Gerät zum Beschreiben der Karten ist fest im Fahrzeug installiert und verschlossen. Ein Zugriff auf die Speicherkarten im Fahrzeug ist nur den Einsatzleitern der Wache mit einem speziellen Schlüssel möglich. Die Speicherkarten können an zentraler Stelle über ein spezielles Lesegerät, das an einem eigens dafür vorgesehenen Notebook angeschlossen ist, ausgelesen werden. Ein Auswählen von Bildsequenzen ist dabei nicht möglich. Die Aufzeichnung wird komplett übertragen und mit einer Signatur versehen, die nach Darstellung der Polizei Bremen beweissicher ist. Bei nachträglicher Veränderung von Videodaten wird die Signatur ungültig. Die Überprüfung dieser Signatur erfolgt mit einer speziell dafür vorgesehenen Software.

Da es sich hier um die automatisierte Verarbeitung personenbezogener Daten handelt, habe ich eine Verfahrensbeschreibung gefordert. Schwerpunktmäßig von Interesse ist aus technischer Sicht die Zugriffs- und Eingabekontrolle sowie das Verfahren zur Signierung der Videodaten, aus rechtlicher Sicht ist die „unverzügliche“ Löschung klärungsbedürftig. Zudem ist die Zweckbindung der Aufzeichnungen („zur Verfolgung von Straftaten, die sich gegen Polizeivollzugsbeamte gerichtet haben“) zu beachten. Die Aufzeichnungen dienen nicht dazu, (Verkehrs)Ordnungswidrigkeiten zu beweisen.

9.2 Videoüberwachung der „Discomeile“

Im Anschluss an die Vorfälle auf der sog. Discomeile Anfang des Jahres 2006 hat die Polizei Bremen ein Konzept zur Durchführung von Videoüberwachungsmaßnahmen nach § 29 Abs. 3, 4 Bremisches Polizeigesetz (BremPolG) erarbeitet. Im Juli 2006 erhielt ich die Angebote verschiedener Anbieter sowie den Vermerk einer Ortsbegehung zur Prüfung vorgelegt. In einem ersten Schreiben vom Juli 2006 wies ich darauf hin, dass vor der technischen Ausgestaltung der Maßnahme zunächst die Frage zu klären sei, ob überhaupt die gesetzlichen Voraussetzungen für eine Videoüberwachung vorliegen. Ich bat um weitere Informationen und wies auf einige ortsspezifische Einschränkungen hin (Schwärzen der Aufnahmebereiche von Privatwohnungen, unklare örtliche Reichweite, erhöhte Kriminalitätsbelastung an bestimmten Tagen und nur zu bestimmten Zeiten). Im Dezember 2006 stellte die Polizei Bremen mir ihr technisches Konzept vor und übersandte im Vorfeld den Entwurf einer Verfahrensbeschreibung. Einsatztaktisch wurde dabei eine 24-stündige Überwachung vorgesehen. Erneut wies ich auf die Betroffenheit von Grundrechten der Anwohner (Geschäfte und Privatwohnungen) hin und den ausstehenden Nachweis der erhöhten Kriminalitätsbelastung rund um die Uhr.

Ende Januar 2007 wurde mir der Entwurf der Deputationsvorlage zur stationären Videoüberwachung an der „Discomeile“ zugeleitet. In meiner Stellungnahme wies ich auf verschiedene technische Fragen hin, etwa zur Datenübertragung und Datensicherheit, die noch offen waren. Zudem enthielt die Deputationsvorlage vielfältige weitere Mängel, z. B. eine falsche Rechtsgrundlage und Zielsetzung und legte teilweise falsche tatsächliche Angaben zugrunde, die ich korrigierte. Auch ging die geplante Überwachung örtlich über die „Discomeile“ hinaus und sollte von 18.00 Uhr bis 10.00 Uhr am Folgetag andauern. Hier erreichte ich eine örtliche und zeitliche Einschränkung auf die „Discomeile“ und die Zeiten von 20.00 Uhr bis 8.00 Uhr am Folgetag, d. h. vor allem außerhalb der normalen Ladenöffnungszeiten.

Im November 2007, nachdem die Polizei Bremen etliche technische Probleme gelöst hatte, nahm ich erneut zu dem gewählten technischen Konzept Stellung und stellte konkrete Sicherheitsanforderungen. Auch wurde ich an der Ausgestaltung der Schilder und deren Standort beteiligt, die einen besonders wichtigen Aspekt für die Erkennbarkeit der Maßnahme und damit der Transparenz für die Betroffenen bedeuten. Am 21. Dezember 2007 begann die Videoüberwachung. Es ist geplant, ihren Einsatz im Jahr 2008 vor Ort bei der Polizei Bremen zu überprüfen.

9.3 Einsatzleitzentrale in Bremen

Im Dezember 2005 habe ich den Einsatz von Softwareprodukten bei der Einsatzleitzentrale der Polizei Bremen vor Ort angesehen. Das Produkt FELIS - „Flexibles Einsatzleitsystem Innere Sicherheit“ - wird eingesetzt zur Erfassung und Dokumentation von Notrufen. Dabei wird die von der Telefonanlage übermittelte Rufnummer bei Eingang eines Notrufs automatisch in die formulargestützte Notruferfassung aufgenommen. Der Bearbeiter ergänzt diese Daten und leitet sie an den Funksprecher zur Koordinierung der Einsätze weiter. Darüber hinaus werden die Gespräche der Einsatzleitzentrale aufgezeichnet und sollen für einen Zeitraum von drei Monaten gespeichert werden.

Eine Verfahrensbeschreibung, wie sie nach § 8 BremDSG erforderlich ist und die die getroffenen Sicherheitsmaßnahmen beschreibt, lag zu diesem Zeitpunkt nicht vor und wurde im Januar 2006 mit Übermittlung meines Berichts zur Ortsbesichtigung angefordert.

Die Ausfertigung und Übersendung der gesetzlich vorgeschriebenen Unterlagen wurde mit dem Hinweis auf technische Umstellungen verschoben. Nach mehreren Erinnerungen übersandte die Polizei Bremen mir ein Jahr später, Ende Januar 2007, eine erste Verfahrensbeschreibung. Ich nahm noch im gleichen Monat dazu Stellung. Die technischen und organisatorischen Maßnahmen wurden nicht vollständig und nur rudimentär beschrieben. Ich habe daher nochmals um ergänzende Angaben gebeten sowie nach dem Ergebnis der Vorabkontrolle, die durch den behördlichen Datenschutzbeauftragten durchgeführt werden muss.

Nachdem weitere zehn Monate vergangen waren und ich trotz wiederholter Erinnerungen und Rücksprachen keine weiteren Informationen erhalten habe, habe ich mich an den Polizeipräsidenten gewandt. Im Januar 2008 habe ich eine angepasste Verfahrensbeschreibung erhalten, die ich derzeit prüfe.

9.4 Automatische Kennzeichenerfassung

Der Polizeivollzugsdienst darf bei Kontrollen im öffentlichen Verkehrsraum durch den offenen Einsatz technischer Mittel zur elektronischen Erkennung von Kfz-Kennzeichen personenbezogene Daten zum Zwecke des sofortigen automatischen Abgleichs mit dem Fahndungsbestand erheben. Dies wurde durch Änderung des Bremischen Polizeigesetzes (BremPolG) vom 23. Februar 2006 (dort § 29 Abs. 6) möglich.

Durch Anfragen der Presse bin ich darauf aufmerksam gemacht worden, dass die Polizei Bremen Kennzeichenlesegeräte testet. Ich habe den behördlichen Datenschutzbeauftragten der Polizei Bremen um Mitteilung gebeten, in welchem Zeitraum die Testphase durchgeführt wird und habe einen kurzfristigen Prüftermin innerhalb der Testphase wahrgenommen. Die Polizei Bremen testete zwei verschiedene Geräte nebst Software. Die ersten Tests fanden im Rahmen von Verkehrskontrollen statt und waren bereits abgeschlossen. Für die Vergleiche der Kennzeichen der vorbeifahrenden Kraftfahrzeuge mit sogenannten Fahndungsnotierungen wurden Datenbestände des polizeilichen Informationssystems des BKA (INPOL) und Auszüge aus dem des Schengener Informationssystems (SIS) verwendet.

Das bei dem Prüftermin vorgeführte Fahrzeug war mit einer Videokamera ausgestattet, die mit einem mobilen Notebook verbunden wurde, auf dem die benannten Datenbestände gespeichert worden sind. Die Kamera lieferte Videobilder der vorbeifahrenden Fahrzeuge. Der Fahrer des vorbeifahrenden Fahrzeugs war dabei nicht erkennbar. Das Kennzeichen wurde mehrfach beim Heranfahren aus unterschiedlicher Entfernung (z. B. 50, 20, 10 Meter) von dem System gelesen (Erkennungssicherheit ca. 85 – 96 %). Die Software zeigte dabei in einem Windows-Fenster das gelesene Kennzeichen an. Die letzten elf Kennzeichen standen zur Ansicht in einem weiteren Windows-Fenster zur Verfügung. Ein Sichtvergleich der durch die Software gelesenen Kennzeichen mit dem tatsächlichen Fahrzeug ergab zu diesem Zeitpunkt keine Fehler.

In der getesteten Software gab es verschiedene Konfigurationsmöglichkeiten zur Bildspeicherung. Es konnte definiert werden, dass kein Bild gespeichert wird, dass alle Bilder gespeichert werden (z. B. im Rahmen einer Ringfahndung) oder dass nur die „Treffer“ gespeichert werden. Beim Test war die Einstellung „Treffer speichern“ eingestellt. Im Falle eines konkreten Einsatzes ist organisatorisch und technisch sicherzustellen, dass jeweils nur die für den Einsatz erforderliche Software aktiviert werden kann.

In diesen ersten Tests hat es Probleme beim Lesen der Kennzeichen gegeben, u. a. durch nicht reflektierende ausländische Kennzeichen (z. B. in Mittel- und Osteuropa keine Pflicht), durch Verschmutzung oder Beulen in Kennzeichen sowie durch schlechte Lichtverhältnisse.

Ich habe gegenüber der Polizei Bremen deutlich gemacht, dass bei Einsatz einer automatischen Kennzeichenüberwachung eine Verfahrensbeschreibung zu erstellen ist. Dabei sind insbesondere die technischen und organisatorischen Maßnahmen (z. B. Festplattenverschlüsselung, Kennwörter, sichere Aufbewahrung) zu benennen. Hier ist ein besonderer Schutz vorzusehen, da das Notebook den aktuellen INPOL- und Schengen-Fahndungsbestand und damit äußerst sensible Daten enthält.

Im Anschluss an die Demonstration der automatischen Kennzeichenüberwachung wurde vereinbart, dass die Polizei Bremen mich über den weiteren Verlauf der Tests und das Ergebnis informiert. Im März 2007 teilte mir der behördliche Datenschutzbeauftragte der Polizei Bremen mit, dass eine Realisierung der Maßnahme aus Kostengründen derzeit nicht weiter verfolgt und die Angelegenheit zu einem späteren Zeitpunkt wieder aufgegriffen werde. Insoweit kann die verfassungsrechtliche Debatte über die Zulässigkeit dieses Instruments abgewartet werden.

9.5 Eingaben im Bereich der Polizeien des Landes Bremen

Auch im vergangenen Jahr erreichten mich wieder eine Vielzahl von Eingaben, die die Polizei betrafen. Wenige möchte ich exemplarisch darstellen. Verschiedentlich habe ich Betroffene bei der Ausübung ihres Rechts auf Auskunft, Berichtigung, Sperrung und Löschung ihrer bei der Polizei Bremen gespeicherten personenbezogenen Daten unterstützt. So erreichte ich die Löschung von Einträgen, beispielsweise weil sich aus dem Einstellungsbescheid der Staatsanwaltschaft ergab, dass bereits der Tatbestand des angezeigten Delikts nicht erfüllt war oder Betroffene, die Zeugen gewesen waren, versehentlich als Tatverdächtige aufgeführt wurden.

In einem Fall stellte ich bei meiner Prüfung fest, dass ein Petent aufgrund des Inhalts von vier Schreiben, die er an den Polizeipräsidenten gerichtet hatte, den personenbezogenen Hinweis „psychisch auffällig“ erhalten hatte. Die Polizei hatte eine solche Speicherung zunächst bestritten, da die Einstufung auf der Einschätzung eines Polizeibeamten beruhte und nicht eines Arztes, wie polizeiintern vorgesehen. Derartige Hinweise zur Eigensicherung der Beamten haben in der Praxis für das Verhalten der Polizeibeamten große Bedeutung. Fehler bei der Vergabe können daher schwerwiegende Konsequenzen nach sich ziehen. Es ist für den Betroffenen auch praktisch kaum möglich, den Hinweis berichtigen oder löschen zu lassen. Wie soll er nachweisen, dass er nicht „psychisch auffällig“ ist, wenn es keine belastbare ärztliche Beurteilung gibt? Die Polizei stimmte mir daher zu, dass der Hinweis zu löschen war. Zudem war der Petent im polizeilichen

Informationssystem unter dem Datum seiner Schreiben jeweils als „Tatverdächtiger“ eines „sonstigen Delikts“ mit Deliktschlüssel vermerkt, obwohl kein Delikt begangen, keine Anzeige erstattet oder Ermittlungen aufgenommen worden waren. Auch fehlten Angaben zu den Umständen der Eintragung, so dass diese nicht nur unrichtig, sondern auch ungeeignet war, einem abrufenden Polizeibeamten Informationen für sein weiteres Vorgehen zu vermitteln. Ferner war der Deliktschlüssel auch noch in sich fehlerhaft und widersprüchlich vergeben worden. Nach dem Deliktschlüssel war der Petent bereits aufgrund einer gerichtlichen Verfügung nach dem Psychisch-Kranken-Gesetz (PsychKG) untergebracht worden, was aber nicht der Fall gewesen ist. Auch hier erreichte ich eine Korrektur. Schließlich teilte die Polizei mir auch noch mit, dass die Schreiben des Petenten, die zu den Eintragungen im polizeilichen Informationssystem geführt hatten, sich nicht mehr vollständig in der Akte befanden. Es ist der Polizei daher gar nicht mehr im Einzelnen möglich, den Hintergrund der Einträge nachzuvollziehen. Auch insoweit habe ich die Polizei aufgefordert, die Datenspeicherung zu korrigieren.

In einem anderen Fall rief mich ein Petent an und berichtete, dass ihn abends unter seiner Privatnummer eine fremde Frau angerufen habe und ihm sagte, er sei Halter eines bestimmten Fahrzeugmodells in einer bestimmten Farbe und seine Tochter habe heute morgen in seiner Wohnstraße ihren Sohn angefahren. Als der Petent wissen wollte, woher die Frau dies alles wisse, teilte sie mit, sie sei die Frau eines Polizeibeamten. Im Laufe des Abends meldete sich dann der Beamte und erklärte die Angelegenheit für erledigt. Der Petent hatte zu diesem Zeitpunkt bereits einen Mann mit seinem Sohn in der Wohnstraße gesehen, der die Wagen der Nachbarn untersuchte. Es stellte sich heraus, dass der Sohn eines Polizeibeamten morgens von einem Fahrzeug angefahren worden war und vom Fahrrad gestürzt war. Die junge Fahrerin hatte den Sohn im Wagen zur Schule gebracht und erwähnt, dass sie „gleich hier“ wohne. Der Vater und Polizeibeamte hatte daraufhin von seiner dienstlichen Möglichkeit einer Kfz-Halterabfrage und Melderegisterabfrage Gebrauch gemacht und mögliche Halter des Fahrzeugtyps in der Gegend und deren Familienverhältnisse (Tochter in bestimmten Alter) ermittelt, „zwecks Geltendmachung schadensersatzrechtlicher Ansprüche“. Allerdings war der angerufene Petent bzw. seine Tochter nicht der vermeintliche Unfallbeteiligte. Seine Tochter lebte samt Fahrzeug in einem anderen Bundesland. Der Beamte hatte daraufhin mit seinem Sohn die Umgebung des Unfallortes erneut abgesucht und das Verursacherfahrzeug ausfindig gemacht. Erneut tätigte der Beamte eine Kfz-Halterabfrage und Melderegisterabfrage und suchte die Telefonnummer aus dem Telefonbuch. Auch diese Familie rief er zur „Schadensregulierung“ an. Eine Strafanzeige wegen Unfallflucht oder fahrlässiger Körperverletzung fertigte der Beamte nicht.

Ich teilte der Polizei Bremen mit, dass das Vorgehen des Beamten in mehrfacher Hinsicht datenschutzwidrig sei, eine Ordnungswidrigkeit darstelle und zudem auch aus polizeitaktischer Sicht fragwürdig sei. Die Polizei führte daraufhin ein ausführliches Gespräch mit dem Beamten über seine datenschutzrechtlichen Pflichten. Der Beamte unterzeichnete eine Datenschutzerklärung. Zugleich erkundigte ich mich, ob es bei der Polizei Bremen Regelungen gibt, die eine Ermittlung von Beamten einschränkt, sofern eigene Belange betroffen sind. Andernfalls sei es nicht möglich, zwischen Abfragen zu dienstlichen bzw. privaten Zwecken zu unterscheiden. Die Polizei teilte mir daraufhin mit, dass derartige Regelungen nicht bestünden und beharrte darauf, dass mangels Wiederholungsgefahr

weiterreichende Maßnahmen nicht erforderlich seien. Dies halte ich im Ergebnis für unbefriedigend und plane, mich für eine derartige Regelung einzusetzen.

In einem weiteren Fall hatte sich ein Petent an mich gewandt, der eine zivilrechtliche Streitigkeit über die Abwicklung von Werkstattkosten austrug, die auch in einer Strafanzeige wegen Betrugs gegen ihn mündete. Dabei war er von dem Werkstattbesitzer im Beisein seines Vaters, der Polizeibeamter ist, unter Druck gesetzt und ihm waren Schwierigkeiten angedroht worden. Wenige Zeit später erhielt der Arbeitgeber des Petenten ein anonymes Schreiben, in dem offengelegt wurde, dass er strafrechtlich in Erscheinung getreten war. Aufgrund des zeitlichen und inhaltlichen Zusammenhangs überprüfte ich die Protokolle der Zugriffe im polizeilichen Informationssystem auf die Daten des Petenten und stellte fest, dass der Vater des Werkstattbesitzers zunächst ohne erkennbaren dienstlichen Hintergrund auf die Daten zugegriffen hatte. Die Ermittlungen der Polizei führten zu einem Strafverfahren wegen des Verrats von Dienstgeheimnissen, das im Ergebnis jedoch eingestellt wurde, da nicht gerichtsfest nachweisbar war, dass die durch den Zugriff erlangten Informationen von dem Beamten weitergegeben worden waren oder er Urheber des anonymen Drohbriefes ist. Die Staatsanwaltschaft räumte allerdings ein, dass es sich insoweit um eine wirklichkeitsnahe Vermutung handele. Erschwert wurde das Verfahren dadurch, dass der Petent um jeden Preis vermeiden wollte, dass sein Arbeitgeber als Zeuge Näheres zu dem Drohbrief aussagt, weil er dann mit einem Verlust seines Arbeitsplatzes rechnete. Ich forderte die Polizei nach Einstellung des Strafverfahrens auf, zumindest den unberechtigten Zugriff disziplinarisch zu ahnden, da der Beamte als Begründung für den Zugriff angab, er habe überprüfen wollen, ob sein Sohn ihn bei der Strafanzeige wegen Betrugs als Zeugen angegeben habe. Insoweit handelte der Beamte jedoch aus privaten Gründen. Andere Privatpersonen könnten eine derartige Abfrage im polizeilichen Informationssystem nicht veranlassen. Auch ist die Aussage lebensfremd, da der Beamte nur seinen Sohn hätte fragen müssen und über die Abfrage eine Vielzahl weiterer Informationen erhielt. Ich bat daher um Stellungnahme, weshalb die Polizei Bremen keinen Raum für Maßnahmen sieht, den Verstoß angemessen zu ahnden. Ich wies auch darauf hin, dass das Fehlen einer Regelung zum Tätigwerden von Beamten bei eigener Betroffenheit die Beurteilung der Zugriffe erschwert. Eine Antwort der Polizei Bremen steht bislang aus.

9.6 Prüfung der Antiterrordatei beim LKA und Landesamt für Verfassungsschutz

Auf Grundlage des Antiterrordateiengesetzes vom 22. Dezember 2006 sollte bis März 2007 bei den beteiligten Behörden, u. a. dem Landeskriminalamt (LKA) Bremen und dem Landesamt für Verfassungsschutz Bremen, die Infrastruktur für den Betrieb der Antiterrordatei aufgebaut und die Datei in den Wirkbetrieb genommen werden.

Ich habe daher im Mai und Juni 2006 die Antiterrordatei bei den beteiligten Behörden in Bremen geprüft und mich u. a. über die vorgenommenen technischen und organisatorischen Maßnahmen, z. B. Verschlüsselungen oder Zugriffsberechtigungen, informiert. Dabei musste ich feststellen, dass die Infrastruktur vorhanden und die Antiterrordatei einsatzbereit war, jedoch das Befüllen der Datei noch andauerte. Dies lag nicht unbedingt an einer großen Zahl von Einträgen, sondern war der Personalknappheit bei Polizei und Verfassungsschutz und der Sicherstellung der Qualität der Daten

geschuldet. Die meisten Probleme, die das Gesetz aufwirft (vgl. 30 JB, Ziff. 9.8) waren in der Praxis in Bremen daher noch nicht relevant geworden. Einzelne Fragen habe ich in einem vorläufigem Prüfbericht festgehalten und beabsichtige im Jahr 2008, wenn die Befüllung voraussichtlich abgeschlossen ist, die Prüfung fortzusetzen.

9.7 Eingaben im Bereich des Verfassungsschutzes

Auch in diesem Jahr haben sich wieder verschiedene Petenten mit Eingaben bzgl. des Landesamtes für Verfassungsschutz (LfV) an mich gewandt. Oftmals werde ich eingeschaltet, wenn die Betroffenen Einsicht in ihre beim Landesamt für Verfassungsschutz gespeicherten personenbezogenen Daten nehmen möchten oder wissen möchten, ob sie Gegenstand einer nachrichtendienstlichen Maßnahme sind. Regelmäßig richtet sich die Anfrage sowohl an die Polizei Bremen als auch das LfV. Das Landesamt kann insoweit die Auskunft in bestimmten Fällen verweigern, muss die Betroffenen jedoch darauf hinweisen, dass sie mich anrufen können. Mir wird dann vom Landesamt Einsicht gewährt bzw. Auskunft erteilt. Allerdings kann ich den Petenten diese vertraulichen Informationen nicht mitteilen, sondern lediglich die Rechtmäßigkeit bzw. Unrechtmäßigkeit der Datenverarbeitung prüfen und das Ergebnis festhalten. Daneben bin ich z. B. in einem Einbürgerungsverfahren angerufen worden, in dem dem Betroffenen die Einbürgerung aufgrund nachrichtendienstlicher Erkenntnisse verwehrt, die Erkenntnisse selbst aus Gründen des Quellenschutzes jedoch nicht mitgeteilt wurden. Auch hier konnte ich durch eine Einsichtnahme die Rechtmäßigkeit der Datenverarbeitung sicherstellen. Zum Prüfumfang zählt dabei selbstverständlich auch, ob die Weigerung der Behörde zur Auskunftserteilung rechtmäßig ist.

9.8 Verfassungsbeschwerdeverfahren gegen das Antiterrordateiengesetz

Im Juli 2007 erhielt ich vom Bundesverfassungsgericht den Abdruck der Verfassungsbeschwerde zum Antiterrordateiengesetz (1 BvR 1215/07) mit der Bitte, zu den aufgeworfenen verfassungsrechtlichen Fragen eine Stellungnahme abzugeben. Die Datenschutzbeauftragten des Bundes und der Länder einigten sich, eine gemeinsame Stellungnahme zu formulieren. Die Vorarbeiten hierfür übernahm der Arbeitskreis Sicherheit der Datenschutzkonferenz und dort vor allem die Länder Schleswig-Holstein und Berlin.

In ihrer gemeinsamen Stellungnahme vertreten die Datenschutzbeauftragten, dass das Antiterrordateiengesetz (ATDG) einen nicht gerechtfertigten Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellt, da es gegen die Grundsätze der Normenklarheit, Bestimmtheit und der Verhältnismäßigkeit verstößt. Dies betrifft die Beschreibung des betroffenen Personenkreises und den Umfang der zu speichernden Daten, aber auch die unklaren Zugriffs- und Verwendungsregelungen sowie die unzureichenden Löschungsregelungen und Auskunftsrechte der Betroffenen. Aufgeworfen wird auch die Frage, inwieweit das ATDG dem Gebot, Polizei- und Nachrichtendienste zu trennen, genügt.

9.9 Entscheidung des Bundesverfassungsgerichts zur

Videoüberwachung

Das Bundesverfassungsgericht hat mit Beschluss vom 23. Februar 2007 (1 BvR 2368/06) entschieden, dass eine Videoüberwachung öffentlicher Plätze in Regensburg nicht auf die allgemeinen Übermittlungsvorschriften des Bayerischen Landesdatenschutzgesetzes gestützt werden kann. Es fehle dabei an einer hinreichend bestimmten und normenklaren Rechtsgrundlage, um den durch die Videoüberwachung verursachten Eingriff in das Grundrecht auf informationelle Selbstbestimmung zu rechtfertigen. Das Urteil enthält einige grundlegende allgemeine Ausführungen zur Videoüberwachung. Das Bundesverfassungsgericht betont in der Entscheidung, dass eine Videoüberwachungsmaßnahme einen Eingriff von erheblichem Gewicht darstellt, weil er verdachtslos und mit großer Streubreite zahlreiche Personen betrifft, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben. Zudem dient die Videoüberwachungsmaßnahme dazu, belastende hoheitliche Maßnahmen vorzubereiten und das Verhalten der den Raum nutzenden Personen zu lenken. Das infolge der Aufzeichnung gewonnene Bildmaterial kann in vielfältiger Weise ausgewertet, bearbeitet und mit anderen Informationen verknüpft werden.

9.10 Entwurf eines Bundesmeldegesetzes

Im Zuge der Föderalismusreform wurde das Meldewesen in die ausschließliche Gesetzgebungskompetenz des Bundes überführt. In Ergänzung der bisherigen kommunalen Register plant das Bundesministerium des Innern den Aufbau eines Bundesmelderegisters (BMR). Ich habe den Senator für Inneres und Sport sowie den Magistrat der Stadt Bremerhaven und das Stadtamt Bremen gebeten, u. a. folgende grundsätzlichen Positionen bei einer anstehenden Gesetzesberatung zu vertreten:

Eine Reform des Melderechts muss den Umfang der im Meldewesen gespeicherten Daten einer kritischen Prüfung unter den Gesichtspunkten der Erforderlichkeit und der Zweckbindung unterziehen.

Ein zentrales Bundesmelderegister und die damit verbundene mehrfache Datenhaltung bei Bund und Länder ist nicht erforderlich. Die Modernisierung des Meldewesens kann durch eine Vernetzung der vorhandenen Melderegister erreicht werden. Hierfür hat man bereits 2002 auf Drängen des Bundes den Datenaustausch im Meldewesen und damit die Voraussetzungen für einen effizienten und sicheren Datenaustausch geschaffen.

Der vollständige Meldedatenbestand muss bei den jeweiligen kommunalen Meldeämtern und unter deren Verantwortung verbleiben.

9.11 Mobiler Bürgerservice

Das Stadtamt Bremen will das Angebot von Verwaltungsdienstleistungen durch Nutzung neuer technischer Entwicklungen der Datenübertragung weiter entwickeln und modernisieren. Im Oktober 2006 wurde ich darüber informiert. Das Pilotprojekt trägt den Namen "Mobiler Bürgerservice".

Es war geplant, durch Einsatz mobiler Endgeräte ein Angebot an wechselnden Standorten in verschiedenen Stadtteilen Bremens anzubieten. Dabei sollte es sich um Anlaufstationen handeln wie beispielsweise Einkaufszentren, Stadtbibliotheken oder Senioreneinrichtungen, die vor allem für Bürger mit Bewegungseinschränkungen gut erreichbar sein sollten. Begonnen werden sollte mit dem am stärksten nachgefragten Angebot, dem Meldewesen.

Ich habe von der ersten Projektsitzung an darauf aufmerksam gemacht, dass ein Datenschutzkonzept für den Anwendungsfall „Mobiler Bürgerservice“ erstellt werden muss, da bereits in dem Pilotprojekt personenbezogene Originaldaten verarbeitet werden.

Da für die Anbindung der Standorte an das Stadtamt die bestehende bremische Infrastruktur genutzt werden sollte, war eine Betrachtung dieser Infrastruktur unter den zuvor genannten Anforderungen nach § 7 BremDSG für das Projekt „Mobiler Bürgerservice“ und das zu erstellende Datenschutzkonzept notwendig.

Das Projekt „Mobiler Bürgerservice“ wurde in zwei Phasen geteilt. In der ersten Phase wählte die Arbeitsgruppe Standorte aus, die über eine Datenleitung zur Nutzung des BVN verfügten, und zwar die Stadtbibliothek Bremen und das Ortsamt Osterholz. Das Stadtamt legte dafür im Dezember 2006 ein entsprechendes Datenschutzkonzept vor. Meine Stellungnahme erhielt das Stadtamt Bremen im Februar 2007. Es ergaben sich u. a. Fragen zur Anbindung der genannten Standorte an das Stadtamt Bremen, zur Leitungsver schlüsselung, zur Härtung der Arbeitsplätze und Protokollierung der Zugriffe.

Im Februar 2007 wurde ich über den Beginn der zweiten Phase dieses Projektes informiert, in dem mobile Endgeräte eingesetzt werden sollten. Aufgrund der vorgesehenen Funkverbindung wurde es möglich, Senioreneinrichtungen und Einkaufszentren als neue Standorte einzubeziehen. Das Stadtamt sicherte mir eine Ende-zu-Ende-Verschlüsselung vom eingesetzten Endgerät bis zur Anwendung im Stadtamt sowie einen zertifizierten Zugang über ein Security-Gateway zu. Des Weiteren habe ich Vorgaben zur eingesetzten Hardware gemacht, wie z. B. den Einsatz einer Firewall, eine Festplattenverschlüsselung und lokale Sicherheitssoftware. Außerdem forderte ich die klare Definition der Administrationsverantwortung.

Im April des Berichtsjahres habe ich mir den für dieses Projekt angefertigten „Bürgeramtkoffer“ angesehen. In diesem sind neben einem Notebook eine so genannte Desktop-Box mit zentralem Stromanschluss und USB-Hub sowie ein Drucker und ein Scanner untergebracht. Die Festplatte des Notebooks ist verschlüsselt. Die Einwahl über das Security-Gateway wurde demonstriert, jedoch konnten bei diesem Termin keine detaillierten Angaben zum eingesetzten Zertifikat sowie zum Aufbau des verschlüsselten Tunnels gemacht werden. Die dazu vorgelegte Skizze war unvollständig und sollte noch ergänzt werden. Eine abschließende Bewertung ist mir erst nach Vorlage des vollständigen Datenschutzkonzepts möglich. Dieses sollte auch organisatorische Regelungen (z. B. Ablaufplan für Mitarbeiter) sowie Konzepte für Wartung und Updates, zur Administration und Angaben zur Protokollierung enthalten. Auch die noch offenen Punkte zum Rahmendatenschutzkonzept sollten darin Berücksichtigung finden.

Im Juli diesen Jahres wies ich erneut auf die noch ausstehenden Unterlagen zum Projekt „Mobiler Bürgerservice“ hin und erhielt im August einen Abschlussbericht. Ich bemängelte nochmals, dass eine

Anpassung des Datenschutzkonzepts für die erste Phase nicht erfolgt war und dass ich für die zweite Phase kein Datenschutzkonzept erhalten hatte. Eine Fortführung bzw. Ausdehnung des Projektes auf weitere Standorte kann nur erfolgen, wenn bis dahin ein vollständiges Datenschutz- und IT-Sicherheitskonzept vorliegt.

Im Dezember 2007 hat mich das Stadtamt informiert, das Projekt „Mobiler Bürgerservice“ werde aufgrund mangelnder personeller Ressourcen derzeit nicht fortgeführt.

9.12 Online-Anmeldung von Kraftfahrzeugen durch Autohäuser

Um die Zulassung von Kraftfahrzeugen zu beschleunigen, können autorisierte Zulassungsdienste und Autohäuser die Kfz- und Halterdaten via Internet im Rahmen einer E-Government-Anwendung an die Zulassungsstellen übermitteln. Durch einen Link auf den Webseiten von Bremen.de gelangen sie auf die Seiten der Kfz-Zulassungsstellen des Stadtamtes Bremen. Im vergangenen Jahr hatte ich berichtet, dass die Daten ungeschützt übertragen wurden (vgl. 29. JB, Ziff. 9.2.3). Das Stadtamt hatte zugesagt, dies zu unterlassen und die Übertragung abzusichern. Geplant war die Umsetzung der Datenübertragung mittels des OSCI-Protokolls. Da es sich nicht um eine unmittelbare Zulassung von Fahrzeugen handelt, sondern nur um die vorbereitende Datenerfassung und die Übermittlung an die Zulassungsstellen, nahm das Stadtamt von einem Authentizitätsnachweis per elektronischer Signatur, wie es der zunächst geplante OSCI-Einsatz ermöglicht hätte, Abstand. Das Stadtamt teilte mit, durch den Geschäftsablauf bedingt würde die Identität des zukünftigen Halters und der Vertretungsvollmacht bei der Abholung der Dokumente geprüft. Das Verfahren sei so geändert worden, dass die Übermittlung der Daten für die Zulassung und die Anmeldung der Nutzer nunmehr verschlüsselt erfolge. Damit ist auf dem Transportweg ein angemessenes Datenschutzniveau erreicht.

9.13 Fingerabdruckdaten in Reisepässen

In Umsetzung der Verordnung (EG) 2252/2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten der Europäischen Union ausgestellten Pässen und Reisedokumenten hat Deutschland in einer ersten Stufe zum 1. November 2005 den biometrischen Reisepass eingeführt und in einem sog. RFID-Chip das Gesichtsbild elektronisch gespeichert. Ab 1. November 2007 kam die Speicherung von zwei Fingerabdrücken hinzu. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte sich bereits im Juni 2005 mit einer EntschlieÙung dagegen gewandt und darauf hingewiesen, dass die Einführung biometrischer Reisepässe nicht automatisch zu mehr Sicherheit führt (vgl. 28 JB, Ziff. 19.11).

Vor der flächendeckenden Einführung sollte das Verfahren unter realen Bedingungen in ausgewählten Passbehörden getestet werden. Zu diesen gehörte die Passbehörde Bremerhaven. Im Dezember 2006 wurde ich um Stellungnahme zu dem bremischen Landesgesetz gebeten, mit dem die Teilnahme der Passbehörde Bremerhaven an der Testphase umgesetzt wurde. Ich habe eine Stellungnahme abgegeben, in der ich verschiedene Anforderungen aufgestellt habe, so z. B. zu rechtstechnischen Vorgaben, insbesondere der Veröffentlichung und Beachtung der Technischen Richtlinie für das Testverfahren durch das Bundesamt für Sicherheit in der Informationstechnik, wie zur Aufklärung der Bürger über die Teilnahmebedingungen.

Ende Mai 2007 habe ich vor Beendigung der Testphase der Passbehörde Bremerhaven einen Besuch abgestattet und mich vor Ort informiert. Zu diesem Zeitpunkt hatten etwa 400 Bürgerinnen und Bürger sich an 32 Geräten an zwei Standorten Reisepässe erstellen lassen. Probleme bei der Durchführung hatte es nicht gegeben. Die Passbehörde hatte ein vom Bundesministerium des Innern zur Verfügung gestelltes Informationsblatt für Bürger bereitgestellt und behördenintern eine Anweisung zur Durchführung des Feldtests erlassen. Beim Einscannen wurden erst von der einen, dann der anderen Hand der Zeigefinger eingescannt, wobei drei Bilder aufgenommen und das beste schließlich weiterverwendet wird. Ich stellte dabei fest, dass das System nicht erkennt, wenn der Zeigefinger der einen Hand bei einer der Aufnahme mit dem Zeigefinger der anderen Hand vertauscht wurde. Das System wählt dann u. U. einen falschen Fingerabdruck als den besten aus. Ich stellte ferner fest, dass die Fingerabdruckdaten entgegen § 23 a Abs. 3 Satz 7 PassG nicht getrennt von anderen Dateien mit Passantragsdaten gespeichert wurden. Die Übermittlung vom Arbeitsplatzrechner an den „Kommunikations-Server“ für die Übermittlung an die Bundesdruckerei erfolgte unverschlüsselt innerhalb des unsicheren (vgl. 23. JB, Ziff. 3.2) Magistrats-Netzes. Eine Änderung des Datenschutzkonzeptes mit Blick auf die Testphase war nicht erfolgt.

Nach der Aufnahme des Produktionsbetriebes bei der Beantragung eines ePasses im November 2007 ist im Jahr 2008 ein erneuter Besuch bei der Passbehörde geplant, bei dem ich u. a. die oben genannten Punkte erneut aufgreifen werde.

9.14 Anmeldung zur Eheschließung im Internet (xStA-Bürger)

Im Sommer 2006 wurde ich durch einen Presseartikel auf ein bei den Standesämtern eingeführtes Datenverarbeitungsverfahren „xStA-Bürger“ aufmerksam. Danach können heiratswillige Bürgerinnen und Bürger sich einen Weg zum Standesamt ersparen, indem sie durch Eingabe verschiedener Daten zu ihrer Person, etwaigen Kindern, ihren Eltern und Trauzeugen, die Anmeldung zur Eheschließung beschleunigen. Das Verfahren wird nicht direkt beim Stadtamt Bremen, sondern im Wege der Auftragsdatenverarbeitung durch das anbietende Unternehmen von einem Rechner in Frankfurt aus betrieben.

Im Sommer 2006 wandte ich mich zunächst an die Standesämter Bremen-Mitte und Bremen-Nord und bat um die Übersendung der Verfahrensbeschreibung und des Datenschutzkonzeptes einschließlich der Unterlagen zur Auftragsdatenverarbeitung. Im November 2006 wurde mir vom Stadtamt Bremen mitgeteilt, dass meine Auffassung zum Bestehen eines Auftragsdatenverarbeitungsverhältnisses geteilt werde, allerdings keine Unterlagen vorhanden seien. Diese sollten erstellt werden. Im Sommer 2007 habe ich mich nach dem Stand der Erarbeitung erkundigt, da weiterhin die gesetzlich vorgeschriebene Dokumentation des Verfahrens und der getroffenen technisch-organisatorischen Maßnahmen ausstand, um das Verfahren datenschutzrechtlich angemessen zu prüfen. Vom behördlichen Datenschutzbeauftragten des Stadtamtes Bremen wurde mir mitgeteilt, dass ihm mittlerweile Entwürfe zur Verfahrensbeschreibung und zum Datenschutzkonzept nebst Anlagen vorlägen, aber weiterer Gesprächsbedarf mit den Erstellern bestünde. Seitdem warte ich weiter auf die angekündigte Übersendung der Unterlagen.

9.15 BVerfG zur TK-Überwachung im Fall Masri

Mit Beschluss vom 30. April 2007 (2 BvR 2151/06) entschied das Bundesverfassungsgericht, dass die Überwachung des Telefon- und Telefaxanschlusses der Rechtsanwaltskanzlei, die den mutmaßlich von Geheimdienstkreisen entführten Khaled El Masri vertrat, eine Verletzung des Fernmeldegeheimnisses und der Berufsausübungsfreiheit des Beschwerdeführers darstellt.

Das Verfassungsgericht ließ dabei die Begründung des anordnenden Gerichts nicht gelten, aufgrund der Medienberichterstattung eineinhalb Jahre nach der Entführung müsse damit gerechnet werden, die Entführer träten mit der Kanzlei in Verbindung. Hierbei handele es sich lediglich um Vermutungen. Das Verfassungsgericht hat damit die hohen Anforderungen an die Rechtfertigung von Eingriffen in das Fernmeldegeheimnisses hervorgehoben und einer allzu ausufernden Praxis bei der Telekommunikationsüberwachung entgegengewirkt.

9.16 Verfahren ADVIS und BONITAET beim Stadtamt Bremen

Im Juli 2007 übersandte mir das Stadtamt Bremen die Verfahrensbeschreibung und das Datenschutzkonzept für die Verfahren „AusländerDatenVerwaltungs- und InformationsSystem“ (ADVIS) und BONITAET, welches ein Programm zum Verwalten und Auswerten von Verpflichtungserklärungen ist, mit denen sich eine Person verpflichtet, für die Lebenskosten eines Ausländers im Bundesgebiet aufzukommen.

Im Juli 2007 übersandte ich dem Stadtamt Bremen meine Stellungnahme zu der Verfahrensbeschreibung und zum Datenschutzkonzept des Verfahrens BONITAET. Die Rechtsgrundlagen waren nicht zutreffend aufgeführt und die Darstellung der verarbeiteten Datenkategorien war teilweise zu allgemein oder unzutreffend. Aus technischer Sicht fehlte eine Authentifizierung und Protokollierung, so dass nicht nachvollzogen werden konnte, wer Eingaben oder Zugriffe in dem Programm tätigt. Das Stadtamt Bremen hat mir daraufhin im November 2007 verschiedene Änderungen mitgeteilt; offen blieb jedoch, wie viele Personen auf das Programm zugreifen, ob eine Anmeldung an dem Verfahren erfolgt und ob eine Protokollierung der Benutzeraktivitäten erfolgt. Daher habe ich Anfang Dezember 2007 einige ergänzende Informationen angefordert. Eine Antwort hierauf steht bislang aus.

Zu dem Verfahren ADVIS, das deutlich umfangreicher ist als BONITAET, nahm ich im Dezember 2007 gegenüber dem Stadtamt Bremen Stellung. Dabei stellte ich fest, dass vor allem eine klare Trennung der Datenverarbeitung nach dem Aufenthaltsgesetz und der Aufenthaltsverordnung einerseits und dem Ausländerzentralregistergesetz und seiner Durchführungsverordnung fehlt. So kam es bei der Angabe der Rechtsgrundlagen, der Beschreibung der Datenkategorien und der Verwendungszwecke zu Unklarheiten und Unrichtigkeiten. Es wurden unzutreffende Rechtsgrundlagen genannt und zutreffende Rechtsgrundlagen weggelassen, die beschriebenen Daten entsprachen nicht den Rechtsgrundlagen und die Verwendungszwecke waren nicht vollständig genannt. Es wurden Fragen zum Trennungsgebot aufgeworfen, da unter ADVIS verschiedene Dateien geführt werden, für die ich zum Teil keine Rechtsgrundlage erkennen konnte. Die Darstellung der Löschfristen und Empfänger von Datenübermittlungen waren teilweise unvollständig oder

unzutreffend. Daneben ergaben sich verschiedene Fragen zur Datensicherheit des Verfahrens, etwa zum Trennungsgebot, zur Weitergabe-, Zugriffs- und Verfügbarkeitskontrolle.

9.17 Übermittlung von Meldedaten an politische Parteien vor den Wahlen

Auch im Vorfeld der Wahlen zur Bremischen Bürgerschaft und zur Stadtverordnetenversammlung Bremerhaven wurden wieder von den Meldebehörden in Bremen und Bremerhaven Daten von wahlberechtigten Einwohnern an Parteien weitergegeben, die an der Wahl teilnehmen.

Die Meldebehörde Bremen übermittelte aus dem Einwohnermelderegister Dateien mit Einwohnerlisten an die CDU, die DVU und die Republikaner (REP). Aus dem Melderegister der Stadt Bremerhaven erhielten vor der Bürgerschafts- und der Stadtverordnetenwahl die CDU, die DVU und die Wählervereinigung „Bürger in Wut“ (BiW) Daten von Wahlberechtigten. Maßgeblich für den Umfang, der von der jeweiligen Datenübermittlung Betroffenen, ist dabei stets die Zugehörigkeit zu einer bestimmten Lebensaltersgruppe. Daten von Einwohnern, die nach § 33 Abs. 1 Meldegesetz (BremMeldG) gegen die Übermittlung ihrer Daten bei der Meldebehörde Widerspruch eingelegt hatten, wurden nicht übermittelt.

Schwerwiegende Mängel wurden bei der Überprüfung der Datenübermittlungen im Vergleich zu vorhergehenden Wahlen nicht festgestellt. Im Hinblick auf die öffentliche Bekanntmachung des Widerspruchs nach § 33 Abs. 1 Satz 7 BremMeldG war in Bremerhaven allerdings festzustellen, dass diese dort erst verspätet erfolgte. Ich habe die Meldebehörde Bremerhaven aufgefordert, bei künftigen Wahlen die sich aus § 33 Abs. 1 Satz 7 BremMeldG ergebende Frist zur Bekanntgabe von acht Monaten vor der jeweiligen Wahl einzuhalten.

9.18 Eingaben in Bezug auf politische Parteien und Wahlinitiativen im Zusammenhang mit den Wahlen

Im Vorfeld der Wahlen zur Bremischen Bürgerschaft und zur Bremerhavener Stadtverordnetenversammlung erhielt ich im Frühjahr des Berichtsjahrs mehrere Eingaben von Bürgern, die die Verarbeitung von Wählerdaten durch an der Wahl teilnehmende Parteien betrafen.

Eine Bürgerin beklagte sich dabei, dass sie von einer bestimmten Partei wiederholt Wahlwerbebriefe erhalten hatte, ohne dass sie hiermit einverstanden gewesen sei. Bereits den ersten Brief, den sie erhalten hatte, habe sie an die Partei zurückgeschickt mit der Aufforderung, ihr keine weitere Wahlwerbung zuzuschicken und ihre Daten zu löschen. Nach § 28 Abs. 4 BDSG hat der Betroffene das Recht, der Nutzung seiner Daten für Zwecke der Werbung zu widersprechen. Im Widerspruchsfall dürfen die gespeicherten Daten für Zwecke der Werbung nicht mehr genutzt werden. Diese Regelung gilt auch für Werbung zu politischen Zwecken. Erst auf meine ausdrückliche und wiederholte Aufforderung hin erklärte sich die Partei schließlich zum Verzicht auf weitere Wahlwerbung und die Löschung der Daten meiner Petentin bereit.

Auch aufgrund vorhergehender Presseartikel erhielt ich eine Vielzahl von Eingaben, die die telefonische Wahlwerbung einer Wahlinitiative betrafen. Bei Annahme des Anrufs erfolgte eine automatische Bandansage durch eine Privatperson, die zugleich der Spitzenkandidat der

Wahlinitiative war und mit dieser im Wahlkampf verbunden wurde. Die Privatperson berichtete über einen von ihr gegründeten Verein, der Deutsche in Not unterstütze und endete mit der Bitte, die Person unter der im Telefonbuch angegebenen Nummer anzurufen, wenn man Menschen kenne, die Hilfe benötigen. Unmittelbar vor der Wahl erfolgten weitere „freundliche Erinnerungsanrufe“. Daneben beschwerten sich verschiedentlich Betroffene, die Telefaxe der Privatperson bzw. des von ihr gegründeten Vereins erhalten hatten. Die Betroffenen beklagten sich darüber, dass sie in die Kontaktaufnahme per Telefon und Telefax nicht eingewilligt hätten. Ich habe die Wahlinitiative angeschrieben und meine Bedenken an der Zulässigkeit der telefonischen Wahlwerbung geäußert. Nach der Rechtsprechung verletzen unerbetene Telefonanrufe das Persönlichkeitsrecht der Betroffenen auch dann, wenn sie von einer politischen Partei während des Wahlkampfes erfolgen. Ihr Interesse, möglichst viele Stimmberechtigte für ihre Ziele zu gewinnen, muss hinter das Recht des Einzelnen auf Respektierung seines häuslichen Lebensbereiches zurücktreten. Zur näheren Aufklärung des Sachverhalts bat ich zunächst um die Beantwortung verschiedener Fragen, da insbesondere die Frage der Urheberschaft nicht klar war und offenbar auch bewusst so gehalten werden sollte.

Der Spitzenkandidat der Wahlinitiative bestritt, dass diese zu irgendeinem Zeitpunkt telefonische Wahlwerbung betrieben habe und drohte gerichtliche Schritte an. Nähere Auskunft zu den Telefonanrufen und Telefaxen, die ihm als Autor der automatischen Bandansage und Gründer des Vereins möglich gewesen wären, gab er nicht.

Da ich eine Verantwortlichkeit des Vereins, der sich in der automatischen Bandansage und über den Briefkopf der Telefaxe als Urheber zu erkennen geben sucht, nicht ausschließen konnte, habe ich mich Anfang Mai an den Hamburgischen Datenschutzbeauftragten zur Aufklärung des Sachverhaltes gewandt, da der Verein seinen Sitz in Hamburg hatte.

Der Hamburgische Datenschutzbeauftragte sah letztlich keinen Grund für sein Tätigwerden, da aller Voraussicht nach die Telefonnummern für die Anrufe und Telefaxe automatisiert ausgewählt und angerufen werden, ohne personenbezogenen Daten der Betroffenen zu speichern. Auch wurde der Aufwand einer kurzfristigen Prüfung als zu groß angesehen.

Dies habe ich im Ergebnis akzeptiert, da wenige Tage später die Bürgerschaftswahl stattfand und die Anrufe der Privatperson bzw. des Verein erwartungsgemäß endeten.

9.19 Neufassung der KpS-Richtlinien

In meinem 28. Jahresbericht (vgl. Ziff. 9.7) hatte ich gefordert, die Richtlinien über die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien) aus dem Jahr 1981 zu aktualisieren. Im Jahr 2006 wurde daraufhin ein erster Entwurf erstellt, der sich allerdings nur mit einem Teilbereich beschäftigte. Ende 2006 sagte der Senator für Inneres und Sport zu, den Entwurf bis zum Sommer 2007 abschließend zu überarbeiten.

Im Februar 2007 übersandte mir der Senator für Inneres und Sport eine überarbeitete Fassung, zu der ich Mitte Juni Stellung nahm und nach Vorlage einer aktualisierten Fassung erneut Ende Juli 2007.

Mitte September 2007 wurde mir abermals ein Entwurf zur Stellungnahme übersandt, zu dem ich abschließend im Dezember 2007 Stellung bezog.

Inhaltlich habe ich neben einer Reihe von redaktionellen Änderungen und Aktualisierungen vor allem eine Einschränkung bei der Speicherung von personenbezogenen Daten von Kindern unter sieben Jahren und zwischen sieben und 14 Jahren durchgesetzt. Zudem wird es in bestimmten Fällen zu einer von fünf auf drei Jahre verkürzten Speicherung kommen und Regelungen zur datenschutzrechtlichen Verantwortlichkeit und Sperrung von Daten wurden aufgenommen. Ferner wurde der Übersichtlichkeit halber ein Ausführungserlass des Senators für Inneres aus dem Jahre 1985 überarbeitet und in angepasster Form in die KpS-Richtlinien integriert.

Im Zusammenhang mit der Überarbeitung der KpS-Richtlinien habe ich den Senator für Inneres und Sport auf verschiedene Probleme aufmerksam gemacht, die mir aus der Beschwerdepraxis bekannt sind. Dies betrifft z. B. die Speicherfristen für sog. personenbezogene Hinweise (PHW), wie etwa „bewaffnet“ oder „Konsument harter Drogen“. Die PHW werden zur Eigensicherung der Beamten im Zusammenhang mit Deliktseinträgen vergeben. Wird ein Deliktseintrag infolge späterer Delikte fortgespeichert, kann dies dazu führen, dass ein PHW über viele Jahre fortbesteht, obwohl es der tatsächlichen Situation des Betroffenen nicht mehr gerecht wird und fehlerhafte Polizeieinschätzungen fördert.

Auch wird nach meiner Erfahrung der PHW „psychisch auffällig“ verschiedentlich vergeben, ohne dass ein ärztliches Attest besteht (vgl. 30. JB, Ziff. 9.5). Eine derartige Vergabe durch nicht geschulte Beschäftigte bedeutet für die Betroffenen eine schwere Stigmatisierung. Die Betroffenen werden, wenn sie sich an die Polizei wenden, z. B. nicht mehr ernst genommen. Faktisch wird die Beweislast umgekehrt, indem den Betroffenen der Nachweis auferlegt wird, dass sie nicht „psychisch auffällig“ sind, was jedoch in der Praxis unmöglich ist. Damit wird das Recht der Betroffenen unterlaufen, unrichtige personenbezogene Daten berichtigen zu lassen.

Ein weiteres Problem ist, dass bei Ersuchen auswärtiger Dienststellen diese personenbezogen gespeichert werden. Da die auswärtigen Dienststellen den Verfahrensausgang, z. B. eine Einstellung des Verfahrens, nicht mitteilen und die Polizeien des Landes Bremen diesen nicht erfragen, kann eine solche Speicherung unter Umständen gravierende Folgen haben. So führte eine solche Speicherung zu einem negativen Ergebnis bei einer Zuverlässigkeitsüberprüfung nach dem Luftsicherheitsgesetz.

9.20 Beteiligung an Errichtungsanordnungen des Bundeskriminalamtes

Auch in diesem Jahr sind mir wieder vom Bundesministerium des Innern verschiedene Errichtungsanordnungen zu automatisierten Dateien mit personenbezogenen Daten beim Bundeskriminalamt (§ 34 BKAG) zur Stellungnahme gegenüber dem Senator für Inneres und Sport übersandt worden, u. a. zu „INPOL Fall Innere Sicherheit“ (IFIS), „WIKRI“ (zur Wirtschaftskriminalität), zur Antiterrordatei, zur „Verbunddatei Geldwäsche-Datei/Hinweisbearbeitung Geldwäsche“, zur „Verbunddatei Straftaten gegen ältere Menschen (SÄM)“, zur Datei „Korruption“ sowie für die Dateien „Gewalttäter rechts“, „Gewalttäter links“ und „Gewalttäter politisch motivierter Ausländerkriminalität“.

9.21 **Verwaltungsvereinbarung mit der Zollverwaltung über Auskünfte nach § 17 Schwarzarbeitsbekämpfungsgesetz**

Im September 2007 erfuhr ich, dass das Bundesministerium der Finanzen beabsichtigt, mit der Freien Hansestadt Bremen eine Verwaltungsvereinbarung über die Datenauskunft nach § 17 Schwarzarbeitsbekämpfungsgesetz zu schließen. Ich habe mir den Entwurf der Vereinbarung daraufhin übersenden lassen und hierzu Stellung genommen. In rechtlicher Hinsicht wies ich auf Abweichungen der Verwaltungsvereinbarung vom Wortlaut des Gesetzes hin, die eine Einschränkung, zum Teil aber auch eine Erweiterung der gesetzlichen Auskunftsmöglichkeiten bedeutet hätten. Daneben waren aus technischer Hinsicht verschiedene Aspekte der Datensicherheit nicht hinreichend beschrieben. Insoweit habe ich darum gebeten, weitere Informationen einzuholen. Schließlich habe ich auf verschiedene Schwierigkeiten hingewiesen, die sich bei der landesseitigen Umsetzung der Vorgaben der Verwaltungsvereinbarung zur Datensicherheit ergeben. Diese beabsichtige ich im Jahre 2008 weiter zu begleiten.

9.22 **Zuverlässigkeitsüberprüfungen auf Einwilligungsbasis**

Seitdem anlässlich der Fußball-WM 2006 im Rahmen der Akkreditierung massenhaft Zuverlässigkeitsüberprüfungen durch den Deutschen Fußball-Bund e. V. (DFB) stattgefunden haben, greifen diese Verfahren um sich. Im Jahr 2007 war ich verschiedentlich mit dieser Thematik konfrontiert, sei es, dass anlässlich des EU-Außenministertreffens in Bremen Mitarbeiter der Senatskanzlei, generell Fremdbeschäftigte bei der Deutschen Bundesbank oder Bewohner, Journalisten und andere Hilfskräfte anlässlich des G 8-Gipfels in Heiligendamm auf ihre „Zuverlässigkeit“ überprüft wurden.

Immer wieder muss betont werden, dass solche Zuverlässigkeitsüberprüfungen in das Grundrecht auf informationelle Selbstbestimmung eingreifen und nicht unter Umgehung gesetzlicher Vorschriften durchgeführt werden dürfen, denn außer etwa beim Bremischen Hafensicherheitsgesetz oder dem Luftsicherheitsgesetz oder dem Sicherheitsüberprüfungsgesetz gibt es keine klaren gesetzlichen Anforderungen an derartige Verfahren. Die allgemeinen Sicherheitsüberprüfungsgesetze des Bundes und der Länder sind in diesen Fällen regelmäßig nicht einschlägig und Einwilligungen der Betroffenen können die Überprüfungen, selbst wenn eine ausreichende Information über das Verfahren erfolgen würde, nicht rechtfertigen, da ihnen in der Regel die Freiwilligkeit als Wirksamkeitsvoraussetzung fehlt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich daher im Herbst 2007 in einer Entschließung gegen die Ausweitung der Zuverlässigkeitsüberprüfungen ausgesprochen und klare, notfalls gesetzliche Regelungen gefordert, die derartige Verfahren für die Betroffenen transparent machen und ihnen unverzichtbare Betroffenenrechte einräumt (vgl. Ziff. 21.11 dieses Berichts).

9.23 **Heimliche Online-Durchsuchung privater Computer**

Im Herbst 2006 lehnte ein Ermittlungsrichter beim Bundesgerichtshof den Antrag des Generalbundesanwaltes zur Durchführung einer „verdeckten Online-Durchsuchung“ zu

Strafverfolgungszwecken ab. Der daraufhin vom Generalbundesanwalt angerufene Bundesgerichtshof (BGH) entschied am 31. Januar 2007 (AZ. StB 18/06), dass „verdeckte Online-Durchsuchungen“ zu Strafverfolgungszwecken mangels Rechtsgrundlage unzulässig sind.

Der Beschluss des BGH löste eine breite, öffentlich geführte Debatte über die Zulässigkeit und Notwendigkeit von heimlichen Online-Durchsuchungen aus. Im weiteren Verlauf wurde bekannt, dass dem Bundesministerium des Innern für das Haushaltsjahr 2007 bereits erhebliche Mittel für die Entwicklung der technischen Fähigkeiten zur Online-Durchsuchung bereitgestellt worden sind und die Nachrichtendienste auf Grundlage einer Dienstanweisung des vorigen Bundesinnenministers bereits seit längerem Online-Durchsuchungen durchführen. Eine in das nordrhein-westfälische Verfassungsschutzgesetz eingefügte Regelung für Online-Durchsuchungen wurde nach Inkrafttreten Anfang 2007 sogleich im Rahmen eines Verfassungsbeschwerdeverfahrens angegriffen. Die Entscheidung des Bundesverfassungsgerichts wird im Frühjahr 2008 erwartet. Es wurde eine zähe, politisch beeinflusste Diskussion unter Beteiligung des Bundesministerium des Innern, aber auch der Justiz über den Sinn und Zweck von Online-Durchsuchungen geführt, die Ausgestaltung einer gesetzlichen Regelung und die Notwendigkeit, die Regelung bereits vor der Entscheidung des Bundesverfassungsgerichts zu verabschieden bis hin zur Verfassungsänderung. Verschärft wurde diese Debatte durch einen im Sommer 2007 in Deutschland vereitelten Terroranschlag, obwohl die Vorgehensweise der Täter keine Argumente für den erfolgreichen Einsatz dieses Instrumentes lieferte, denn die Täter wechselten häufig ihre mobilen PC und loggten sich über fremde Funknetze ein.

Von Beginn an stieß die Online-Durchsuchung privater Computer auf Skepsis oder Ablehnung bei der rechtswissenschaftlichen und technikorientierten Literatur und bei Sachverständigen. Mit Entschließungen im März und Oktober 2007 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ihre entschieden ablehnende Haltung zum Ausdruck gebracht (vgl. Ziff. 21.9 dieses Berichts).

Heimliche Online-Durchsuchungen privater Computer stellen aufgrund der Vielzahl und Sensibilität der dort gespeicherten Daten (Fotografien, Tagebuch, Reiseberichte, persönlicher Schriftverkehr, Telefonrechnungen, Konto- oder Bewerbungsunterlagen) einen tiefen Eingriff in die Privatsphäre dar und können auch die Unverletzlichkeit der Wohnung und das Telekommunikationsgeheimnis beeinträchtigen. Die Maßnahme soll sich nicht auf eine Durchsuchung beschränken, sondern auch eine anhaltende Überwachung umfassen, um Passwörter zu erspähen und alle elektronischen Aktivitäten zu protokollieren. Sie soll sich neben Computern auch auf andere Kommunikations- und Datenverarbeitungssysteme, wie Mobiltelefone und PDAs (Personal Digital Assistant) erstrecken. In vernetzten Systemen können auch unverdächtige Nutzer mitbetroffen sein.

Dabei ist nach wie vor völlig ungeklärt, wie der verfassungsrechtlich absolut geschützte Kernbereich privater Lebenssphäre bei der Online-Durchsuchung durch technische Maßnahmen gewährleistet werden soll. Darüber hinaus steht die Beweiseignung der gewonnenen Erkenntnisse in Frage, da die eingesetzte Software die auf den Festplatten gespeicherten Daten unbemerkt manipulieren kann. Schließlich führt bereits die Möglichkeit staatlicher Ausforschung des eigenen Computers mittels Schadsoftware („Bundestrojaner“) zu einem massiven Vertrauensverlust in die Sicherheit von Informationstechnik, insbesondere E-Government- und E-Commerce-Anwendungen und konterkariert

hohe Aufwendungen für IT-Sicherheit in Staat und Wirtschaft. Ob eine angekündigte enge Zweckbindung auf die Bekämpfung des Terrorismus tatsächlich erfolgt und lange anhält, darf aufgrund der Erfahrungen der letzten Jahre ernsthaft bezweifelt werden. Auch dürften Terrorverdächtige, anders als der normale Bürger, Mittel und Wege finden, sich der Online-Durchsuchung zu entziehen. Diese wird daher voraussichtlich kein Mehr an Sicherheit bringen, aber sicher die Freiheiten der Bürger einschränken.

9.24 Bericht aus dem Arbeitskreis Sicherheit

Der Arbeitskreis Sicherheit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, in dem ich mitarbeite, beschäftigt sich u. a. mit folgenden Themen: Konzeptionelle Weiterentwicklung des polizeilichen Informationssystems INPOL, Vorgangsbearbeitungssysteme bei den Polizeien der Länder, ein Gesichtserkennungssystem des Bundeskriminalamtes, der Stand der Einführung der Anti-Terror-Datei, die Gewährleistung des Kernbereichsschutzes und der Benachrichtigungspflicht bei verdeckten Ermittlungsmaßnahmen, die Ausweitung von sog. Zuverlässigkeitsüberprüfungen bei Akkreditierungsverfahren, datenschutzrechtliche Fragen bei der Durchführung der Operation „MIKADO“, Änderungen in Bezug auf Europol und das Schengener Informationssystem auf europäischer Ebene und die Zulässigkeit von Online-Durchsuchungen. In der Herbstsitzung wurde vor allem eine Stellungnahme zu der beim Bundesverfassungsgericht anhängigen Verfassungsbeschwerde gegen das Antiterrordateiengesetz abgestimmt. Ein weiteres Thema war erneut die Regelung zur Online-Durchsuchung im geplanten Bundeskriminalamtsgesetz, die Weiterentwicklung von INPOL, insbesondere die Protokollierung und die neuen Entwicklungen im Schengener Informationssystem und bei Europol, die zunehmend unmittelbare Auswirkungen auf das nationale Polizeirecht entfalten. Zudem widmete sich der Arbeitskreis erneut den verschiedenen Fallkonstellationen von Zuverlässigkeitsüberprüfungen auf Einwilligungsbasis und tauschte Erfahrungen zur Datenspeicherungspraxis durch den polizeilichen Staatsschutz aus.