Bericht der Aufsichtsstelle für Datenschutz

3. Bericht der Aufsichtsstelle für Datenschutz

3.1 Einleitung

3.1.1 Auf einen Blick

Mit der neuen Krankenversicherungsverordnung verpflichtet der Regierungsrat das Amt für Sozialversicherung und Stiftungsaufsicht – auf dessen Antrag – zu periodischen externen Kontrollen des Persönlichkeitsschutzes. Solche Kontrollen halten auch die Verantwortlichen der BEDAG-Informatik zum Betrieb des Rechenzentrums für nötig. Das Datenschutzgesetz geht dagegen immer noch von einem Konzept der Kontrollen durch die Datenschutzaufsichtsstelle aus. Diese haben sich aber als nicht machbar erwiesen. Die bisherige Vorgabe ist durch eine Verpflichtung der Datenbearbeiter zum Beizug externer Kontrollstellen zu ersetzen.
Ohne Vernehmlassungsverfahren hat der Bundesrat die Botschaft zum DNA-Profil-Gesetz (Verwendung von DNA-Profilen im Strafverfahren) an die Räte verabschiedet. Gerade aus Sicht der Datenschutzaufsichtsstelle des Kantons Bern ist dieser Verzicht auf ein Vernehmlassungsverfahren bedauerlich.

3.1.2 Zusammenarbeit mit dem eidgenössischen Datenschutzbeauftragten und den Datenschutzaufsichtsstellen der Kantone, VII. Nationale Konferenz der Datenschutzbeauftragten

Gemeinsam mit der fachtechnisch vorgesetzten Bundesstelle fördert der eidgenössische Datenschutzbeauftragte neu Ausbildungsveranstaltungen für kantonale Stellen, die Bundesrecht vollziehen. Das KIGA führte für die Mitarbeiter der regionalen Arbeitsvermittlungsstellen in diesem Rahmen Ausbildungsveranstaltungen zu Datenschutzfragen beim Umgang mit dem Informatiksystem AVAM durch. Für die Kader kantonaler Invalidenversicherungsstellen fand ein schweizerischer Kurs zu Datenschutzfragen statt. Das neue – praxisnahe – Ausbildungskonzept des eidgenössischen Datenschutzbeauftragten hat in beiden Fällen überzeugt.
Am 28. März gründeten eine Mehrheit der Kantone und der eidgenössische Datenschutzbeauftragte den Verein «Die schweizerischen Datenschutzbeauftragten, Les commissaires suisses à la protection des données, DSB+CPD.CH». Ab dem 1. Januar 2001 gehören dem Verein ausser dem Kanton Wallis alle Kantone an. Die vorbestehende Arbeitsgruppe der kantonalen Datenschutzaufsichtsstellen und des eidgenössischen Datenschutzbeauftragten hat damit eine schlagkräftigere Form erhalten. Ausbildungsveranstaltungen können besser finanziert und Stellungnahmen (vorab zu eidgenössischen Gesetzesvorlagen) mit einem verbesserten Stellenwert abgegeben werden. Der gemeinsame Nenner der Mitglieder darf allerdings nicht darüber hinwegtäuschen, dass die schweizerischen Datenschutzbeauftragten drei unterschiedliche Gruppen bilden: Die «professionellen», auch im Informatikbereich mit Ressourcen ausgestatteten Aufsichtsstellen, die als professionelle Anlaufstelle ausgestalteten Aufsichtsstellen und schliesslich die Milizaufsichtsstellen. Bern gehört zur zweiten Kategorie. Diese Zusammensetzung von DSB+CPD.CH ist nicht frei von Konflikten: Die Auseinandersetzung um das richtige Mass der Kontrolle gegenüber dem Dienstleistungszentrum für die Volkszählung illustriert dies.
An der VII. Nationalen Konferenz der Datenschutzbeauftragten in Basel wurden unter anderem Fragen zum E-Government behandelt.

3.2 Aufgabenumschreibung, Prioritäten, Mittel

3.2.1 Prioritäten

Für die Bearbeitung der Geschäfte gilt unverändert folgende Prioritätenfolge: 1. Informatikprojekte, 2. Allgemeine Gesetzgebung vor Spezialerlassen, 3. Generelle Weisungen vor Einzelfällen, 4. Beratung und Instruktion vor Inspektion und 5. Einzelprobleme mit vielen Betroffenen vor solchen mit wenig Betroffenen und geringen Wiederholungschancen. Geschäfte, die weder Rücksprachen bei andern Stellen noch langwierige eigene Abklärungen erfordern, werden als Tagesgeschäfte nach Eingang sofort erledigt. Die in früheren Jahresberichten erwähnten überlangen Wartezeiten für Rechtsauskünfte haben sich erwartungsgemäss verschlimmert. Wohl werden überalterte Geschäfte noch in der Geschäftskontrolle als hängig geführt, mit ihrer Erledigung rechnen die Fragesteller aber so wenig wie die Datenschutzaufsichtsstelle.
Verschiedene Kantone schaffen Dienststellen für die Informatiksicherheit (auch mit Kontrollaufgaben). Neben den Kantonen Freiburg (Sicherheitsverantwortlicher) und Zürich (Sicherheitsauditor beim Datenschutzbeauftragten) ist vorab der Kanton Waadt zu erwähnen: Dessen seit 1998 aufgebaute Sicherheitsorganisation (OSIC) umfasst ein fünfköpfiges Team mit Stützpunkten in den Departementen. Gerade im Hinblick auf eine Zusammenarbeit mit dem Kanton Waadt im Informatikbereich (Projekt INTEGRIS: BEDAG-Informatik als Rechenzentrum beider Kantone) ist zu fragen, ob der Kanton Bern seine Informatiksicherheitsorganisation nicht verbessern sollte (siehe auch 3.1.1 und 3.2.4).

3.2.2 Eigenverantwortung der Daten bearbeitenden Stellen

Nach wie vor besteht die Haupttätigkeit der Datenschutzaufsichtsstelle in Stellungnahmen zu Anfragen von amtlichen Stellen. Die Teilnahme solcher Stellen an Weiterbildungsveranstaltungen, die sich auch mit Datenschutzfragen befassen, ist hoch. Richtigerweise finden diese zunehmend in nationalem Rahmen statt (zu E-Government beispielsweise die vom Institut für Wirtschaft und Verwaltung der Berner Fachhochschule mitgetragene Veranstaltung vom 22. August in Zürich oder diejenige der BEDAG-Informatik vom 5. September in Bern). Mit dem Projekt SAVE II soll die Grundausbildung des Personals zur Informatiksicherheit auch in Zukunft durchgeführt werden können (interaktive Ausbildungs-CD-ROM, neu auch netzwerkfähig). Das Projekt «Integrale Sicherheit» der Justiz-, Gemeinde- und Kirchendirektion und der Finanzdirektion zeigt die Bereitschaft, für die Informatiksicherheit auch Mittel bereit zu stellen.

3.2.3 Verhältnis Informatikmittel/Mittel für Datenschutz und Datensicherheit

Im Jahr 2000 waren 28,1 Mio. Franken in Informatikmittel zu investieren. 116,3 Mio. Franken sollte der Betrieb der Informatikmittel kosten (Budgetzahlen). Mit rund 0,25 Mio. Franken sind die Gesamtkosten der Datenschutzaufsichtsstelle unverändert geblieben. Die Projekte «Integrale Sicherheit», BEMAIL II, SAVE II sind – wie auch der neu anfallende Jahresbeitrag an DSB+CPD.CH – positiv zu vermerken. Insgesamt steht aber der Aufwand für Informatik und derjenige für Datenschutz nicht in einem adäquaten Verhältnis.

3.2.4 Kontrollen von Informatikdatenbearbeitungen

Das DSG verpflichtet die Datenschutzaufsichtsstelle die Anwendung der Datenschutzvorschriften und die Informatiksicherheit zu kontrollieren. Schon im Vortrag zum Datenschutzgesetz hielt die Justizdirektion damals fest, die Überprüfungen verlangten von den Mitarbeitern der Aufsichtsstelle selbstverständlich auch ein gewisses technisches Fachwissen. Wie unter 3.1.1 dargelegt, ist dieses Kontrollkonzept gescheitert: Über die Ressourcen verfügen die Datenbearbeiter. Das Gesetz auferlegt ihnen aber einzig, bei Kontrollen mit der Datenschutzaufsichtsstelle zusammenzuarbeiten. Die Datenschutzaufsichtsstelle ihrerseits nimmt keine Kontrollhandlungen vor, da ihr die hierzu erforderlichen Ressourcen fehlen (Personal und Kredite). Dort wo die Ressourcen vorhanden sind, fehlen demnach die Pflichten und dort wo die Pflichten vorhanden sind, fehlen die Ressourcen. Der Regierungsrat hat – auf Antrag des Amtes für Sozialversicherung und Stiftungsaufsicht (ASVS) – dieses Konzept in der Krankenversicherungsverordnung umgedreht: Das über Ressourcen verfügende ASVS ist verpflichtet, periodisch eine externe Kontrollstelle beizuziehen. Die Datenschutzaufsichtsstelle kann sich darauf beschränken, die Qualität der Kontrollen zu überprüfen. Wie die Auseinandersetzungen über die Kontrollen gegenüber dem Dienstleistungszentrum für die Volkszählung gezeigt haben (auch hier bestand eine externe, durch das Dienstleistungszentrum zu finanzierende Kontrollstelle), sind noch Fragen zu klären. Es ist aber damit zu rechnen, dass sich von der Privatwirtschaft (Banken) ausgehende Kontrollstandards durchsetzen werden. Offensichtlich dürfte sein, dass ein Kanton heute kaum mehr in der Lage ist, in eigener Regie kompetente Kontrollstellen aufzubauen. Etwa um die Zugriffsberechtigungen im Rechenzentrum der BEDAG zu kontrollieren, bedurfte es denn auch ausländischer Spezialisten. Das in der Krankenversicherungsverordnung erstmals umschriebene Prinzip, das die Datenbearbeiter mit einbindet, muss aus Sicht der Datenschutzaufsichtsstelle weiter verbreitet werden.

3.2.5 Aufgaben

Mit dem neuen Informationskonzept des Kantons entfällt für die Datenschutzaufsichtsstelle die Möglichkeit, in der Personalzeitschrift BE-info regelmässig Artikel erscheinen zu lassen. Ihre Ressourcen erlauben es der Datenschutzaufsichtsstelle nicht, eigene Informationsinfrastrukturen aufzubauen. Es wird somit darum gehen müssen, bestehende Informationsinfrastrukturen auch für Datenschutzinformationen einzusetzen. Zu denken ist etwa an Internetseiten des Amtes für Gemeinden und Raumordnung oder (künftig) des Rechtsamtes der Justiz-, Gemeinde- und Kirchendirektion.

3.2.6 Register

Das Inselspital reichte im Juni die bei ihm erfolgten 224 Anmeldungen in das Register der Datensammlungen ein. Weder durch den Datenschutzbeauftragten des Inselspitals, noch durch die kantonale Datenschutzaufsichtsstelle erfolgte eine Prüfung. Eine erste Sichtung zeigte durchaus einen erheblichen Handlungsbedarf (etwa zu den Aufbewahrungsfristen). Die Ressourcen dazu fehlen jedoch. Der gesetzliche Auftrag bleibt hier genau so unerfüllt wie beim Gesamtregister, dessen Stand unverändert ist (812 ungeprüfte Einträge).

3.3 Datensicherheit

3.3.1 Sollvorgaben

Beauftragte die kantonale Informatikkonferenz im Vorjahr das Organisationsamt noch mit der Prüfung einer Übernahme des Regelwerks des Kantons Zürich, beschloss sie im Berichtsjahr neu, dasjenige des Bundes (Weisung S 02) weiter zu verfolgen. Nicht zuletzt Probleme mit der Übersetzung waren für diesen Beschluss massgebend. Die Ergebnisse des Projektes «Integrale Sicherheit» sollen zudem vor einem Entscheid abgewartet werden. Mit diesem zögerlichen Vorgehen vergrössert sich der Rückstand des Kantons Bern gegenüber andern Kantonen. Die teilweise überalterten, uneinheitlichen und unvollständigen Informatiksicherheitssollvorgaben bilden kein tragfähiges Fundament für die Informatiksicherheit. Eine Lösung des Problems drängt. Dass die Verantwortlichen diesen Umstand bei der Suche nach der guten Lösung nicht aus dem Auge verlieren, ist (nicht zuletzt mit Blick auf hängige Verfahren: Betriebsbewilligung der Datenbearbeitungssysteme der Kantonspolizei: vgl. 3.8.1) anzumahnen.
Die Geschäftsleitung der BEDAG-Informatik setzte für das Rechenzentrum den british standard 7799 (Management von Informationssicherheit) in Kraft.

3.3.2 Sicherheit von E-Mail

In seiner Weisung Nr. 4 regelt das Organisationsamt die Verantwortlichkeiten im Umgang mit E-Mail und gibt den E-Mail-Benutzenden Rahmenbedingungen. Der Regierungsrat beschloss das Projekt BEMAIL II: Neben technischen Verbesserungen des bestehenden Mail-Systems sieht dieser Beschluss erneut auch Mittel für die Einführung sicherer E-Mails vor. Eine beschränkte Anzahl von E-Mail-Benutzenden soll – unter Einsatz einer vorbestehenden, externen Zertifikationsstelle – digital signierte Mails intern und extern versenden und empfangen können. Für die Pilotphase waren rechtliche Sollvorgaben zu machen. Erneut erwies sich dies, etwa zum Umgang des Benützers mit dem privaten Schlüssel, als schwierig. Auch der neuen Bundesversuchsverordnung über Dienste der elektronischen Zertifizierung ist hierzu einzig zu entnehmen, der Zertifizierungsdienst müsse dem Benutzer geeignete Massnahmen zur Geheimhaltung des privaten Schlüssels vorschlagen. In diesem mathematisch und informatiktechnisch hochkomplexen Umfeld mag die Verwaltung allenfalls noch in der Lage sein, die Tauglichkeit der vorgeschlagenen Massnahmen zu beurteilen. Der Bürger aber – als Mail-Absender und -Empfänger – wird hierzu nicht in der Lage sein. Sicheres E-Mail ist für E-Government ein zentrales Mittel. Es wird überkantonalen Stellen obliegen, mit Normen und Komponenten bürgerfreundliche Lösungen zu schaffen, zu denen ein verantwortungsvoller Bürger auch ja sagen kann.

3.3.3 Viren, I-love-you-Virus

Der Kanton Bern ist vor diesem Virus nicht verschont geblieben. Seine Informatik ist nicht weniger verletzlich als diejenige der Bundesverwaltung oder der Privatwirtschaft. Die Überarbeitung von Alarmierungs- bzw. Notfallkonzepten wurde angegangen.
Die Aktualisierung von Virenschutzprogrammen hat rasch zu erfolgen. In einem professionellen Umfeld dürfen aber auch diese (wöchentlichen) Updates erst nach einem Test verteilt werden: Unverträglichkeiten der Updates mit dem eingesetzten Virenscanner führten in einer Direktion während einer kurzen Zeitspanne praktisch flächendeckend zum Ausfall der Informatik.

3.4 Informatikprojekte

Das Projekt GELAN 2002 der Volkswirtschaftsdirektion (Auszahlung von Beiträgen an Landwirte gemeinsam mit den Kantonen Freiburg und Solothurn) wurde mit einem Workshop fortgesetzt. Ein Mitarbeiter des KIGA verfasste ein Sicherheitskonzept. Das Amt für Wald und Natur liess abklären, welche Rechtsgrundlagen zur Publikation der Försterverzeichnisse auf Internet erforderlich sind. Das

Amt für Finanzen und Administration der Erziehungsdirektion unterbreitete seine Online-Anmeldeformulare für die Lehrmeisterkurse zur Prüfung. Zum Projekt BEMAIL II siehe 3.3.2. Während für das Projekt GRUDIS (Grundstückinformationssystem der Justiz-, Gemeinde- und Kirchendirektion) eine Mitarbeit der Datenschutzaufsichtsstelle in der Arbeitsgruppe Recht eingeleitet wurde, verzichtete die Finanzdirektion auf ein Unterbreiten des Systems KOFINA (Ablösung des bisherigen Finanzverwaltungssystems). Wohl ist die Einschätzung richtig, dass eine Prüfung dieses Projekts zu Kapazitätsengpässen bei der Datenschutzaufsichtsstelle geführt hätte. In Anbetracht der Bedeutung des Projekts ist das Vorgehen allerdings bedauerlich.

3.5 Internet und E-Government

Insgesamt 52 Mio. Franken will der Bundesrat für die Jahre 2001–2004 für das E-Government-Projekt «Guichet virtuel» bereitstellen. Der Kanton Bern hat für eine Teilnahme bereits in der Pilotphase Interesse. Die Datenschutzaufsichtsstelle begrüsst das Projekt, das nicht zuletzt datenschutzfreundliche Technologien fördern soll und auch Kantone und Gemeinden mit den Vorgaben zum Persönlichkeitsschutz im Umgang mit Internet vertraut machen will. Wenn kantonale Datenschutzaufsichtsstellen in das Projekt bisher nicht einbezogen worden sind, dürfte deren Ressourcensituation zwar richtig eingeschätzt worden sein. Die Bedeutung des Datenschutzes für E-Government-Projekte gebietet aber einen Beizug.
Hinweise zu E-Government-Projekten sind im Berichtsjahr im Übrigen zur Routinearbeit geworden: Rechtsgrundlagen für das weltweite Zugänglichmachen von Personendaten mittels Abrufverfahren müssen nach wie vor noch geschaffen werden. Elektronische Datenübertragungen (z. B. E-Mail) ohne Verschlüsselung sind unsicher und dürfen für das Übertragen von besonders schützenswerten Daten nicht Einsatz finden. Auch wenn Daten (z. B in elektronischen Formularen mit SSL) verschlüsselt übertragen werden, ist die Identität des Bürgers ohne digitale Signatur nicht überprüfbar. Damit sind Antworten, die nur einem identifizierten Bürger zustehen, auch über diese verschlüsselte Verbindung nicht zu erteilen.
Mit dem Projekt «Guichet virtuel» des Bundes wird E-Government in einem bewussten Schritt eingeführt. Dessen Einführung kann auch schleichend als Folge technischer Änderungen erfolgen (ein Grossteil der Verwaltungsstellen ist heute über E-Mail erreichbar und hat die Möglichkeit Informationen auf Internetseiten bekanntzugeben). Auch vor Privaten, die öffentliche Aufgaben erfüllen, macht diese Erscheinung nicht halt: Ein Vereinsmitglied eines Schiessvereins baute für den Verein eine Internetseite auf. Den Schiessvereinen obliegt als öffentliche Aufgabe die Durchführung der obligatorischen Schiessübungen. Deren Ergebnisse auf Internet bekannt zu geben war damit bereits eine Aktivität des E-Government. Eine unzulässige allerdings: Gestützt auf einen Hinweis eines Betroffenen empfahl die Datenschutzaufsichtsstelle, die Schiessresultate von der Seite zu entfernen. Der Verein akzeptierte die Empfehlung. (Vergleiche zu E-Government auch: 3.2.2, 3.2.4 und 3.3.2).

3.6 Gesetzgebung

Im Entwurf zum Sozialhilfegesetz wird die bisherige besondere Geheimhaltungspflicht aufgegeben. Die Datenschutzaufsichtsstelle begrüsst diesen Schritt: Massnahmen der sozialen Hilfe oder fürsorgerischen Betreuung sind besonders schützenswerte Daten. Für diese besteht ein hoher Schutz. Diesen hohen Schutz zusätzlich mit dem durch die besondere Geheimhaltungspflicht entstehenden Schutz zu überlagern macht nur Sinn, wenn dem Schutzbedürfnis der Betroffenen anders nicht entsprochen werden kann. Im Umfeld der Sozialhilfe fehlt es an einem solchen Bedürfnis. Der bisherige «doppelte» Schutz ist viel mehr dadurch zu erklären, dass das «Fürsorgegeheimnis» als besondere Geheimhaltungspflicht bereits vor der Datenschutzgesetzgebung (Einführung der besonders schützenswerten Daten) bestand.
Gegenüber dem neuen Personalgesetz (PELAG) war festzuhalten, dass zu spezifischen Datenschutzregelungen zum Umgang mit Lohndaten kein Anlass besteht.
Die Mitarbeit in der Arbeitsgruppe zum Überarbeiten des Gesetzes über die BEDAG-Informatik erlaubt es der Datenschutzaufsichtsstelle, zu einem frühen Zeitpunkt auf Datenschutzfragen in diesem Umfeld hinzuweisen.
Zur Krankenversicherungsverordnung siehe 3.1.1. und 3.2.4.
Zu Bundeserlassen beschränkt sich die Datenschutzaufsichtsstelle darauf, sich den von DSB+CPD.CH ausgearbeiteten Stellungnahmen zuhanden der Bundesstellen anzuschliessen oder diese kantonsintern in das Vernehmlassungsverfahren einzureichen. Dies betraf den Artikel 179 StGB, das Öffentlichkeitsgesetz und das Ausländergesetz. Zum EDNA-Profil Gesetz siehe Ziffer 3.9.1.

3.7 Gemeinderechtliche Körperschaften

3.7.1 Allgemeines

Ein hoher Anteil der erteilten Rechtsauskünfte geht nach wie vor an gemeinderechtliche Körperschaften. Die Ausbildung von neuen Gemeindebehördemitgliedern (organisiert durch das Amt für Gemeinden und Raumordnung) und von Gemeindemitarbeitern (organisiert von den Berufsverbänden, im Berichtsjahr erstmals auch für den Berner Jura) erscheint sinnvoll.
Geburten werden von den Zivilstandsämtern nach ihrer Reorganisation neu nicht mehr gemeldet. Gegenüber Privaten können die Einwohnerkontrollen diese Meldungen nicht ersetzen. Gegenüber Behörden, auch gegenüber mit öffentlichen Aufgaben betrauten Privaten wie etwa die Väter- und Mütterberatung, sind sie aber zur Meldung verpflichtet.
Videoüberwachungen sind gerade auch für Gemeinden aktuell. Dies zeigte einerseits der Beschluss des Gemeinderats von Bern vorerst auf eine Überwachung öffentlicher Plätze zu verzichten, andererseits das Eingeständnis einer kleinen Gemeinde, bei der zur Überwachung der Kehrichtsammelstelle eingesetzten Videokamera handle es sich einzig um eine Attrappe.
Wenn Milizbehördemitglieder zu Hause und von zu Hause aus oder von ihrem Arbeitsplatz aus für die Gemeinde mit elektronischen Mitteln arbeiten, hat diese Arbeit alle Merkmale der Telearbeit. Die hierzu bestehenden Informatiksicherheitsvorgaben werden dabei aber in aller Regel nicht umgesetzt. Handlungsbedarf besteht.
Nach einem Serverabsturz stellte die St. Galler Stadtverwaltung fest, dass ihre regelmässig gemachten Datensicherungen seit längerer Zeit leer waren. Das legte Teile der Verwaltung während einer Woche lahm und allein die Datenrekonstruktion hätte einen Schaden von einer halben Million Franken ausgelöst. Es ist davon auszugehen, dass sich ähnliche Vorfälle auch in Berner Gemeinden ereignen könnten.

3.7.2 Volkszählung

Die Aufgaben des bundesrechtlich vorgeschriebenen Kontrollorgans für die Volkszählung oblag im Kanton Bern den Datenschutzaufsichtsstellen der Gemeinden. Die Datenschutzaufsichtsstelle beschränkte sich darauf, in einem Rundschreiben die Aufgabenstellung zu konkretisieren. Eine Beurteilung der Qualität der durchgeführten Kontrollen ist zurzeit schon deshalb verfrüht, weil die Aufgabe nicht abgeschlossen ist. Auffällig ist immerhin, dass Anzeichen für ein Ernstnehmen der Aufgabe nicht fehlen: Eine beigezogene professionelle Revisionsstelle erstellte beispielsweise eine praxistaugliche Checkliste und stellte diese auch allen weiteren von ihr betreuten Gemeinden zur Verfügung. Eine Milizaufsichtsbehörde stellte fest, dass die Gemeindeverwaltung die erstmals erlaubte

Zuordnung der Haushaltsnummern an die Einwohner ohne Rechtsgrundlage bereits seit längerer Zeit vorgenommen hatte. Zu den Differenzen betreffend Kontrollhandlungen gegenüber dem Dienstleistungszentrum siehe 3.1.2 und 3.2.4.

3.8 Berichtspunkte des Vorjahres

3.8.1 Betriebsbewilligung für die Datenbearbeitungssysteme der Kantonspolizei

Die Vorarbeiten für den entsprechenden Regierungsratsbeschluss nahmen im Berichtsjahr ihren Fortgang. Ein Abschluss der Arbeiten ist für die erste Hälfte 2001 zu erwarten.

3.8.2 Sicherheit von E-Mail

Siehe 3.3.2.

3.9 Besonderes

3.9.1 DNA

Jeder Umgang des Staates mit DNA birgt Gefahren: Genetisches Material erlaubt beispielsweise Aussagen über den aktuellen Gesundheitszustand und über künftige gesundheitliche Entwicklungen (Erbkrankheiten). Es kann auch Aussagen über weitere Eigenschaften der Betroffenen erlauben. Auch das zur Identifizierung dienende DNA-Profil allein erlaubt Aussagen über verwandtschaftliche Beziehungen und lässt Zuordnungen zu Herkunftsgruppen zu. Welche Aussagen künftige Forschungsergebnisse erlauben werden, ist offen. Der Umgang mit DNA erfolgt in hochtechnisierten Abläufen. Bei Fehlleistungen genügt die Lebenserfahrung der Betroffenen zu Richtigstellungen häufig nicht.
Die im Vorjahresbericht erwähnte Weisung der Erziehungsdirektion für den Persönlichkeits- und Datenschutz am Institut für Rechtsmedizin ist Ende März in Kraft gesetzt worden. Am 1. Juli trat die EDNA-Verordnung des Bundesrates in Kraft. Gestützt darauf betreibt der Bund eine DNA-Profildatenbank (auf dreieinhalb Jahre befristeter Versuchsbetrieb). In einem Deliktskatalog sind die Delikte aufgezählt, die zu einer Aufnahme des DNA-Profils in die Datenbank führen dürfen. Die Justiz-, Gemeinde- und Kirchendirektion hielt in einer Stellungnahme an die Polizei- und Militärdirektion fest, der Kanton Bern dürfe sich am Versuchsbetrieb beteiligen. Zur Erhebung der DNA-Profile genüge die aktuelle Strafverfahrensgesetzgebung als Rechtsgrundlage. Ob die bundesrechtliche Verordnungsgrundlage für den Betrieb der DNA-Datenbank genüge, brauche aus Sicht der Kantone nicht weiter geprüft zu werden. Das bernische Strafverfahren verlange aber immer, also auch dann, wenn ein Delikt im Deliktskatalog des Bundes enthalten sei, eine einzelfallweise Prüfung der Verhälnismässigkeit des mit der DNA-Profilierung verbundenen schweren Eingriffs in die Persönlichkeitsrechte des Betroffenen.
Eine Vertretung von DSB+CPD.CH konnte Mitte Juni an einem Hearing zum Entwurf zu einem DNA-Profil-Gesetz des Bundes teilnehmen. In schwer verständlichem Gegensatz zu dieser Mitwirkungsmöglichkeit steht der Umstand, dass der Entwurf zu diesem Gesetz mit Botschaft vom 8. November durch den Bundesrat ohne Vernehmlassungsverfahren verabschiedet worden ist. Unzutreffend ist jedenfalls, dass sich die Interessierten in der Vernehmlassung zum Entwurf eines Bundesgesetzes über genetische Untersuchungen beim Menschen zur Frage der Ausgestaltung der DNA-Datenbank zu Strafverfolgungszwecken hätten äussern können: Dieser Entwurf behielt die Regelung der DNA-Datenbank vielmehr gerade der Spezialgesetzgebung vor. Zudem war die Justizreform, die dem Bund die Kompetenz zu strafprozessualen Bestimmungen gibt, damals noch nicht verabschiedet. Gerade aus Sicht der Datenschutzaufsichtsstelle des Kantons Bern weckt der Verzicht auf eine Vernehmlassung Bedenken, lösten die gleichen Fragen auf kantonaler Ebene im Vernehmlassungsverfahren zu den DNA-Bestimmungen im bernischen Strafverfahren doch engagierte Stellungnahmen aus. Wird nun die gleiche Materie in einem auch im Kanton Bern vollumfänglich anwendbaren Bundesgesetz geregelt, bleibt das Bedürfnis der Betroffenen im Vernehmlassungsverfahren Gehör zu finden, unvermindert gross. Dies umso mehr, als mit dem Versuchsbetrieb der eidgenössischen DNA-Datenbank die zeitliche Dringlichkeit für das Gesetzgebungsverfahren nicht mehr gegeben ist.
Im Entwurf zum DNA-Profil-Gesetz wird der im aktuellen Versuchsbetrieb angewendete (und im Entwurf zum bernischen Strafverfahren ebenfalls enthaltene) Deliktskatalog zu Gunsten einer umfassenden DNA-Profilierung aufgegeben. Der Bereich, in dem Löschungen in der Datenbank einzig auf Gesuch der Betroffenen und nicht von Amtes wegen vorgenommen werden, ist sodann zu weit gefasst.
Eine differenzierte Überprüfung des Entwurfs ist nötig: So sollten etwa die Ergebnisse aus der aktuellen Versuchsphase mit der eidgenössischen DNA-Datenbank Berücksichtigung finden. Es ist vor diesem Hintergrund verständlich, wenn die Polizeiverantwortlichen angesichts der hochanspruchsvollen Umsetzung der DNA-Technik erste Fahndungserfolge der eidgenössischen DNA-Datenbank hervorheben. Im Hinblick auf das künftige Gesetz wird allerdings nicht nur das Funktionieren der Strafverfolgung mittels DNA-Profilen darzulegen sein, sondern vor allem, in welchen Bereichen eine Verbesserung gegenüber den bisherigen Mitteln (Fingerabdruck) erzielt werden kann. Erst mit solchen Informationen wird der Gesetzgeber abwägen können, wo sich der mit der DNA-Profilierung verbundene schwere Eingriff in die Persönlichkeitsrechte der Betroffenen rechtfertigen lässt.

3.9.2 Feststellung der Kundenzufriedenheit in der Psychiatrie

Mit einem von einer amerikanischen Firma ausgearbeiteten Fragebogen befragten zwei Kliniken im Rahmen der neuen Verwaltungsführung (NEF) austretende Patientinnen und Patienten über ihre Zufriedenheit mit der Behandlung. Die Datenschutzkommission einer Klinik warf die Frage auf, ob die Anonymisierung der Fragebogen nicht entscheidend verbessert werden müsse. Sie wies zudem daraufhin, die Zustimmung zur Mitbekanntgabe von Diagnosedaten nach dem ICD 10 Code erfolge zu unklar. Dies auch vor dem Hintergrund, dass Patientenantworten gestützt auf Diagnoseangaben relativiert würden. Die Datenschutzaufsichtsstelle bestätigte die Bedenken und stellte weitere Mängel beim Fragebogen fest (beispielsweise eine mögliche unzulässige Erhebung von Daten über das Personal bei Patienten). Die Verantwortlichen der Gesundheits- und Fürsorgedirektion erarbeiteten rasch und umfassend einen datenschutzkonformen Fragebogen.

3.9.3 Universität

Im März erfolgte auf das Computersystem der Universität Bern ein Hackerangriff. Es entstand kein Schaden. Im April berichteten die Medien über kinderpornografische Bilder, die auf einem Server der Uni abrufbar abgelegt waren. Die Universitätsleitung setzte darauf eine Task-Force ein, der auch die Datenschutzaufsichtsstelle angehörte. Neben der Einführung einer Benutzerkennung und der Schaffung eines Sicherheitsdienstes beantragte die Task-Force der Universitätsleitung, Informatikweisungen zu erlassen und das Einsetzen eines Konsultativgremiums der Universitätsleitung in Fragen der Informatiksicherheit und eines Datenschutzberaters zu prüfen. Die Anträge werden zurzeit geprüft, die Weisungen sind erlassen worden.

3.9.4 **Telefonabhörmöglichkeit**

Eine aufmerksame Mitarbeiterin wies die Datenschutzaufsichtsstelle darauf hin, sie habe die Möglichkeit Telefongespräche (im konkreten Fall auch diejenige eines Regierungsmitgliedes) abzuhören. Die mit dem Organisationsamt durchgeführten Abklärungen zeigten, dass diese Möglichkeit durch mehrere Programmaufdatierungen der Telefonapparate ungewollt entstanden war. Wohl war beim Aufschalten für die Gesprächsteilnehmer ein Warnton hörbar. Dieser war aber von den regelmässig auch aus andern Gründen hörbaren Warntönen (z. B. leere Akkus bei Funktelefonen oder Handys) nicht zu unterscheiden und wurde von den Betroffenen nicht wahrgenommen. Das Organisationsamt liess die Apparate inzwischen umprogrammieren.

16. Januar 2001

Der Datenschutzbeauftragte: *Siegenthaler*