Unterrichtung

Der Niedersächsische Ministerpräsident Hannover, den 10.06.2005

Herrn
Präsidenten des Niedersächsischen Landtages

Hannover

Sehr geehrter Herr Präsident,

als Anlage übersende ich die

Stellungnahme der Landesregierung zum XVII. Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz Niedersachsen (Drs. 15/1580)**.**

Federführend ist das Ministerium für Inneres und Sport.

Mit vorzüglicher Hochachtung

Christian Wulff

Inhaltsverzeichnis

Vorbemerkung:

Der vom Landesbeauftragten für den Datenschutz (LfD) gemäß § 22 Abs. 3 Satz 1 Niedersächsisches Datenschutzgesetz (NDSG) vorgelegte Tätigkeitsbericht für die Jahre 2003 und 2004 unterscheidet sich maßgeblich von den Berichten der Vorjahre und ist nach seinen Angaben Ausdruck eines neuen Ansatzes. Die Tätigkeitsberichte der Vorjahre enthielten vor allem datenschutzrechtlich relevante Sachverhalte aus dem öffentlichen Bereich und deren rechtliche Bewertung, außerdem wurden wichtige Tätigkeitsfelder aus dem nicht öffentlichen Bereich beschrieben. In dem aktuellen Bericht beabsichtigt der LfD, in Anlehnung an andere Jahresberichte in Wirtschaft und Verwaltung nunmehr in einer Art „Management summary“ über wichtige Entwicklungen des Datenschutzes und bedeutsame Ergebnisse seiner Arbeit zu berichten.

Der Bericht gibt im Vergleich zu den Vorjahren und zu den Tätigkeitsberichten der anderen Länder und des Bundes weniger Auskunft darüber, inwieweit sich der LfD und die Mitarbeiterinnen und Mitarbeiter der Geschäftsstelle im Tätigkeitszeitraum mit den verschiedenen datenschutzrechtlichen Problemen im Einzelfall zu befassen hatten. Für die Dokumentation der Einzelergebnisse seiner Tätigkeit verweist der LfD auf sein Internetangebot. Es bleibt abzuwarten, ob mit dem Wechsel der Berichtsart das vom LfD angestrebte Ziel, eine bessere Grundlage für eine problembezogene Erörterung des Tätigkeitsberichts im Landtag und in seinen Ausschüssen zu schaffen, erreicht und angenommen wird.

Die Landesregierung unterstützt die vom LfD angestrebte frühzeitige Beratung und Mitgestaltung von datenschutzgerechten Lösungen, wie sie bei der Ausarbeitung von Rechts- und Verwaltungsvorschriften im NDSG ihren Ausdruck finden. Die Landesregierung weist jedoch darauf hin, dass es allein der Entscheidung der Abgeordneten des Niedersächsischen Landtages vorbehalten bleibt, inwieweit die im Rahmen der Beratung und des Anhörungsrechts des LfD gegebenen datenschutzrechtlichen und -politischen Stellungnahmen die Entscheidungsabläufe und Meinungsbildungsprozesse beeinflussen werden. Datenschutzrechtliche Belange sind in der Regel immer nur neben anderen wie z. B. sicherheits-, wirtschafts- oder sozialpolitischen Aspekten zu berücksichtigen und zu gewichten.

Aus Sicht der Landesregierung ist von datenschutzrechtlicher Bedeutung für den Tätigkeitszeitraum vor allem die Ergänzung des § 25 a NDSG durch Artikel 11 des Gesetzes zur Änderung des Niedersächsischen Verwaltungsverfahrensgesetzes und anderer Gesetze vom 16.12.2004 (Nds. GVBl. S. 634). Diese Vorschrift ist in vollem Einvernehmen mit dem LfD erarbeitet worden. Sie trägt in erheblichem Maße zur Rechtssicherheit bei, da nunmehr die Einzelheiten der durch Bildübertragung erfolgenden Beobachtung von öffentlich zugänglichen Räumen im Umfeld öffentlicher Einrichtungen vor allem des Landes und der Kommunen ausdrücklich geregelt werden.

Die Stellungnahme der Landesregierung beschränkt sich im Folgenden auf die öffentlichen Bereiche, für die der LfD einen „datenschutzrechtlichen Handlungsbedarf“ geltend gemacht hat:

Zu 1: Lauscher an der Wand oder:
Die Entscheidungen des Bundesverfassungsgerichts vom 03.03.2004 und ihre Folgen

Auf der Grundlage der beiden am 03.03.2004 getroffenen Entscheidungen des Bundesverfassungsgerichts (BVerfG) zum sogenannten Großen Lauschangriff und zur präventiven Überwachung der Telekommunikation durch das Zollkriminalamt fordert der LfD, dass alle Regelungen im niedersächsischen Landesrecht, die durch verdeckte Datenerhebungen in das Recht auf unbeobachtete Kommunikation aus Artikel 10 und 13 GG oder in das Recht auf informationelle Selbstbestimmung aus Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG eingreifen, darauf hin überprüft werden müssten, ob sie die Grenzen, die sich aus einem absolut geschützten Kernbereich privater Lebensgestaltung ergeben, einhalten. Auch bundesgesetzliche Regelungen sollten auf notwendigen Änderungsbedarf hin untersucht werden.

Auswirkungen auf Bundesrecht

Die aufgrund der Entscheidungen des BVerfG vom 03.03.2004 unmittelbar notwendig gewordenen Änderungen von Bundesgesetzen sind bereits vollzogen oder in absehbarer Zeit zu erwarten.

Das Gesetz zur Neuregelung der präventiven Telekommunikations- und Postüberwachung durch das Zollkriminalamt (NTPG) vom 24.12. 2004 (BGBl. I S. 3603) ist am 28.12.2004 in Kraft getreten. Der Bundestag hat das Gesetz zur Umsetzung des Urteils des BVerfG vom 03.03.2004 (akustische Wohnraumüberwachung) am 12.05.2005 verabschiedet und dem Bundesrat zugeleitet. Dieser hat in seiner Sitzung am 27.05.2005 beschlossen, den Vermittlungsausschuss anzurufen. Das weitere Vermittlungsverfahren bleibt somit abzuwarten.

Die Landesregierung hat sich im Rahmen dieser Gesetzgebungsverfahren dafür eingesetzt, dass einerseits die Rechte der Betroffenen gewahrt, andererseits aber auch die Belange einer effektiven Strafverfolgung und der Schutz der Bevölkerung gebührende Berücksichtigung finden. An dieser Linie wird die Landesregierung weiterhin festhalten. Eine wirksame Kriminalitätsbekämpfung ist ohne verdeckte Ermittlungsmaßnahmen wie etwa die Telekommunikationsüberwachung undenkbar.

Dass sich die Strafverfolgungsbehörden und Gerichte insgesamt der Tragweite von verdeckten Ermittlungsmaßnahmen und der sich daraus ergebenden besonderen Verantwortung bewusst sind, lässt sich dem Abschlussbericht des Max-Planck-Instituts für ausländisches und internationales Strafrecht zur Rechtswirklichkeit und Effizienz der akustischen Wohnraumüberwachung („großer Lauschangriff“) nach § 100 c Abs. 1 Nr. 3 Strafprozessordnung (StPO) entnehmen. Die umfassende Untersuchung aller in den Jahren 1998 bis einschließlich 2001 durchgeführten Wohnraumüberwachungsmaßnahmen kommt zu dem Ergebnis, dass die Strafverfolgungsbehörden und Gerichte verantwortungsvoll, behutsam und sorgfältig mit dem Ermittlungsinstrument der akustischen Wohnraumüberwachung umgehen. Darüber hinaus wird die Unverzichtbarkeit dieser Maßnahme als Instrument effektiver Strafverfolgung festgestellt und bestätigt.

Auswirkungen auf das niedersächsische Landesrecht

Auch wenn das BVerfG unmittelbar nur über die Bestimmungen zur akustischen Wohnraumüberwachung nach der Strafprozessordnung entschieden hat, so hat die Landesregierung diese Entscheidung vor dem Hintergrund der in dem Niedersächsischen Gesetz über die öffentliche Sicherheit und Ordnung (Nds. SOG) und dem Niedersächsischen Verfassungsschutzgesetz (NVerfSchG) getroffenen Regelungen sehr ernst genommen und wird die nach eingehender Prüfung sich als erforderlich darstellenden Änderungen in entsprechenden Novellierungsgesetzen vorlegen.

Dabei werden auch die Vorgaben der zweiten Entscheidung des BVerfG zur präventiven Überwachung der Telekommunikation durch das Zollkriminalamt zu berücksichtigen sein. Allerdings hat das BVerfG mit dieser Entscheidung eine präventive Telekommunikationsüberwachung durch das Zollkriminalamt unter bestimmten Voraussetzungen für zulässig erachtet und eine Verletzung des Kernbereichs privater Lebensgestaltung gerade nicht festgestellt.

Bei der Prüfung ist insbesondere zu berücksichtigen, dass die in der StPO geregelte repressive Tätigkeit von Polizei und Staatsanwaltschaft und die Vorschriften zur präventiven Tätigkeit der Polizei nach dem Nds. SOG und des Verfassungsschutzes nach dem NVerfSchG dem Schutz unterschiedlicher Rechtsgüter dienen, sodass eine generelle Übertragung der Vorgaben des Urteils des BVerfG angesichts dieser unterschiedlichen Rechtsgüter und Anwendungsbereiche nicht möglich ist. Vielmehr bedarf es einer differenzierten Betrachtungsweise und Entscheidung, ob und welche Vorgaben des BVerfG auf die Regelungen des Nds. SOG und NVerfSchG zur Wohnraumüberwachung übertragbar sind. Entsprechende Entscheidungen werden zurzeit vorbereitet.

Die Forderung des LfD, die vom BVerfG gemachten Vorgaben zur Wohnraumüberwachung nach der StPO auf alle verdeckten Datenerhebungen, die in das Recht auf informationelle Selbstbestimmung eingreifen, zu übertragen, führt zu weit und findet in dem Urteil selbst keinerlei Bestätigung. Änderungen des Niedersächsischen Ausführungsgesetzes zum Artikel 10-Gesetz oder Initiativen zur Änderung von Bundesrecht (Artikel 10-Gesetz) sind daher nicht beabsichtigt.

Zu 2: Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung (Nds. SOG)

Bei der Beurteilung der Verfassungsmäßigkeit der §§ 33 a ff. Nds. SOG bleibt die Entscheidung des BVerfG über die Normenkontrollklage eines niedersächsischen Bürgers abzuwarten. Erst dann wird zu klären sein, ob und ggf. welcher gesetzgeberischer Handlungsbedarf besteht.

Es bleibt bis dahin festzustellen, dass das BVerfG mit seinem Beschluss vom 03.03.2004 jedoch grundsätzlich eine präventive Telekommunikationsüberwachung durch das Zollkriminalamt unter bestimmten Voraussetzungen für zulässig erachtet, die der Bund mit dem NTPG erneut geregelt hat.

Das Gericht hat die präventive Telefonüberwachung als ein für die Verhütung von Straftaten erforderliches polizeiliches Instrument anerkannt. Vor diesem Hintergrund kann die Kritik des LfD an der Verlagerung der Aufgaben und Befugnisse der Polizei in das Vorfeld von Gefahren und Straftaten nicht geteilt werden.

Die Befürchtung des LfD, durch die §§ 33 a ff. Nds. SOG entferne sich die Polizei so weit von ihren klassischen Aufgaben der Gefahrenabwehr und Strafverfolgung, dass man ihre Aufgaben und Befugnisse demnächst nicht mehr von denen des Verfassungsschutzes wird unterscheiden können, wird nicht geteilt.

Das Trennungsgebot ist eine Reaktion der Alliierten auf den Terror der Gestapo im Dritten Reich und geht zurück auf den so genannten „Polizeibrief“ der drei alliierten Militärgouverneure aus dem Jahr 1949 an den Präsidenten des Parlamentarischen Rates. Darin wurde der Bundesregierung gestattet, eine Stelle einzurichten zur Sammlung und Verbreitung von Auskünften über umstürzlerische, gegen die Bundesrepublik gerichtete Tätigkeiten. Diese Stelle sollte angesichts der Erfahrungen der jüngsten Vergangenheit keine Polizeibefugnisse haben. Zweck war in erster Linie, die Entstehung eines Supergeheimdienstes nach Art der Gestapo von vornherein zu verhindern. Aus diesem „Polizeibrief“ hat sich das auch heute noch aktuelle Trennungsgebot zwischen Nachrichtendiensten und Polizei entwickelt, das in verschiedenen einfachgesetzlichen Regelungen seinen Niederschlag gefunden hat. So ist in § 2 Abs. 2 NVerfSchG geregelt, dass das Niedersächsische Landesamt für Verfassungsschutz einer polizeilichen Dienststelle nicht angegliedert sein darf und ihm nach § 5 Abs. 4 NVerfSchG keine polizeilichen Befugnisse oder Weisungsbefugnisse zustehen. Das Trennungsprinzip verbietet eine organisatorische und befugnismäßige Zusammenlegung von polizeilichen und nachrichtendienstlichen Behörden. Ähnliche Regelungen gelten auch für das Bundesamt für Verfassungsschutz und die anderen Landesämter.

Das Trennungsgebot trifft jedoch keine Aussage darüber, dass die Polizei zu Zwecken der Gefahrenabwehr keine Maßnahmen der verdeckten Datenerhebung mit besonderen Mitteln und Methoden nach den §§ 33 a bis 37 Nds. SOG ergreifen darf. Auch hier hat das BVerfG mit seiner Entscheidung zur Überwachung der Telekommunikation nach dem Außenwirtschaftsgesetz sehr wohl deutlich gemacht, dass diese Maßnahme auch im Bereich polizeilicher Gefahrenabwehr zulässig ist und diese Befugnis keine Beschränkung findet allein auf den Verfassungsschutz.

Zu 3: DNA-Analyse in Strafverfahren

Die DNA-Analyse im Strafverfahren ist eines der wirksamsten und effizientesten Mittel zur Strafverfolgung und zu einem unverzichtbaren Instrument der Verbrechensbekämpfung geworden. Aus dem polizeilichen Alltag ist sie nicht mehr wegzudenken. Viele schwere Straftaten wie Mord, Vergewaltigung und sexueller Missbrauch konnten mittels der hierfür beim Bundeskriminalamt eingerichteten DNA-Analyse-Datei zuverlässig aufgeklärt werden; insbesondere auch solche Straftaten, die teilweise Jahrzehnte zurücklagen und bei denen niemand mehr an Aufklärung glaubte.

Bei der DNA-Analyse im Strafverfahren werden lediglich die bei jedem Menschen unterschiedlichen Abstände zwischen den Genen mit den entsprechenden Spuren verglichen, jedoch nicht die sich auf den Genen selbst befindenden Informationen. Damit ist die Gewinnung weiterer Informationen etwa über Herkunft, Augenfarbe oder vielleicht auch Krankheitsdispositionen nach dem Stand der Wissenschaft ausgeschlossen.

Auch wenn das BVerfG in seinen bisher vorliegenden Entscheidungen deutlich gemacht hat, dass die Feststellung, Speicherung und (künftige) Verwendung des DNA-Identifizierungsmusters in das durch Artikel 2 Abs. 1 GG i. V. m. Artikel 1 Abs. 1 GG verbürgte Grundrecht auf informationelle Selbstbestimmung eingreift, dürfte dies einer Ausweitung des Anwendungsbereichs der DNA-Identifizierung nicht entgegenstehen. Das BVerfG hat sich nur mit der Rechtslage de lege lata beschäftigt und an keiner Stelle zu erkennen gegeben, dass eine gesetzliche Ausweitung verfassungsrechtlich unzulässig wäre. Einen Eingriff in den absolut geschützten Kernbereich des Persön-

lichkeitsrechts, in den auch aufgrund eines Gesetzes nicht eingegriffen werden dürfte, hat das BVerfG durch die Feststellung des DNA-Identifizierungsmusters nicht gesehen (BVerfG, 2 BvR 1741/99 vom 14.12.2000).

Eine Ausweitung der DNA-Analyse ist im Interesse einer effektiven Strafrechtspflege geboten, zumal der Schutz der Bevölkerung erheblich verbessert würde.

Darüber hinaus wird nicht in Zweifel gezogen werden können, dass durch die Aufnahme des genetischen Fingerabdrucks in der Vergangenheit bereits eine Vielzahl von zu Unrecht beschuldigter Personen entlastet werden konnten. In den USA mussten beispielsweise in den letzten zehn Jahren allein 163 Todesurteile auch deswegen aufgehoben werden, weil es mithilfe des DNA-Identifizierungsmusters gelungen war, die Unschuld des Verurteilten zu beweisen bzw. eine andere Person als Täter zu überführen. Im Interesse einer wirksamen Strafrechtspflege besteht daher ein dringendes Bedürfnis, unter Berücksichtigung des verfassungsrechtlichen Rahmens den Aufbau und die Pflege der DNA-Analysedatei auf eine möglichst breite Grundlage zu stellen und damit die Effizienz der Tataufklärung weiter zu verbessern.

Der Eingriff durch eine DNA-Speichelprobe in die körperliche Unversehrtheit ist mit der Abnahme eines Fingerabdrucks durchaus vergleichbar. Die mithilfe des allein festgestellten und gespeicherten DNA-Identifizierungsmusters erreichbare Code-Individualität wird in forensischer Hinsicht am besten durch ihre Nähe zum Daktylogramm verdeutlicht. Dabei muss Berücksichtigung finden, dass durch die Feststellung des DNA-Identifizierungsmusters anhand des Probenmaterials Rückschlüsse auf persönlichkeitsrelevante Merkmale wie Erbanlagen, Charaktereigenschaften oder Krankheiten des Betroffenen, also ein Persönlichkeitsprofil, nicht ermöglicht werden. Die im Strafverfahren angewandte DNA-Analyse offenbart den polizeilichen Untersuchungsstellen daher nicht mehr als der seit Jahrzehnten angewandte Fingerabdruck.

Für die Gefahr eines potenziellen Missbrauchs von Befugnissen gibt es keine Anhaltspunkte. Jede Untersuchungsmaßnahme - sei sie polizeilich oder rein medizinisch veranlasst - birgt grundsätzlich die Gefahr des Missbrauchs. So könnten natürlich auch anhand der häufig im Strafverfahren angewandten Blutprobe eine Reihe nicht erkennbarer Krankheiten festgestellt werden wie Hepatitis, HIV usw. Es ist nicht erkennbar, warum bei DNA-Analysen eine höhere Missbrauchsgefahr bestehen soll als bei anderen kriminaltechnischen Auswertungsmethoden, zumal etwa aus den täglich in großer Anzahl von der Polizei veranlassten Blutproben schon jetzt durch medizin-wissenschaftliche Untersuchungen grundsätzlich mehr Informationen missbräuchlich erlangt werden könnten als aus dem DNA-Spurenmaterial.

Darüber hinaus sind die molekulargenetischen Untersuchungsstellen jenseits der Erhebung des Identifizierungsmusters technisch, apparativ und durch die spezifischen Präparate ohnehin nicht in der Lage - außer der Feststellung der Geschlechtszugehörigkeit -, andere aussagekräftige Hinweise über körperliche, geistige oder charakterliche Eigenschaften eines Menschen zu geben. Abgesehen davon ist das Ziel der Strafverfolgungsbehörden nicht die vage Wahrscheinlichkeitsaussage über die Zugehörigkeit zu einer ethnischen Gruppe, die Feststellung von Erbkrankheiten oder eventuellen Krankheitssymptomen, sondern die beweissichere und gerichtsverwertbare Identifizierung von Straftätern. Die Gefahr einer Ausforschung besteht daher gerade nicht, zumal das DNA-Material entsprechend der gesetzlichen Vorschriften nach der Analyse vernichtet wird. Gespeichert werden lediglich Buchstaben-/Zahlenkombinationen, mit denen ein automatisierter Abgleich in der DNA-Analyse-Datei möglich ist.

Zu 4: Einheitliches Personenkennzeichen

Der LfD stellt zutreffend fest, dass durch das Steueränderungsgesetz 2003 die gesetzlichen Grundlagen für die Einrichtung eines bundesweit einheitlichen persönlichen Identifikationsmerkmals für steuerliche Zwecke geschaffen worden sind. Es handelt sich jedoch ausdrücklich nicht um ein allgemein gebräuchliches Personenkennzeichen.

Die maßgeblichen Vorschriften für das Gesamtvorhaben - es handelt sich um die Regelungen der §§ 139 a bis d Abgabenordnung (AO) und § 5 des Einführungsgesetzes zur AO sowie die Ergänzung des Finanzverwaltungsgesetzes und die Ergänzung des Melderechtsrahmengesetzes - ver-

deutlichen die Einführung eines bundeseinheitlichen steuerlichen Identifikationsmerkmals als eine sehr komplexe Aufgabenstellung.

Ein besonderes Anliegen war dabei die Verbesserung der Effizienz der Steuerverwaltung unter gleichzeitiger Wahrung des Grundrechts auf informationelle Selbstbestimmung der Bürgerinnen und Bürger.

Da zwischen den Identifikationsanforderungen für natürliche Personen und allen übrigen Bereichen unterschiedliche Kontinuitätsregeln und datenschutzrechtliche Einschränkungen gelten, sieht die Konzeption des neuen Ordnungsnummernsystems eine klare Trennung zwischen der persönlichen Identifikationsnummer nach § 139 b AO und der Wirtschafts-Identifikationsnummer gemäß § 139 c AO vor. Mit der Vergabe der persönlichen Identifikationsnummer wird jede natürliche Person, die im Inland einen Wohnsitz oder ihren gewöhnlichen Aufenthalt hat und unbeschränkt bzw. beschränkt einkommensteuerpflichtig ist, erfasst. Ein Generalverdacht oder die Vermutung einer potenziellen Steuerhinterziehung einer einzelnen Person ist damit nicht verbunden.

Die unter der Identifikationsnummer gespeicherten Daten unterliegen einer eindeutigen Zweckbindung für steuerliche Zwecke, um im Besteuerungsverfahren die Beteiligten bundesweit auch über die Landesgrenzen hinweg eindeutig identifizieren und ihnen Besteuerungsdaten zuordnen zu können.

Die Befürchtung des LfD, dass der künftig vorhandene „Datenpool“ auch zweckentfremdet genutzt werden könnte, wird nicht geteilt. Die Steuerverwaltung hat nicht die Absicht, den Datenbestand zur Identifikationsnummer zu anderen als im Gesetz bereits vorgesehenen Verwaltungsbereichen zugänglich zu machen.

Die Forderung des LfD, im Fall einer eventuell geänderten Gesetzgebung strenge Zweckbindungen und Verwendungsverbote vorzusehen, wird von der Landesregierung geteilt.

Zu 5: Neue Personalverwaltungssysteme - Droht der „Gläserne Bedienstete“?

Die Wahrung der Schutzrechte der betroffenen Landesbediensteten bei der Einführung einer einheitlichen Software für Personalmanagement in der Landesverwaltung ist auch der Landesregierung ein wichtiges Anliegen. Aus diesem Grund wurden sowohl der LfD als auch die Spitzenorganisationen der Gewerkschaften bereits frühzeitig in das Projekt eingebunden, was der LfD in seinem Tätigkeitsbericht entsprechend gewürdigt hat. Es ist beabsichtigt, den Dialog mit dem LfD, den Gewerkschaften und den Personalvertretungen in allen den Datenschutz und die Datensicherheit betreffenden Fragen auch in Zukunft fortzuführen.

Zu 6: Betriebswirtschaftliche Steuerungsinstrumente (Kosten- und Leistungsrechnung)

Die vom LfD vertretene Auffassung, dass bei der Einführung betriebswirtschaftlicher Steuerungsinstrumente in die Haushaltswirtschaft datenschutzrechtliche Vorgaben u. a. zur Vertraulichkeit, Anonymisierung und Sicherheit gewährleistet sein müssen, wird von der Landesregierung geteilt. Dementsprechend wurde bei allen von ihr veranlassten Maßnahmen zur Einführung betriebswirtschaftlicher Steuerungsinstrumente in der Landesverwaltung, insbesondere in der zum Projekt LoHN geschlossenen Vereinbarung nach § 81 Niedersächsisches Personalvertretungsgesetz, dem Datenschutz eine hohe Priorität eingeräumt. Insoweit wird auch die Ankündigung des LfD, den weiteren Einsatz der neuen betriebswirtschaftlichen Steuerungsinstrumente unter Einbeziehung der praktischen Erfahrungen der Dienststellen weiter begleiten zu wollen, im Interesse der Akzeptanz des Verfahrens bei den Bediensteten nachdrücklich begrüßt.

Zu 9: Datenschutz in der Arztpraxis

Die Landesregierung und hier vor allem das MS wird die vom LfD geplante Ausweitung der Aktion „Datenschutz in der Arztpraxis“ auf den Bereich der Krankenhäuser ausdrücklich unterstützen. Die bisher in den ärztlichen, zahnärztlichen und psychotherapeutischen Praxen erreichten Verbesserungen des Datenschutzes im täglichen Ablauf bestätigen den vom LfD gewählten Ansatz des Vorgehens und ermutigen dazu, Gleiches im Kliniksektor anzustreben. Damit wird nicht nur dem Interesse der Patientinnen und Patienten an einem datenschutzgerechten Umgang mit ihren äußerst

sensiblen Gesundheitsdaten Rechnung getragen, sondern auch Rechtssicherheit für die Beschäftigten und Verantwortungsträger geschaffen.

Zu 15: Biometrie und Datenschutz

Mit dem In-Kraft-Treten des Terrorismusbekämpfungsgesetzes zum 01.01.2002 wurde durch die Änderung des Passgesetzes und des Personalausweisgesetzes die Rechtsgrundlage geschaffen, in Pässen und Personalausweisen neben dem Lichtbild und der Unterschrift zusätzliche biometrische Merkmale aufzunehmen. Diese Merkmale können auch verschlüsselt werden, die Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung der Merkmale sowie die Speicherung, Verarbeitung und Nutzung sind durch ein Bundesgesetz zu regeln. Diese Regelung zur Einführung biometrischer Merkmale in deutsche Personaldokumente steht derzeit noch aus.

Inzwischen hat der Rat der EU in seiner Verordnung über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten (Verordnung [EG] Nr. 2252/2004 des Rates vom 13.12.2004) beschlossen, verbindlich die Einführung von zwei biometrischen Merkmalen in Reisepässen vorzuschreiben: das Gesichtsbild sowie die Fingerabdrücke der Passinhaberin oder des Passinhabers. Damit würden die Mitgliedstaaten auch die Erfordernisse des „US Visa Waiver Program“ in Übereinstimmung mit internationalen Normen erfüllen.

Die Einführung der beiden biometrischen Merkmale erfolgt stufenweise. Für die Umsetzung hinsichtlich des Gesichtsbildes haben die Mitgliedsstaaten 18 Monate und hinsichtlich der Fingerabdrücke 36 Monate Zeit. Da die EU-Verordnung unmittelbar anzuwenden ist, verbleibt bei der Entscheidung über die Einführung biometrischer Merkmale in Pässen den einzelnen Mitgliedstaaten jedoch kein Spielraum.

Durch die geplante Einführung biometrischer Identifikatoren in Reisepässen würde eine verlässliche Verbindung zwischen dem Dokument und dessen Inhaberin oder Inhaber hergestellt werden können. Einheitliche Sicherheitsstandards für Pässe und Reisedokumente würden in einem größeren Umfang als bisher die Verwendung gefälschter Pässe und Ausweise zu verhindern helfen.

Es ist derzeit nicht absehbar, ob der Forderung des LfD nach Speicherung der Biometrie als mathematische Komprimate und nicht in Form von Rohdaten gefolgt werden wird. Die Regelung des Artikel 1 Abs. 2 der EG-Verordnung vom 13.12.2004 schreibt insoweit nur vor, dass das Speichermedium geeignet sein muss, die Authentizität und die Vertraulichkeit der Daten sicherzustellen. Da die technische Ausgestaltung in die Zuständigkeit des Bundesgesetzgebers fällt, eine Mitteilung über die beabsichtigte Form der Speicherung der Daten den Ländern bis zum jetzigen Zeitpunkt noch nicht erfolgt ist, ist eine Stellungnahme hierzu noch nicht möglich. Gleiches gilt im Übrigen für die Entscheidung über die Schaffung einer möglichen Zentraldatei.

Die Befürchtung des LfD, dass eine automatisierte Identifikation ohne Kenntnis der betroffenen Person durchgeführt werden könnte, ist unbegründet. Die Bundesdruckerei hat auf der CeBit 2005 detailliert dargestellt, wie die Biometriedaten der Pässe ausgelesen werden können. Der Pass muss zunächst willentlich von der Passinhaberin oder dem Passinhaber herausgegeben und dann auf das Lesegerät aufgelegt werden, bevor die Biometriedaten zugänglich gemacht werden. Ein unbefugtes und verdecktes Auslesen der Biometriedaten wird damit wirksam verhindert.

Eine Regelung hinsichtlich der Einführung biometrischer Merkmale in Personalausweise ist von der Verordnung indes unberührt. Hier wird davon ausgegangen, dass sich das Bundesministerium des Innern hinsichtlich der Einführung biometrischer Merkmale in deutsche Personalausweise an den Vorgaben der Verordnung über Normen für Sicherheitsmerkmale und Biometrie in Pässen der EU-Bürgerinnen und EU-Bürger orientieren wird. Konkretere Informationen über den genauen Regelungsinhalt bzw. den beabsichtigten Zeitpunkt der Einführung einer bundesgesetzlichen Regelung zur Einführung biometrischer Merkmale in deutsche Personalausweise sind nicht bekannt.

Die vom LfD in seinem Tätigkeitsbericht beschriebene Beobachtung öffentlicher oder privater Plätze unter Nutzung von Video-Technik, die mit einem biometrischen Erkennungssystem gekoppelt ist, wird in Niedersachsen nicht durchgeführt. Die gängigen Verfahren und Produkte der Gesichtserkennung scheinen bisher auch technisch nicht in der Lage, den Anforderungen der polizeilichen Fahndung gerecht zu werden.

Zu 16: Sichere Funknetzwerke

Der Markt für drahtlose lokale Datennetze (Wireless Local Area Network, WLAN) entwickelt sich rasant. Zahlreiche Produkte werden auf diesem Markt für den privaten Endnutzer und die professionellen Anwender in der Wirtschaft und Verwaltung angeboten.

Seit 1997 wurden verschiedene Standards (802.11a/b/g/h, HyperLAN/2 usw.) geschaffen und weiterentwickelt. Gegenwärtig stehen Bruttoübertragungsraten von bis zu 54 Mbit/s zur Verfügung. Damit können WLANs als Ersatz oder zur Erweiterung bestehender kabelgebundener Netze eingesetzt werden. Die WLAN-Technologie kann im Indoor-Bereich und im Outdoor-Bereich für Punkt-zu-Punkt-Verbindungen (kein Richtfunk) eingesetzt werden.

Bei der Planung eines WLAN sind verschiedene Parameter wie beispielsweise das Versorgungsgebiet (Festlegung der Bereiche mit WLAN-Versorgung), die Zellplanung (Bestimmung der Zellgrößen und Zellüberlappungen, Vorauswahl von Antennentypen, grobe Festlegung der Position von Antennen usw.), die Anwendungs- (z. B. Client-Anzahl) und Verkehrsprofile (z. B. Datenvolumen, Antwortzeit) sowie die Festlegung der benötigten Bandbreite im Versorgungsgebiet zu beachten. Für den Betrieb eines WLAN müssen Sicherheitsmaßnahmen realisiert werden, die im Regelfall deutlich über die Sicherheitsmaßnahmen in drahtgebundenen LAN hinausgehen.

Diese grobe Aufzählung zeigt, dass die Projektierung, der Aufbau und der Betrieb eines WLAN spezielle Fachkenntnisse erfordern, wie sie zurzeit in der Landesverwaltung im notwendigen Umfang nicht vorhanden sind.

Aus diesem Grund hat das MI (Zentrales IT-Management - ZIM) die Erarbeitung eines Betriebs- und Sicherheitskonzeptes WLAN für die Landesverwaltung im Dezember 2004 in Auftrag gegeben. Die Vorlage des Konzepts wird im zweiten Quartal 2005 erwartet. Bis dahin werden in der Landesverwaltung keine WLAN aufgebaut.

Durch diese Vorgehensweise soll ein durchgängig hohes IT-Sicherheitsniveau für WLAN in der Landesverwaltung erreicht werden, das auch den datenschutzrechtlichen Handlungsbedarf abdeckt.

Zu 17: eGovernment

Die Entwicklung der Informations- und Kommunikationstechnik, insbesondere des Internets, stellt die Verwaltung vor immer neue Aufgaben. Diese Technik ermöglicht die Übermittlung von Inhalten jeder Art, insbesondere auch Willenserklärungen, schnell und grundsätzlich ohne Qualitätsverlust.

Mit dem Gesetz zur Änderung des Niedersächsischen Verwaltungsverfahrensgesetzes und anderer Gesetze vom 16.12.2004 wurden u. a. das allgemeine Verwaltungsverfahrensrecht und - soweit Bedarf gesehen - niedersächsisches Fachrecht für die neuen technischen Möglichkeiten rechtssicher geöffnet. Bürger, Wirtschaft und Verwaltung können somit neben der Schriftform und der mündlichen Form - grundsätzlich gleichrangig - auch die elektronischen Kommunikationsformen rechtssicher verwenden.

Durch die Verweisung des § 1 Abs. 1 NVwVfG auf die bundesgesetzliche Generalklausel in § 3 a VwVfG gilt somit auch die Regelung, dass eine durch materielles Gesetz angeordnete Schriftform durch eine elektronische Form gleichwertig ersetzt werden kann. Für die Formfreiheit bedarf es - wie bisher - weiterhin keiner gesonderten Regelung, sodass grundsätzlich die Verwendung elektronischer Dokumente jeder Art möglich ist.

Mit der Novellierung des niedersächsischen Verwaltungsverfahrensrechts wurde daher ein verlässlicher und klarer Rechtsrahmen für einen modernen Rechtsverkehr und zugleich eine wesentliche landesrechtliche Voraussetzung für eGovernment geschaffen.

Zu 18: Informationszugang als Konsequenz des Rechts auf informationelle Selbstbestimmung

Zur Frage der Erforderlichkeit eines niedersächsischen Informationszugangsgesetzes hat die Landesregierung bereits zu Nummer 4.7 des XVI. Tätigkeitsberichts des LfD Stellung genommen (Drs. 15/283 S. 4/5) und bekräftigt, dass die notwendige Transparenz der öffentlichen Verwaltung durch

bestehende bereichsspezifische Informationsrechte und Veröffentlichungspflichten nach Auffassung der Landesregierung bereits gewährleistet wird und sich die Informationsmöglichkeiten des Einzelnen gegenüber öffentlichen Stellen durch ein niedersächsisches Informationszugangsgesetz nicht nachhaltig verbessern würden.

In der 35. Plenarsitzung des Landtages hat Herr Minister Schünemann am 27.05.2004 zu TOP 24 (Niedersachsen durch ein Informationsfreiheitsgesetz fit machen für die demokratische Wissensgesellschaft im 21. Jahrhundert - Antrag der Fraktion Bündnis 90/Die Grünen - Drs. 15/1027) bekräftigt, dass es in Niedersachsen keinen Bedarf für ein solches Gesetz gibt.

Der Landtag hat nach der ersten Beratung den Antrag zunächst zur Beratung in die Ausschüsse überwiesen. Federführend ist der Ausschuss für Rechts- und Verfassungsfragen, mitberatend der Ausschuss für Inneres und Sport und der Ausschuss für Haushalt und Finanzen. In seiner 30. Sitzung am 09.06.2004 beauftragte der Ausschuss für Rechts- und Verfassungsfragen die Landtagsverwaltung, aus den Ländern Nordrhein-Westfalen und Schleswig-Holstein Informationen über die Gebührenhöhen einzuholen, die dort auf kommunaler Ebene und auf Landesebene für Akteneinsichten und -auskünfte erhoben werden. Die Ergebnisse sind der Landesregierung nicht bekannt.

Auf Bundesebene wurde am 17.12.2004 der Entwurf eines Gesetzes zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz - IFG) der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN auf der Grundlage der BT-Drucksache 15/4493 in erster Lesung im Bundestag beraten und federführend an den Innenausschuss überwiesen.

Der Innenausschuss des Bundestages hat in seiner 58. Sitzung am 14.03.2005 zu dem Fraktionsgesetzentwurf eine öffentliche Anhörung von Sachverständigen durchgeführt, eine abschließende Beschlussempfehlung an den Bundestag hat der Innenausschuss jedoch noch nicht gegeben.

Der Hinweis des LfD, dass die Erfahrungen in den Bundesländern, in denen schon seit längerem Informationsfreiheits- oder -zugangsgesetze bestehen, durchweg positiv sind, entkräftet nicht die Annahme, dass im Gesetzesvollzug Probleme auftreten können, die einen erheblichen Abstimmungsaufwand bewirken und somit Kosten verursachen. Denkbar wären Fälle, in denen zu einem Thema pauschal Einsichtnahme „in alle Akten“ begehrt oder verschiedene Stellen zu einem gleich lautend vorgetragenen Antragsbegehren verschiedene Entscheidungen treffen würden. Zudem könnte diese Konkurrenz auch zu Wertungswidersprüchen im Verhältnis zu spezialgesetzlichen Akteneinsichts- und Aktenauskunftsrechten und zu Unsicherheiten bei der Rechtsanwendung führen.

Es ist daher kein Zufall, dass die überwiegende Anzahl der Bundesländer - und der Bund - bisher kein IFG beschlossen haben.

Die Landesregierung wird dem Fortgang und den Ergebnissen der weiteren Behandlung des Themas durch die Ausschüsse des Landtages wie auch dem Abschluss des Bundesgesetzgebungsverfahrens zuwarten.

Zur Rückschau:

5. Forderung: Modernere Chipkartensysteme

In den vergangenen Jahren kam die SignaturCard Niedersachsen fast ausschließlich im Haushaltswirtschaftssystem auf ca. 16 000 IT-gestützten Arbeitsplätzen zum Einsatz. Nach Abkündigung des für die SignaturCard Niedersachsen eingesetzten Chipkartensystems durch den Lieferanten ist die Migration der Karte erforderlich geworden.

In diesem Zusammenhang müssen die strategischen Ziele für den Einsatz der SignaturCard in der Landesverwaltung beachtet werden. Zukünftig soll die SignaturCard als Multifunktionskarte (Single-Sign-On, Zeiterfassung, Zutrittskontrolle, Dienstausweis usw.) bei weiteren Projekten (z. B. PMV, remoteAP) und letztendlich auf allen IT-gestützten Arbeitsplätzen eingesetzt werden. Durch die neue Ausrichtung der SignaturCard Niedersachsen soll die Wirtschaftlichkeit der Karte erhöht, ein höheres Niveau der IT-Sicherheit erreicht und die Mitarbeiterinnen und Mitarbeiter in der Landesverwaltung bei ihren dienstlichen Aktivitäten unterstützt werden.

Aus den angeführten Gründen hat MI (ZIM) das Informatikzentrum Niedersachsen (IZN) damit beauftragt, auf ein neues Chipkartensystem (Arbeitsbegriff Netkey2048) zu migrieren. Diese Chipkarte gewährleistet aufgrund der Schlüssellänge langfristig ein hohes Sicherheitsniveau und entspricht technisch den künftigen Anforderungen der Landesverwaltung. Flexibilität bei variierenden Anforderungen ist durch das Design der Chipkarte gewährleistet. Schlüsselpaare für verschiedene Funktionalitäten (Signatur, Verschlüsselung, Authentifizierung, qualifizierte Signatur usw.) können implementiert werden. Das Chipkartensystem gestattet es auch Gruppenschlüssel zu realisieren.

Zeitgleich wurde das IZN auch mit dem Aufbau und Betrieb einer landeseigenen Certification Authority (Niedersachsen-CA) beauftragt. Die Niedersachsen-CA wird in die Verwaltungs-PKI unter der Wurzelzertifizierungsstelle PCA-1-Verwaltung, die durch das Bundesamt für Sicherheit in der Informationstechnik betrieben wird, integriert. Der Produktionsbetrieb wird im vierten Quartal 2005 beginnen.

8. Forderung: Meldewesen

In der Rückschau seines Tätigkeitsberichts (8. Forderung) fordert der LfD die baldige Umsetzung des novellierten Melderechtsrahmengesetzes in niedersächsisches Landesrecht. Das Niedersächsische Meldegesetz (NMG) wird zurzeit entsprechend novelliert. Momentan erfolgt die Beteiligung der Arbeitsgruppe „Rechtsvereinfachung“ bei der Niedersächsischen Staatskanzlei. Die Veröffentlichung des novellierten NMG wird voraussichtlich im Herbst 2005 erfolgen können.

Das NMG wird das elektronische Rückmeldeverfahren zwischen den Meldebehörden innerhalb Niedersachsens vorschreiben. Zur technischen Umsetzung dieses Verfahrens wurde seitens MI bereits eine Projektgruppe mit der Erstellung eines Grobkonzepts beauftragt. Der LfD wurde von dort bereits einbezogen.