



Der Thüringer Landesbeauftragte für den Datenschutz

17. April 2008

Sperrfrist 12:00 Uhr

Pressemitteilung

Landesbeauftragter stellt 7. Tätigkeitsbericht vor

„Mit der ständig zunehmenden Digitalisierung unserer Lebensumwelt wachsen die Bedrohungen für die Privatsphäre der Bürger durch Staat und Wirtschaft stetig an. Deshalb ist die Schärfung des Datenschutzbewusstseins, aber auch eine funktionierende Datenschutzkontrolle wichtiger denn je“, erklärte Harald Stauch, Thüringer Landesbeauftragter für den Datenschutz, bei der Vorstellung seines ersten und des insgesamt 7. Tätigkeitsberichts. Dieser enthält einen Überblick über die Schwerpunkte der Tätigkeit des TLfD sowohl bei der beratenden Mitwirkung an der Gesetzgebung im Land, im Bund und der EU als auch bei der Bearbeitung von Bürgereingaben, der Kontrolle der öffentlichen Stellen des Landes und nicht zuletzt bei deren Beratung in datenschutzrechtlichen Fragen. „Weil unser Alltag immer mehr von informationstechnischen Systemen regelrecht beherrscht wird und diese zunehmend in den öffentlichen Stellen des Landes zum Einsatz kommen, sehe ich meine Aufgaben neben der Kontrolle verstärkt darin, die öffentlichen Stellen im Vorfeld der Verarbeitungen personenbezogener Daten zu beraten, damit Missstände erst gar nicht entstehen“, hob Stauch hervor.

Ein Schwerpunkt der Arbeit des TLfD in den letzten beiden Jahren sei wiederum das Ringen um die Balance zwischen Freiheit und Sicherheit gewesen. Jeweils nach Bekanntwerden spektakulärer Kriminalfälle oder terroristischer Aktivitäten habe sich die Diskussion um einen erweiterten Zugang der Sicherheitsbehörden zu personenbezogenen Daten erneuert. Es sei aber nicht bei einer Diskussion geblieben, sondern die politisch Handelnden in Europa, im Bund und im Land hätten solche zusätzlichen

Befugnisse zum Eingriff in die Privatsphäre der Menschen geschaffen oder pflanzen sie. Beispiele hierfür seien die Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten (4.1), Pläne für eine heimliche Online-Durchsuchung privater Computer (10.1) oder die im Thüringer Polizeiaufgabengesetz (7.1) geplante Kennzeichen-erkennung. Häufig würden bei diesen Maßnahmen Daten weit im Vorfeld von Gefahren und Straftaten erfasst und zudem von einem ganz überwiegend unverdächtigen Personenkreis. Das führe dazu, dass die Menschen unberechtigt unter einen Generalverdacht gestellt werden und unverhältnismäßige Eingriffe in ihre Privatsphäre erdulden müssen. Andere Maßnahmen seien zwar durch einen Verdacht begründet, griffen aber so tief in die Privatsphäre ein, dass sie die im Grundgesetz garantierte Menschenwürde verletzen.

„Ermutigend ist es deshalb, dass das Bundesverfassungsgericht in einer Reihe von Entscheidungen solche übermäßigen Eingriffe korrigiert hat“, so Harald Stauch weiter. „Auch nach Redaktionsschluss zu dem vorliegenden Bericht hat das Bundesverfassungsgericht seine Rolle als rechtsstaatliches Korrektiv in den Entscheidungen zur Online-Durchsuchung, zur Kfz-Kennzeichenerfassung und zur Vorratsdatenspeicherung eindrucksvoll unter Beweis gestellt. Im Urteil zur Online-Durchsuchung hat es zudem das Datenschutzgrundrecht vor dem Hintergrund der Gefahren einer elektronischen Ausforschung der Bürger über informationstechnische Systeme weiterentwickelt. Das wird positive Auswirkungen für den Datenschutz weit über die Frage der Online-Durchsuchung hinaus haben.“

Bei der Kontrolltätigkeit zeigte sich eine Tendenz, wonach die Sensibilisierung für den Datenschutz sowohl hinsichtlich technisch-organisatorischer Maßnahmen als auch bezüglich der rechtlichen Grenzen der Datenverarbeitung vor allem in den Kommunen zum Teil noch erhebliche Defizite aufweise. So hätten, auch wenn die Kommunen zahlenmäßig den größten Anteil der öffentlichen Stellen darstellten, in diesem Bereich die meisten der insgesamt 12 Beanstandungen ausgesprochen werden müssen. Das reiche vom Verkauf von PC mit nicht gelöschten Daten (5.6), dem unsensiblen Umgang mit Postsendungen (5.7) über die unzulässige Datenveröffentlichung im Internet (5.4) bis hin zur Observierung von Mitarbeitern (6.2), zu unzulässigen Presseauskünften zu Personaldaten (6.3) sowie zur unbefugten Erstellung und Übermittlung eines amtsärztlichen Gutachtens (11.7). Für den kommenden Berichtszeitraum werde daher diesem Bereich besondere Aufmerksamkeit zu schenken sein.

Bei der Kontrolltätigkeit habe sich auch erstmals ein generelles Problem im Zusammenhang mit der bundesweiten Einführung biometrischer Reisepässe (5.5) gezeigt. Obwohl die mit elektronisch gespeicherten Fingerabdrücken versehenen ePässe besonders sicher sein sollen, sei es für den Bürger noch nicht möglich, nach der Ausstellung die Übereinstimmung der gespeicherten mit seinen eigenen Fingerabdrü-

cken zu überprüfen. Hier sei der Bund aufgefordert worden, schnellstens für Abhilfe zu sorgen.

Wichtige Hinweise für datenschutzrechtliche Mängel sind häufig auch Eingaben der Bürger. So habe die Überprüfung einer solchen Eingabe eine unzureichende Protokollierung von Kfz-Halterabfragen im Computersystem ZEVIS durch die Polizei ergeben (7.8). „Es sollte auch im Interesse des Ansehens der Polizei liegen, dass solche Abfragen besser dokumentiert werden, um berechnigte Vorwürfe eines Datenmissbrauchs überprüfen sowie unberechnigten Vorwürfen entgegentreten zu können“, mahnte Stauch.

Neben der zahlreichen Kritik, die der Bericht enthält, hob Stauch auch ein positives Beispiel hervor, wie in enger Abstimmung mit dem Datenschutzbeauftragten durch technische Verfahrensausgestaltungen grundrechtsschonende Ermittlungsmethoden entwickelt werden können. So könne durch den intelligenten und stufenweisen Einsatz von Videoüberwachungstechniken an einem Tunnel der Autobahn 71 (7.6) weitgehend verhindert werden, dass Unbeteiligte, die keinen Anlass für eine Prüfung ihrer Verhaltensweise geboten haben, erfasst werden.

Schließlich seien auch Fragen zu bewerten gewesen, die sich aus dem Einsatz neuer Techniken erst nach und nach ergeben. Dazu gehöre die Nutzung von Luftaufnahmen (12.1), die in immer höherer Auflösung vorlägen und als sogenannte Geodaten, auch mit anderen Daten verknüpft, neue Gefahren für die Privatsphäre darstellten. Ebenfalls noch nicht annähernd abschätzbar seien die neuen Risiken für das informationelle Selbstbestimmungsrecht durch den Einsatz von RFID-Technologie (14.3). Hier habe die Diskussion erst begonnen. „Ein weiteres Beispiel, wie im Beratungswege sachgerechte Lösungen gefunden werden, ist das Verfahren der Filterung von unerwünschter elektronischer Post und Viren aus dem E-Mail-Verkehr der Landesverwaltung bei gleichzeitiger Beachtung des Telekommunikationsgeheimnisses der Beteiligten (15.7)“, so Stauch abschließend.

Kahl

-Öffentlichkeitsarbeit -