Schleswig-Holsteinischer Landtag
Umdruck 17/2903

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Klosterwall 6 (Block C), D – 20095 Hamburg

Herrn
Thomas Rother
Vorsitzender des
Innen- und Rechtsausschusses
im Schleswig-Holsteinischen Landtag
Postfach 71 21

24171 Kiel

Klosterwall 6, Block C
D – 20095 Hamburg
Telefon: 040 - 428 54 - 40 41 Zentrale - 40 40
Telefax: 040 - 428 54 - 40 00
Ansprechpartner: Prof. Dr. Caspar
E-Mail*: Johannes.Caspar@datenschutz.hamburg.de

Az.: D /

Hamburg, den 21. Oktober 2011

Entwurf eines Gesetzes zur Änderung des Landesdatenschutzgesetzes und des Landesverfassungsschutzgesetzes /Gesetzentwurf der Landesregierung – Drucksache 17/1698

Sehr geehrter Herr Rother,

haben Sie vielen Dank für die Gelegenheit, zum o.g. Gesetzentwurf der Landesregierung Stellung zu nehmen.

Hierzu darf ich folgende Ausführungen machen:

Zu § 20 (Video-Überwachung und -Aufzeichnung)
Das Ziel der Regelungen ist die Beobachtung der öffentlichen Räume, soweit dies zur Erfüllung der behördlichen Aufgaben oder zur Wahrnehmung eines Hausrechts erforderlich ist. Im Hinblick auf diese Formulierung bestehen Defizite hinsichtlich der Bestimmtheit der Regelung. Nach der Rechtsprechung des Bundesverfassungsgerichts stellt die Videoüberwachung durch öffentliche Stellen einen Eingriff in das informationelle Selbstbestimmungsrecht dar und bedarf einer normenklaren gesetzlichen Grundlage. Hierbei müssen insbesondere Anlass, Zweck und die Grenzen des Eingriffs in der Ermächtigungsgrundlage bereichsspezifisch, präzise und normenklar festgelegt werden (vgl. BVerfG 1 BvR 2368/06, Rn. 46 m.w.N.) .

Zunächst erscheint der Hinweis auf den unspezifischen Begriff des Hausrechts sehr vage.

Die Hamburgische Bürgerschaft hat im letzten Jahr mit der Bestimmung des § 30 HmbDSG eine Vorschrift für die Videoüberwachung durch öffentliche Stellen in das Landesdatenschutzrecht aufgenommen. Um hier eine klare Eingriffsgrundlage zu schaffen, wurde eine Beschränkung zur Ausübung des Hausrechts der verantwortlichen Stelle auf den Schutz von *Personen und Sachen* oder die *Überwachung von Zugangsberechtigungen* vorgenommen. Damit sind die Eingriffsbefugnisse auch im Bereich des behördlichen Hausrechts stärker auf den Schutz von konkreten Rechtsgütern zentriert, was eine normklarere Rechtsanwendung zulässt.

Die Befugnis, eine Video-Überwachung zur Erfüllung der *behördlichen Aufgaben* anzuordnen, erweitert die Eingriffsbefugnis in der Entwurfsfassung des § 20 auf die behördliche Funktionszuschreibung. Die Anknüpfung an die bloße Aufgabenwahrnehmung stellt eine unspezifische Generalklausel für das Betreiben von Videokameras dar. Diese ist als rechtsklare Ermächtigungsgrundlage nicht ausreichend. Durchaus berechtigt werden im Schrifttum rechtsstaatliche Bedenken gegen die Norm des § 6 b BDSG vorgetragen, an die die Regelung des Gesetzentwurfs anknüpft: Soweit der Gesetzgeber in § 6 Abs. 1 Nr. 1 BDSG allgemein auf die Aufgabenerfüllung Bezug nehme und daher allein auf das Erforderlichkeitsgebot rekurriere, sei ein hinreichend bestimmter Kontrollmaßstab für die behördliche Praxis nicht gegeben (so Scholz, in: Simitis (Hrsg.), § 6 b Rn.32, 7. Aufl. 2011, der auf die Rechtsprechung des BVerfG verweist). Es sollte daher die Formulierung „zur Erfüllung ihrer Aufgaben“ in § 20 Abs. 1 gestrichen werden.

Soweit für das Betreiben von Videoanlagen keine technisch-organisatorischen Anforderungen innerhalb des Datenschutzgesetzes bestehen, sollten diese in der Vorschrift geschaffen werden. Gleiches gilt für die Pflicht zur Verfahrensbeschreibung/Dokumentation.

In die Bestimmung sollte eine Regelung für Kameraattrappen aufgenommen werden, da auch diese Auswirkungen auf das informationelle Selbstbestimmungsrecht der Betroffenen haben können.

Es sollte eine Regelprüfpflicht aufgenommen werden, wonach die Videoüberwachung innerhalb eines Zeitraums auf ihre weitere Erforderlichkeit zu überprüfen ist.

Zu § 21 (Veröffentlichung von Daten im Internet)

Bislang gibt es keine Norm des allgemeinen Datenschutzrechts, die die Veröffentlichung von Daten im Internet durch öffentliche Stellen mit einem Verbot mit Erlaubnisvorbehalt regelt. Die Norm ist angemessen und hilfreich. Sie errichtet eine rechtliche Hürde (Rechtsnorm oder

Einwilligung) für die besondere Übermittlungs*form* der Internetveröffentlichung. Dies ist angesichts des „qualitativen Sprungs“ der weltweiten Zugänglichkeit, Kopierbarkeit und Suchfähigkeit von Daten im WWW datenschutzrechtlich zu begrüßen. Dem besonderen Risiko der Online-Veröffentlichung von Daten wird dadurch Rechnung getragen.

Die Norm spricht ganz allgemein von der „Veröffentlichung personenbezogener Daten“. Es sei in diesem Zusammenhang jedoch darauf hingewiesen, dass die Vorschrift jedenfalls für die Bereitstellung von Geodaten und Luftbildern im Internet kaum eine klarere Basis zur Rechtsanwendung bringen wird. Zum einen bleibt das zentrale Problem bestehen, ab wann (Bildschärfe, Zugänglichkeit von Referenzsystemen) von einem Personenbezug ausgegangen werden muss, zum anderen richtet sich die Beurteilung nach den spezialgesetzlichen Regelungen des Vermessungsgesetzes und Geodateninfrastrukturgesetzes. Soweit diesen jedoch keine spezielle Norm zur Internetveröffentlichung zu entnehmen ist, würde § 21 bei „personenbezogenen“ Daten die Hürde für den Datenzugang wohl eher erhöhen, die durch die INSPIRE-Richtlinie und das Geodateninfrastrukturgesetz gerade abgesenkt werden soll. Hinsichtlich der Datenschutzprobleme *des Personenbezugs* bei Geodaten ist § 21 „neutral“. Damit wird auch diese Vorschrift die grundsätzlichen Anwendungsschwierigkeiten, ob und inwieweit bestimmten Veröffentlichungen von Bildern die Qualität von personenbezogenen Daten zukommt, am Ende nicht lösen und dieselben Wertungsfragen wie bisher aufwerfen.

Die Ausnahmeregelung für die Adressdaten von öffentlich Bediensteten und Mandatsträgern im Rahmen ihres Aufgabenbereichs in § 21 Abs. 1 S. 2 ist ebenfalls sinnvoll. Die Regelung greift auf, dass der Schutzbedarf deutlich geringer ist als bei „privaten“ und „inhaltlichen“ personenbezogenen Daten. Durch die ergänzende Abwägungsklausel wird die Möglichkeit eröffnet, besondere Situationen (z.B. besonderer Sicherheitsbedarf) zu berücksichtigen. Allerdings erscheint die als allgemeine, immer zu prüfende weitere Voraussetzung formulierte Abwägungsklausel problematisch in Bezug auf die praktische Umsetzung. Hier wird jedem öffentlich Bediensteten praktisch ein Diskussions- und Einspruchsrecht eingeräumt, ohne inhaltliche Kriterien für die Entscheidung zu benennen. Das ist in Datenschutzgesetzen zwar nicht unüblich, dennoch spricht vieles dafür, im vorliegenden Zusammenhang ein Regel-Ausnahme-Verhältnis vorzuziehen: “…zulässig, wenn… *und im Einzelfall besondere schutzwürdige Interessen* ….“ Letztlich setzt gerade die Transparenz der öffentlichen Verwaltung einer durchgängigen Geheimhaltung der behördlichen Ansprechpartner enge Grenzen. Die Transparenz in diesem Bereich baut Hürden zwischen Bürgern und der Verwaltung ab und sollte dort grundsätzlich gewährt werden, wo dies mit den Belangen der Beschäftigten im öffentlichen Dienst vereinbar ist.

Die Befristung in Abs. 2 ist zu begrüßen. Ob das technisch mit einer auflösenden Bedingung funktioniert (dies suggeriert der Wortlaut), ist zu bezweifeln. Wahrscheinlich muss die Dienststelle nach 5 Jahren (oder früher) selbst aktuell die Löschung anstoßen und kann die

Fristüberwachung nicht dem Provider überlassen. Im Wortlaut sollte der verantwortliche Akteur, nämlich die Dienststelle, benannt werden.

Zu § 27 a (Informationspflicht bei unrechtmäßiger Kenntnisnahme von Daten)

Die Übertragung eines für die Rechtswahrung der Betroffenen präventiven Informationsinstruments in § 42a BDSG auf verantwortliche Stellen im öffentlichen Bereich ist positiv zu sehen. Die Regelung des § 42 a BDSG hat sich bereits im Rahmen von verschiedenen Vorfällen im Bereich privater Stellen als sinnvoll erwiesen. Ihre Geltung gegenüber öffentlichen Stellen ermöglicht den Betroffenen, gegenüber möglichen Missbräuchen ihrer Daten Vorsorge zu treffen. Anderenfalls würde es gegenüber den von einer unzulässigen Übermittlung Betroffenen an der gerade von öffentlichen Stellen zu gewährleistenden Transparenz fehlen.

Dies gilt insbesondere vor dem Hintergrund, dass die Regelung erst dann greift, wenn „schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen“ drohen. Unter diesen Umständen wäre es nicht nur unter Datenschutzgesichtspunkten, sondern auch aus allgemeinen rechtsstaatlichen Erwägungen heraus schwer nachvollziehbar, die Betroffenen im Unklaren über die drohenden Beeinträchtigungen durch einen Missbrauch ihrer persönlichen Daten zu lassen.

Die Erfahrungen der Aufsichtsbehörde mit dem neuen § 42a BDSG gestalten sich so, dass einige Meldungen nicht erforderlich waren, weil die gesetzlichen Voraussetzungen nicht vorgelegen haben. In anderen Fällen wurde auch von außen unrechtmäßig auf Daten zugegriffen. Immer aber ist es sinnvoll, dass sich die Daten verarbeitende Stelle aktiv mit dieser Problematik auseinandersetzt und nach Lösungen sucht, die die Betroffenen vor den Folgen schützt. Gerade öffentliche Verwaltungen sollten auch in diesem Sinne handeln.

Für Rückfragen stehe ich Ihnen jederzeit gern zur Verfügung.

Mit freundlichen Grüßen

Prof. Dr. Johannes Caspar