

quintessenz

Verein zur Wiederherstellung der Bürgerrechte im Informationszeitalter
Quartier21 / Museumsquartier
Museumsplatz 1, 1070 Wien
ZVR-Zahl: 635616285

Wien, 21. Mai 2008

Parlamentsdirektion
Begutachtungsverfahren
1010 Wien

**Betreff: BKA-810.026/0002-V/3/2008
Stellungnahme zur Begutachtung DSG-Novelle 2008**

(In Kopie elektronisch an begutachtungsverfahren@parlinkom.gv.at übermittelt.)

Einleitung

Der Verein quintessenz begrüßt eine Novellierung des DSG, bemängelt aber vor allem zwei Punkte:

- a) Eine detaillierte Regelung der Videoüberwachung ist längst überfällig um den Wildwuchs eindämmen. Die Gleichsetzung dieser Überwachungsform mit jeder anderen Datenverarbeitungsanlage ignoriert jedoch die Grundrechtseingriffe die mit so ein Installation dauerhaft und systematisiert einhergehen. Der Grundsatz müsste lauten: **Überwachung muss der geregelte Ausnahmefall bleiben, und darf nicht der anerkannte Normalzustand werden.**
- b) Es gibt große Auslassungen im neuen Regelwerk, die alte Kritikpunkte und Schwächen des DSG und der DSK nicht adressieren: Immer noch nehmen viele Unternehmen das DSG nicht besonders ernst. Die meisten Verwaltungsstrafen werden von mittleren und größeren Wirtschaftsbetriebe als kalkulierbarer Faktor mit geringem Risiko wahrgenommen.

Videoüberwachung

Sichtbare und Unsichtbar angebrachte optische Aufzeichnungsgeräte sind nicht wie eine beliebige Datenverarbeitung einzustufen. Ihr Einsatz sollte streng geregelt sein, und ihre Wirksamkeit und ihre rechtmäßige Verwendung sollte jederzeit überprüfbar sein. Ihre Anwendung und Installation soll ein geregelter Ausnahmefall sein, da er in der Regel eine große Anzahl an unbeteiligten Personen miterfasst. Bei festgestellter Unwirksamkeit oder Missbrauch sollte eine verpflichtende Demontage angeordnet werden können, die DSK auch eine Beschlagnahme veranlassen können.

Der Gesetzesentwurf vernachlässigt, wie und welcher Typ Kameras überhaupt montiert werden dürfen. So finden sich keine Einschränkungen bezüglich Schwenk- und Vergrößerungsfaktoren oder der Auflösung bezüglich bestimmter Einsatzgebiete.

Viele Kameras eignen sich, auch wenn sie für einen klar eingegrenzten Zweck installiert wurden, den öffentlichen Raum oder auch andere umliegende Grundstücke mitzuüberwachen.

Kameras sollten daher wirksam mit Sicht- und Schwenk- und Neigungsbegrenzungen ausgestattet werden, so dass diese nicht über ihren eigentliches Einsatzgebiet hinaus Aufzeichnungen tätigen können.

Beispiel: Im März 2006 wurde bekannt, dass Wachpersonal eines Berliner Museums mit Ihren schwenk- und zoombaren Kameras quer über die Spree in das Wohnzimmer der Bundeskanzlerin Angela Merkel hineinschauen konnten und haben.

Das Register von Videoüberwachungsanlagen sollte in geeigneter Form öffentlich zugänglich gemacht werden. Anderenfalls (Zugriff nur durch Polizei und Behörden) zementiert diese Datenbank nur die hoheitsrechtlichen Ansprüche des Staates, ohne die Rechte der Betroffenen gleichermaßen zu stärken.

Datenschutzkommission

Die Datenschutzkommission sollte zu einer unabhängigen aktiven selbstständigen Behörde mit ausreichenden finanziellen und personellen Mitteln aufgewertet werden. Eine Behörde mit „Biss“, die nach dem Vorbild der Kartellbehörden auch investigativ tätig ist. Es sollte ihr, personell und rechtlich möglich sein – bzw ihr dezidiertes Auftrag – zu den Unternehmen und Datenverarbeitern zu gehen, unangemeldete Kontrollen durchzuführen, sich vom rechtmäßigen Betrieb zu überzeugen und anderenfalls die sofortige Einstellung einer Anlage bzw Teile davon anzuordnen. Nötigenfalls sollte ebenfalls eine Beschlagnahme von Datenträgern, Daten oder essentiellen Teilen der Datenverarbeitungsanlage möglich sein.

Vergehen nach dem DSK müssen für die Verursacher ernsthafte Konsequenzen nach sich ziehen. Dazu könnte auch eine Ausweitung der gerichtlich strafrechtlichen Tatbestände sinnvoll sein. Entstehen oder entstanden dem Betroffenen ernsthafte wirtschaftliche Nachteile sollte die DSK direkt über Schadenersatz entscheiden, und sich nicht mit einer reinen Richtigstellung der Daten zufrieden geben.

Die DSK muß Anlaufstelle für betroffene und Opfer von Datenmissbrauch werden und schnell und unbürokratisch (Ab)hilfe schaffen können. Ist der Schaden nicht wiedergutzumachen, sollte die DSK den Opfern helfend bei anderen Behördenwegen (zb Meldedatensperre,...) zur Seite stehen.

Nur wenn sich die öffentliche Wahrnehmung von einer Verwaltungsbehörde zu einer aktiven investigativen Institution wandelt, wird sie von Datenverarbeitern ernst genommen.

Vergessen wurde ebenfalls eine verpflichtende Information von Betroffenen falls persönliche Daten bei Behörden und anderen Datenverarbeitern entwendet werden, sonstwie „abhanden“ oder in fremde Hände kommen. Ist eine direkte Kontaktierung der Personen nicht möglich, so ist auch eine verpflichtende Information über Medien vorstellbar. Der Verursacher sollte für entstandene Kosten und Nachteile der

Betroffenen aufkommen. (Änderungen von Kontoverbindungen, Benachteiligungen, etc..)

Die Regelungen im Detail

§1) Die Einschränkung des DSG auf natürliche Personen würde nun das letzte Argument beseitigen, um Anfragen ins DVR nicht als Internet-Anwendung bereitstellen zu können. Auf der anderen Seite entfällt zb der Schutz von Firmenkundendaten: So sind über das Flugmeilenkonto eines Unternehms, oder über die Bestelldaten bei einem Buchhändler Rückschlüsse auf die Geschäfts- und Entwicklungstätigkeit möglich.

Die Änderung §8 (3) 5 verneint ein schützungswürdiges Interesse auch wenn diese Daten nicht rechtmäßig ermittelt wurden. Dies ist ein Ansporn, auch illegale Daten zu ermitteln, aufzubewahren und zu Verwerten. Eine solche Einschränkung ist aber wichtig um die unrechtmäßige Erhebung unattraktiv zu machen.

Die Einrichtung eines Betrieblichen Datenschutzbeauftragten ist wichtig und gutzuheißen. Es ist klarzustellen, dass solche Datenschutzbeauftragten auch in Dienststellen des Bundes und der Länder, sowie an Schulen und Universitäten einzurichten sind.

Das Datenschutzgesetz ist nicht der richtige Ort, um Akzeptanzprobleme der Bürgerkarte (§17 1a) zu lösen. Die verpflichtende Verwendung der relativ kompliziert zu handhabenden und mit zusätzlichen bürokratischen, finanziellen und technischen Aufwand verbundenen Bürgerkarte wird die Anmeldemoral nachhaltig senken. Das ist nicht im Sinne des Datenschutz(gesetz)es.

Eine so hohe Sicherheitsstufe erscheint bei Anmeldungen im DVR im Vergleich zu vielen anderen Anwendungen im öffentlichen Bereich unverhältnismäßig. So ist es zb. in vielen Gemeinden möglich, eine Wahlkarte per unverschlüsselter und unsignierter eMail zu bestellen. eMails eignen sich, wie viele an ihrem SPAM-Aufkommen erkennen können, besonders gut Absendedaten zu verfälschen.

Eine Bürgerkarte kann auch kein Ersatz für inhaltliche Prüfungen sein. Eine bloße formelle Prüfung auf Eingabefehler ist unzureichend.

Die in einer Meldung angegebenen Begründungen zur Betrieb einer (Video-)Überwachungsanlage sollten regelmäßigen Revisionen ugf. Korrekturen unterliegen. Beim Wegfall der Gründe ist eine Demontage der Anlage durchzuführen. Ist anzunehmen, dass sich die Gründe für die Videoüberwachung in einer bestimmten Zeit ändern, so ist grundsätzlich nur eine befristete Inbetriebnahme zu erlauben.

§50a (3) Punkt 3 erlaubt die Videoüberwachung wenn der Betroffene ausdrücklich Zustimmt. Es ist leider zu erwarten, dass aufgrund wirtschaftlicher Interessen (zb durch ein Dienstverhältnis) oder andere Druckmittel eine solche Zustimmung allzu leicht einzuholen ist.

§50a (3) Punkt 3 a) erlaubt die Aufstellung einer Videoüberwachung wenn das überwachte Objekt in den letzten 10 Jahren Ort eines gefährlichen Angriffs wurde und eine Wiederholung wahrscheinlich ist.

Ein Zeitraum von 10 Jahren erscheint unverhältnismäßig lange. Es handelt sich um defakto eine Generalermächtigung für jedes Wirtshaus, jeden Supermarkt oder jeden anderen urbanen Ort mit überdurchschnittlichem Menschenaufkommen.

§50 (3) Z 7 (und andere, betreffend verdeckter Videoüberwachung und Datenermittlung) müssen befristet werden und an einen konkreten Verdachts- oder Anlassfall gekoppelt werden. Fällt einer dieser Faktoren aus, oder konnte in der gegebenen Frist kein verwertbares Material (zb für die gerichtliche Verwendung) gefunden werden, ist die Videoüberwachungsanlage zu entfernen und die gewonnenen Daten sind zu vernichten.

Das Verbot des Abgleichens von automatisationsgestützten Bilddaten (§50 (6)) ist nicht nur auf den Abgleich und Auswahlkriterien zu beschränken. Bereits die Extraktion von elektronisch verwertbaren Informationen aus dem Bildmaterial sollte verboten werden. Das betrifft zb. die Extraktion von biometrischen Gesichtsdaten, automatisches Lesen von Kennzeichen, die automatische Weg-Verfolgung von Personen (zb durch einen Bahnhof oder ein Verkehrsnetz) oder die Analyse von Bewegungsmustern und Körpersprache (Blickfeldanalyse in Kaufhäusern, Verbindungen mit anderen Kundendaten).

Eine Meldebefreiung (§50c (1) Z2) für analoge Videoverarbeitungsanlagen ist uneinsichtig: Der Grundrechtseingriff aus der Sicht des Betroffenen ist der Selbe. Eine mögliche vereinfachte Speicherung oder Auffindbarkeit einer bestimmten Stelle in digitalen Aufzeichnungen rechtfertigt keine Meldebefreiung. Vielmehr handelt es sich um eine pauschale Legalisierung älterer Anlagen.

Die Kennzeichnung einer Videoüberwachung gemäß §50d sollte zwingend Informationen beinhalten, die es dem potentiell Betroffenen ermöglicht seine Rechte gegenüber dem Betreiber wahrzunehmen. Dies sollte der Name des Betreibers, eine Adresse oder Kontaktmöglichkeit für Anfragen und die betreffende DVR-Nummer der Anlage beinhalten.